Definitive Guide™

to

Internet Isolation

Stop phishing attacks and web-borne threats from reaching user endpoints

Crystal Bedell

FOREWORD BY:
Kowsik Guruswamy

Compliments of:

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security helps hundreds of Global 2000 companies and major government agencies achieve a Zero-Trust Internet. The company's cloud-based Internet Isolation scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Definitive Guide™

to

Internet Isolation

Stop phishing attacks and web-borne threats from reaching user endpoints

Crystal Bedell

Foreword by Kowsik Guruswamy

CYBEREDGE
GROUP

Definitive Guide™ to Internet Isolation

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

IISBN: 978-1-948939-90-4 (paperback); ISBN: 978-1-948939-91-1 (eBook)
Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from Menlo Security: Young-Sae Song, Ed Jones, and Mehul Patel

Table of Contents

Foreword

How many times have you heard the phrase, "it's not if, but when"? Unfortunately, the saying can easily refer to the inevitable failure of a company's cybersecurity defenses, and it's surprising how widely accepted this view is.

Imagine someone selling you a bottle of water that was only 99 percent water, and they didn't tell you what the rest was. Would you buy it, let alone drink it? What about a $600 phone that's "guaranteed" to work 99 percent of the time—would you buy that? And yet, we don't even question security vendors that tout a 99 percent detection rate. Isn't the last 1 percent the main reason why companies get breached? Most of the spend, headaches, wasted time, and processes are centered around this 1 percent—leading to false-positive triaging, expedited recategorization, endpoint reimaging, and so on. After 20 years of cybersecurity's existence as an industry, we owe it to ourselves and our customers to conclusively solve something in security—anything at all.

The traditional approach to cybersecurity has reached its potential, and attackers have learned how to bypass even the most sophisticated defenses. According to the Verizon Data Breach Report 2019, there were 41,686 reported security incidents and 2,013 confirmed cybersecurity breaches in 2018. What's more appalling? Studies have shown that 68 percent of breaches take months or longer to detect. This means that the two primary defense methods of blocking an attack and detecting a breach once it has occurred are failing miserably.

The problem is only getting worse as companies continue to move to the cloud and adopt software as a service (SaaS) platforms to deliver mission-critical business applications. Billions of malware exploits are being created, and users are now more likely to encounter these cyberthreats outside the safety of their corporate network. The cloud and SaaS require users to connect directly to the Internet, bypassing network security and potentially costing the organization millions of dollars in damages from breaches.

Upgrading to the next-generation product won't fix this problem. To address this growing and dangerous situation, we need to fundamentally rethink the security paradigm.

What if there was another way?

- What if you could separate your enterprise network from the public web while still allowing employees to have seamless access to the Internet?
- What if you could warn employees when they're on a phishing site and prevent them from entering credentials or uploading sensitive company data?
- What if you never had to worry about malware, viruses, ransomware, or another phishing attack?

All of these "what ifs" can become a reality with a Zero Trust Internet.

Internet isolation is the technology that delivers a Zero Trust Internet by separating an enterprise network from the public web, while still allowing users to access the Internet seamlessly. The solution moves the viewing of email attachments and web browsing from the user's device to the cloud. By isolating Internet content in the cloud, users are protected from malware, ransomware, and phishing attacks that bypass legacy defenses, thereby eliminating the most prolific sources of breaches.

As many cybersecurity experts continue to lose sleep trying to perfect a faulty paradigm, the Zero Trust Internet has emerged as the best way to achieve the unthinkable: 100 percent safe email and web browsing. Rather than relying on the ability to detect threats and block them, Internet isolation simply assumes that all web content is malicious. Content is cleaned and safely rendered on users' devices for safe viewing and consumption. This prevents malware from accessing endpoints, effectively taking them off the battlefield and preventing threats from using them as a foothold to get access to the rest of the corporate network. The result? Completely safe email and web browsing.

Don't just take my word for it. Here's an example showing how Internet isolation helped a large global financial services company. As you can imagine, this Fortune 100 company has one of the most advanced security operations in the world and some of the most sophisticated cybersecurity products. Despite the millions of dollars the company was spending on cybersecurity, phishing and malware attacks were still occurring and getting past its cyber defenses—until the organization moved to a Zero Trust Internet enabled by Internet isolation.

Since the company deployed an Internet isolation cloud:

- 1,089 phishing and malware links were able to bypass traditional defenses but were stopped by Internet isolation technology.
- 8,541 known malware sites were missed by existing web filters but were blocked by Internet isolation technology.

Cybersecurity is always evolving, but it's time for a revolution. The best way to protect your organization from today's threats is to separate your users from the Internet, while still giving them access to the Internet-based tools and information they need to do their jobs. It's a radical concept, but you can't argue with the logic. The standard approach is not working, and the industry has accepted that it will fail. We need something different, and that something is the Zero Trust Internet.

Read on to learn how the cybersecurity industry is changing, how existing technologies and solutions are failing, and how Internet isolation can prevent 100 percent of all email- and web-based attacks.

Kowsik Guruswamy
CTO
Menlo Security

Introduction

IT infrastructures are rapidly evolving. Cyberattackers are continually honing their tactics. And the cybersecurity industry? It's desperately trying to catch up to new threats and cloud environments, all the while admitting failure. Security organizations must find and stop attacks before they result in a security breach. It sounds ludicrous, but organizations have had no alternatives. Until now.

Internet isolation technology turns security on its head. The concept breaks the vicious cycle of *reacting* to cybersecurity threats. By assuming that all active web content is malicious, Internet isolation delivers full protection against even the most insidious web and email threats, including phishing.

This book provides an in-depth look at Internet isolation, including how security organizations can leverage the technology as part of a cloud platform to transform their security strategy for the digital age.

Chapters at a Glance

Chapter 1, "Understanding the Security Industry's Failure to Stop Cyberattackers," discusses how security strategy has evolved and the unique challenges organizations face.

Chapter 2, "Getting to Know Today's Threats," reviews the email- and web-based threats security organizations face on a daily basis.

Chapter 3, "Understanding How the Internet Has Changed," describes how companies are embracing cloud computing and mobile applications, and the implications of cloud transformation for security.

Chapter 4, "Introducing a New Paradigm," outlines the requirements for a wholly new approach to cybersecurity: Internet isolation.

Chapter 5, "Digging Deeper into Isolation," explores how Internet isolation eliminates the risk of email- and web-based threats.

Chapter 6, "Reimagining Cloud Access," examines the components in an Internet isolation cloud platform.

Chapter 7, "Exploring Use Cases," illustrates how a platform can enable a secure cloud transformation.

Chapter 8, "Preparing for the New Regulatory Trend," highlights the power of Internet isolation when complying with regulatory requirements.

Chapter 9, "Evaluating Internet Isolation Cloud Platforms: 10 Must-have Features," reviews the features that organizations need in a platform.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Chapter 1

Understanding the Security Industry's Failure to Stop Cyberattackers

In this chapter

- Review how the security industry responded to threats in the past
- Learn why post-breach detection and response are a losing battle
- Understand the disadvantages of traditional email and web security solutions

Businesses today face a stark reality: their IT environment *will* be breached. The security industry has all but admitted its failure to get ahead of cyberthreats by advocating that organizations shift their focus from prevention to detection and response. But the truth is, this approach doesn't offer any more protection than prevention does. Security as we know it is broken. As you'll see in this chapter, the current method not only fails to solve the security problem, it also compounds existing challenges.

A Bad Game of Cat-and-Mouse

Early efforts to prevent a security compromise looked a lot like a game of cat-and-mouse. Attackers realized early on that they could send viruses and other malware to unsuspecting users via email. It was fairly easy to persuade recipients to double-click an infected attachment or visit an infected web page.

To stop these virus and other malware attacks, email security vendors created a signature by which the malware could be identified and blocked by the vendor's tool. Once a piece of malware was blocked and rendered useless, attackers went back to the drawing board to try again. For security vendors and their customers, the focus was on prevention.

Even early on there were problems with this preventative approach to security. For starters, in this game of cat-and-mouse, casualties were a given. You can only prevent what you know exists. Someone somewhere had to be patient zero before vendors learned what to look for and to block from their customers' networks so that they could create a signature. In many cases, being patient zero landed companies on the front page with thousands of employees infected.

What's more, security organizations had to continually update their security tools with the latest signatures that would protect them against current attacks. This race against time only became more challenging with the proliferation of point solutions.

As attackers began exploiting different aspects of the IT environment, security vendors responded in much the same way they did to viruses—reactively. To combat each new security threat, they built a specialized tool: antispam, antivirus, data loss prevention, encryption, etc. Even today, security teams implement and manage myriad point solutions, each intended to address a specific security threat. This approach is expensive and ineffective.

Many of the point solutions continue to leverage legacy prevention methods, even as adversaries evolve their attack methods. For example, polymorphic malware changes its code with each iteration, enabling it to bypass legacy prevention tools that depend on signature-based detection.

With threats growing increasingly sophisticated and legacy prevention no longer providing sufficient protection, the industry has been forced to face the truth: signature-based detection is far from perfect. Sooner or later, it will fail.

(Not So) Secure Gateways

In an effort to provide organizations control and security over which Internet traffic can enter the corporate network, security manufacturers designed the *secure web gateway* and an email security solution focused on web links sent via email. Unfortunately, such legacy solutions do not provide the protection organizations need against modern cybersecurity threats.

A traditional secure web gateway is intended to protect endpoints from web-based threats by enforcing security policies and filtering malicious traffic. A secure web gateway gives organizations the ability to block malicious Internet traffic from entering their private network or systems. However, administrators must know which websites to block and which to allow—an insurmountable challenge considering that a benign site can become malicious literally overnight.

An email security solution focused on malicious links and phishing attacks typically analyzes the links either before the user clicks or at the time of the click. Determining whether the link is malicious relies on a user informing security it's malicious or a sandbox analyzing it, which is an art.

The issue with such legacy solutions is their detect-and-respond approach to security, identifying only known threats. They rely on risk data or signatures from threat intelligence databases or user behavior monitoring to detect traffic anomalies. These tactics cannot keep up with increasingly sophisticated cyberattacks.

Not only do they fail to block all threats, they also generate a fair number of false positives and false negatives. The security organization has to verify each one, delaying detection and remediation of the true threat.

Next Up: Detect and Respond

The security industry can't keep up in this game of cat-and-mouse—at least not so long as it continues its current strategy. But instead of rethinking how security is done, vendors and analysts have bowed to cyberattackers. The industry has accepted that a security compromise is inevitable. Vendors have essentially said, "We can't stop an attacker from getting into your environment, so now we're going to help you contain and remediate the breach as soon as possible." As a result, the onus is on security teams to reduce the time it takes to detect and respond to a breach in hopes of minimizing the loss.

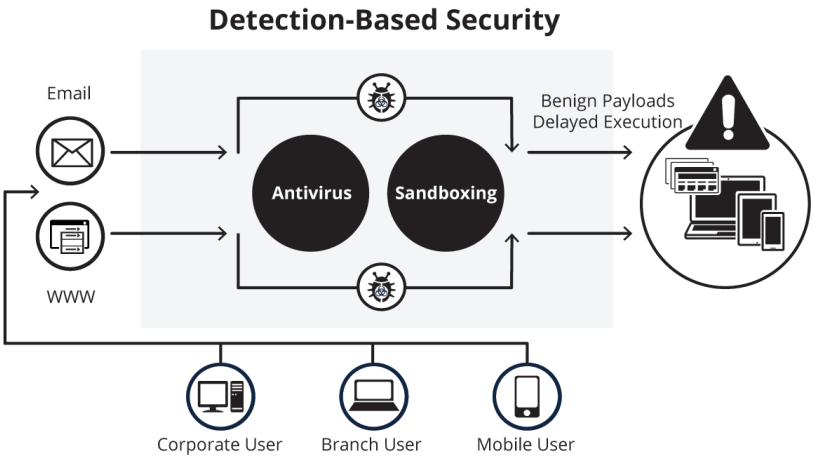

Figure 1-1: Malware can evade detection by traditional email and web security solutions.

Challenges with detect and respond

The security industry has essentially shifted the responsibility of threat detection and response onto resource-strapped security teams. These teams have a difficult task, at best. They must sift through reams of security alerts in an effort to validate and correlate true positives that point to actual malicious activity occurring on the network. It's time-consuming and resource intensive.

Security teams can't detect every breach, and according to Verizon's 2018 Data Breach Investigations Report, 68 percent of the breaches security teams do find take a month or more to discover. You can hardly call it a game of cat-and-mouse anymore. Attackers lie low, biding their time until the opportunity is right to move laterally and steal data, disrupt services, etc.

Teams are under pressure to move faster because the longer it takes to contain a threat, the greater the risk. But attackers' tactics continue to evolve more rapidly than security teams can detect them.

In addition, protecting the organization from modern cybersecurity threats requires deep insights into and context about threats and vulnerabilities, as well as web and email behavior

by users. Security analysts and threat detection and response teams need to know exactly what users were doing at the moment an attack occurred to prevent it from happening in the future. However, visibility into user behavior is difficult to come by, if it exists at all.

But, My Sandbox...

Organizations have invested millions of dollars in sandbox technology. In fact, the sandbox has become the tool of choice for protecting users against web-based threats. Unfortunately, the sandbox is also quickly becoming one more control in the IT infrastructure that attackers can evade.

A sandbox sits in a web security or email security solution as a means to detect and quarantine malicious content before it has a chance to infect an endpoint. A sandbox is designed to analyze how a web link, attachment, or document behaves on an endpoint and detect when that behavior is abnormal. This is just another example of a detect-and-respond approach to security. Although the sandbox has its downside (namely, it requires a patient zero), this technology largely succeeded in preventing web and email links/attachment-based threats—until recently.

Attackers are increasingly developing methods for evading detection by sandboxes. In one case, a file arrived via email with a .doc extension. The sandbox looked at that file, determined that it didn't have any macros, and let it through to the user. However, the file was actually an .xml file. When the user double-clicked on the attachment, it phoned home and executed malware on the endpoint.

That's just one example of attackers' full awareness about what the sandbox looks for to detect a threat. In another example, attackers have developed software that can automatically recognize if it's running on a bare metal machine with an actual user versus a sandbox in a virtual environment.

Attackers will always find ways to get past detect-and-respond controls, forcing security organizations to participate in an arms race of sorts. The question is, how long will security organizations continue to participate in this arms race? How many more millions of dollars will they spend on technology that works for only a limited time?

Additional Challenges

The threat landscape and defense strategies don't evolve in a vacuum. Other IT and business trends create additional challenges that exacerbate security issues.

Security staffing shortages

Perhaps most notably, organizations in every industry are experiencing a shortage of skilled security personnel. According to ISACA's workforce development survey, 59 percent of organizations have unfilled cybersecurity positions. If that's not sobering enough, then a forecast by (ISC)2 certainly is: the organization estimates a shortfall of 1.8 million information security professionals by 2022.

As digital becomes the new norm, companies increasingly recognize the need for security professionals to protect data and other IT assets. But—at the risk of sounding redundant –the security industry can't keep up with the rapid pace of technological innovation. There simply aren't enough people learning how to plan, manage, integrate, and optimize security devices and strategies.

Unpredictable end users

The IT environment and threat landscape continue to evolve, but one thing remains the same: the end user. End users remain the weakest point in the environment, and they can't be directly controlled with software. They are problem solvers, and they're also unpredictable and easily manipulated.

End users' primary concern is not security. It's getting their job done. They find workarounds for any technical controls that slow down their work processes.

Security awareness training is an important piece of any security program, but it only goes so far. So long as people post personal information on social media sites, attackers will know more about end users than end users know about security. This information is a powerful tool in the attackers' arsenal. Attackers use it to manipulate users and gain their trust when executing attacks.

The same ol' paradigm

The cloud offers IT organizations an opportunity to transform how they deliver services to the business. Unfortunately, when it comes to security, organizations aren't taking advantage of the cloud's benefits. Most are simply moving their on-premises security solutions to the cloud—essentially moving the problem from one datacenter to another. As a result, these organizations aren't realizing the true value of the cloud. For example, moving a security information and events management (SIEM) system to the cloud doesn't eliminate the need to review the alerts that the SIEM generates. Whether the system is in the cloud or on premises, the organization still requires human resources to manage the output.

Mind the Gap

Best practices dictate that IT organizations deploy layer upon layer of security controls, as listed in Figure 1-2, to stop cybersecurity threats from infiltrating IT assets. This approach, known as *defense-in-depth*, is intended to provide layers of defense so that if one control fails, another is in place to thwart an attack. Unfortunately, a significant gap remains.

Consider that 10 percent of web links are categorized as benign when in fact they are not (according to Menlo Security). That percentage might not sound like much until you consider what threats are involved. IT organizations lack protection against some of the most dangerous cybersecurity threats. These are highly successful and can lead to catastrophic data loss.

Catastrophic data loss usually means significant financial loss. According to the Ponemon Institute's 2018 Cost of a Data Breach Study, the average cost of a single data breach is $3.86 million, up 6.4 percent from the previous year. The average global cost for each lost stolen record containing sensitive or confidential information also increased. Each record costs $148, up 4.8 percent from 2017.

That gives a whole new perspective to 10 percent.

Figure 1-2: Despite a plethora of security solutions, security organizations lack protection against today's high-risk attacks.

Chapter 2

Getting to Know Today's Threats

In this chapter

- Understand why email and web browsing are highly vulnerable
- Explore the scope of the risk posed by insecure web browsers
- Learn how attackers exploit end users

The most common malware attack vectors today also happen to be the most frequently used applications in the workplace: email and web browsers. The majority of cyberattacks come from an attachment or link in an email or from a malicious website. The simple act of loading a malicious web page—just one little click—can result in a malware-infected endpoint, data theft, and penetration of the corporate network. Email security products identify known threats, which is great unless the attacker is using a zero-day threat. Bottom line: email and the web browser are the most important—and most vulnerable—productivity applications in use today.

Coming to an Inbox Near You

Email continues to be a primary communication medium in the workplace and, as shown in Figure 2-1, it remains a successful attack vector for adversaries. What's more, email-based attacks continue to grow more dangerous. Security organizations are no longer dealing with viruses intended to temporarily wreak havoc but instead are faced with sophisticated attacks by adversaries who have financial gain in their sights.

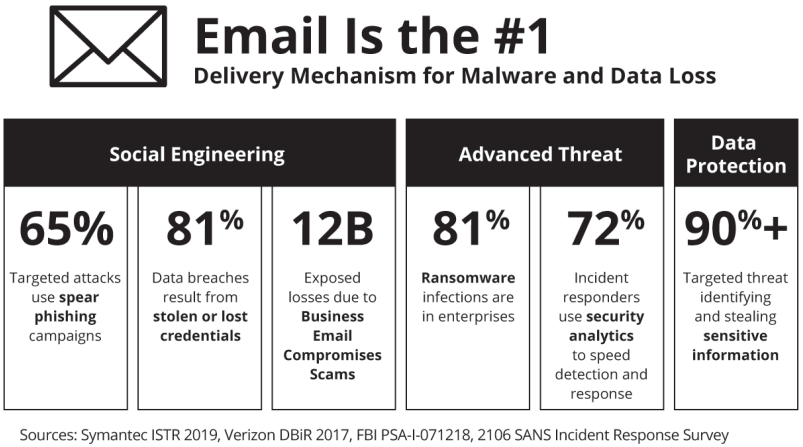

Figure 2-1: The majority of successful cyberattacks use email as a threat vector.

Phishing for data

One of the more popular attacks used by adversaries today is *phishing*—and for good reason. Phishing is considered the most effective attack method. Phishing is successful because it leverages the weakest point in the IT environment: the end user.

In a phishing attack, the adversary sends an email to a group of recipients under the guise of a company or well-known brand. The attacker requests that the recipient submit some personal details (often financial data), usually to prevent something bad from happening. For example, the attacker may pose as the recipient's financial institution and request account data so that "suspicious account activity" can be validated and blocked. A trusting user may be taken in by the urgency of the message and not think twice about clicking on an infected link or entering their sensitive financial data in a fake web form.

An especially insidious form of phishing is *spearphishing*. A spearphishing attack is more targeted. The attacker sends an email to an individual that includes personal details, adding to the message's apparent validity. Social media and other online profiles can provide a wealth of information about who the user reports to, what brands they use, their hobbies, etc.

Adversaries leverage this data to outsmart security controls and obtain the recipient's trust.

Here's an example: Brad receives an email purportedly from Sue, his manager. Sue reports to the CFO. It's the end of the quarter and a report is due by the end of the week. Brad is aware of the pressure Sue is under to deliver this report on time, so when he receives her email the night before the due date, he takes notice. She's working after hours to meet her deadline and has forgotten her password to one of the financial systems. Can Brad please help her out so that she doesn't have to wait for IT to reset her password?

The personalized nature of phishing and especially spearphishing attacks makes them incredibly difficult to prevent using traditional security controls. There's no third-party reputational data available or enough data to analyze messages internally to accurately identify them as phishing attacks. As a result, phishing and spearphishing attacks make it past the organization's defenses and land straight in users' inboxes, where users themselves are the last line of defense.

Attackers make it their business to determine how to exploit end users. With the volumes of data users share about themselves on social media, they make it pretty easy for attackers. But it's not the users' job to know how to identify and prevent every cybersecurity attack—they have other work to do. So long as these emails are received by users, attackers will always have the upper hand.

Ransomware and malware

Malware continues to evolve a step ahead of most security controls. Driven by financial gain, attackers have good motivation to develop a worm, virus, or Trojan that can bypass preventative controls and carry out its mission.

Today's sophisticated attacks are often highly targeted. Attackers may be sponsored by nation-states or organized crime groups, which provide the resources necessary to develop and execute an *advanced persistent attack*. These attacks move "low and slow," with the goal being to obtain network access, move laterally across the network, and exfiltrate data, all the while evading detection.

Malware to launch an advanced persistent attack may be sent by email as an infected attachment or a link to an infected web page. Once the user downloads the document or clicks on the link, the malware infects the endpoint and enables the attacker to gain a toehold in the organization.

A company doesn't have to be a high-profile financial institution or a critical government organization to be hit with an advanced persistent attack or malware. The truth is: no company is safe. Devices can spread malware intended for another target, or an attacker may try to exploit an organization that it suspects lacks a robust security program. And there's no need to dedicate significant resources to building a sophisticated piece of malware. Attackers can buy ransomware, for example, on the dark web.

Rather than hit a company with an advanced persistent attack, an adversary may use ransomware to con a user or the company into paying a ransom. Ransomware is a type of malware that locks the user or organization out of their device or files and threatens to publish the victim's data or permanently block access to it unless a ransom is paid. Unfortunately, even if payment is made, there's no guarantee that the adversary will deliver on his promises.

Everything Is on the Internet

Think about the various applications end users require during the course of an average work day: email and calendaring apps, customer relationship management (CRM) software, marketing automation software, project management software… the list goes on. Virtually all of them are available on the Internet as *software as a service (SaaS)* and/or mobile apps. As organizations increasingly embrace mobile and cloud computing, more and more business processes are moving to SaaS, applications hosted in the cloud by a service provider and accessed as a service via the Internet. Unfortunately, there is a flip side to these valuable web-based business resources.

The Internet is also fraught with malicious content. Virtually any website, link, or web advertisement can be used to deliver malware to an endpoint device. Most websites consist of a variety of third-party components, such as advertisements,

plugins, and content feeds, as shown in Figure 2-2. While the user may initiate only one request in the foreground, multiple requests are made in the background, and each one represents a security risk. Malicious links and malware are constantly emailed to unsuspecting people in hopes that someone will download and install it. Each of these malware risks has the potential to infect the host site without the owner or user ever being the wiser.

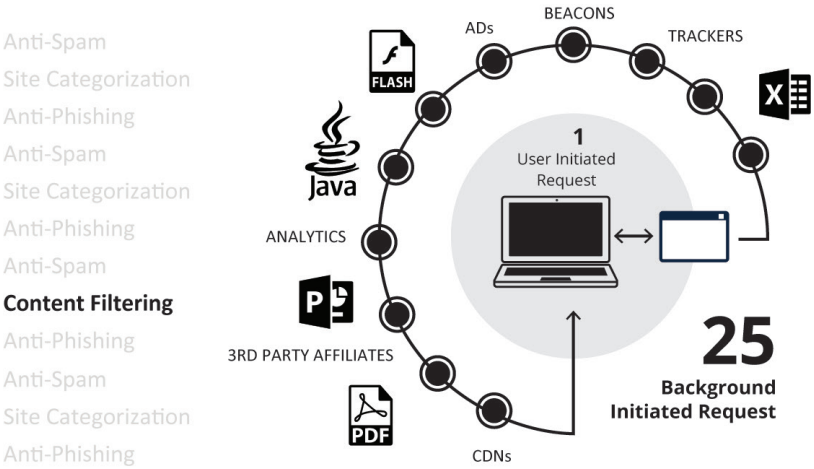

Figure 2-2: A security solution like content filtering must correctly evaluate each piece of active content on a website to determine whether it is benign or malicious.

The state of the web browser

The web browser represents a huge attack surface whereby adversaries can infect systems with malware, steal data, infiltrate networks, and disrupt services. The many ways attackers can leverage web browsers make them all the more difficult to protect.

Abounding with vulnerabilities

Like any application, web browsers have their fair share of vulnerabilities. It doesn't matter whether users are browsing the web via open-source Mozilla Firefox or a security-focused browser like Google Chrome. All browsers have security vulnerabilities that attackers can exploit. What's worse, these

attacks show no sign of slowing down. The ever-increasing number of browser features and plugins ensures that attackers will continue to have new vulnerabilities to exploit for the foreseeable future.

To further complicate matters, security solutions may block users from accessing URLs that are unknown, new, or just don't fall neatly into an existing category. However, users may still need access to these potentially dangerous sites. If users are allowed unfettered access, it may expose the organization to security threats such as malware, phishing, credential theft, and ransomware. If access is blocked, the organization risks false positives that inhibit user productivity and create a flood of help desk requests.

The problem with active content

Active content is interactive or dynamic website content that executes in the user's web browser. Examples of active content include animated images, streaming video, and embedded objects.

Unfortunately, active content is also a key component of today's browser exploits. Most of today's active content is written in either Flash or JavaScript. These programming languages can be used to deliver a malicious script to the browser, where it can give an attacker control over and visibility into the browser's operation and its vulnerabilities—all without the user's knowledge.

Chapter 3

Understanding How the Internet Has Changed

In this chapter

- Explore how the Internet has evolved
- Review the benefits of cloud transformation
- Learn how cloud computing impacts network infrastructure

The Internet has come a long way since the early days of AOL and Internet Explorer—and so have we. We do far more than passively consume web content as a form of entertainment. We use and interact with the web many times a day for anything and everything. It is so much a part of our work and personal lives that we personify our favorite web-based Internet services, like Siri and Alexa. You could say that our growing dependence on the web has given it a life force of its own. That life force is the cloud.

Cloud Transformation: The Internet Changes Everything

The concept of a remote pool of computing resources—what is essentially the Internet—led to the development of *cloud computing:* on-demand compute resources that are consumed as a service. The advent of cloud-based IT services has transformed the way businesses think about technological systems and infrastructure by commoditizing them.

Cloud-based services eliminate the need to build and manage an on-premises datacenter, leveling the playing field for

small and midsized businesses everywhere. The cloud has thus given rise to new industries and disrupted established, commoditized industries like financial services and insurance seemingly overnight.

While this transformation continues on a macro level, it's also occurring on a micro level, within businesses themselves. As more and more IT services become available in the cloud, companies are increasingly moving their IT assets and systems to the cloud as part of a *cloud transformation*. This can be a significant endeavor that involves rearchitecting systems and applications to take advantage of cloud capabilities. But the benefits, as we'll explain in the next section, make it well worth the effort. So much so, in fact, that companies are adopting a *cloud-first* strategy for net-new systems, meaning that they're prioritizing cloud-based options over those that run on premises.

The business benefits of moving to the cloud

Increasingly, companies are not just moving applications to the cloud but also purchasing applications as a service. The cloud transforms IT operations by virtually eliminating the overhead associated with running business applications and IT systems. Adopting an application, for example, as a cloud-based service avoids the need to procure and deploy the software itself, as well as the operating system and hardware it runs on. The hardware and software run in the service provider's datacenter—that is, in the cloud. The cloud service provider is responsible for the general health and maintenance of the software and hardware, including performing upgrades and managing patches and other updates. IT organizations, as a result, benefit from a significant reduction in operational expenses and workload as they relate to the application's administration and maintenance. IT organizations can also benefit from a reduction in capital expenses, as there's no need to procure the hardware for the software to run on.

Other benefits of cloud-based services include the ability to continually increase their return on investment. With traditional software, manufacturers release periodic updates and customers are expected to upgrade their software to obtain

access to the new features and functionality. Cloud service providers can continually roll out new features, and customers have immediate access to them.

IT organizations also gain agility from moving to the cloud. They can easily accommodate a growing—or shrinking—workforce or fluctuating service levels without the hassle of procuring additional servers and software licenses. Business units can turn on new features and functionalities—even launch entire business applications—at the push of a button. All it takes is a credit card. This scalability can be particularly useful for organizations that are undergoing rapid growth through mergers and acquisitions, and for those that experience seasonal spikes in resource demands.

Other factors driving cloud transformation

The operational benefits of adopting cloud-based services are reason enough to embrace a cloud transformation strategy. But other factors are coming into play as well. The Internet has changed, and so has the workforce.

Anywhere, anytime access

The workforce has become untethered from the corporate LAN, thanks to the Internet and the advent of mobile devices. Armed with their smart phones, tablet computers, and laptops, end users can work at any time and from any place. That is, so long as they have access to the business applications they need to do their jobs. Increasingly, those applications are available via the Internet as SaaS and mobile applications. SaaS solutions are accessible from anywhere, so long as the user has an Internet connection.

Anywhere, anytime access isn't just about the user's convenience—although that can improve employee productivity. The 24/7 access provided by SaaS solutions also serves as a competitive advantage for businesses, especially those in fast-moving, rapidly changing global markets. SaaS enables users to make quick, informed decisions no matter where work takes them, enabling faster, more-agile organizations.

It's all SaaS and mobile apps now

The growth of mobile computing and SaaS has transformed the Internet as we know it. The web is no longer populated with static websites. Increasingly, web-based properties are applications that support key business processes. These business processes are a tap away on the user's preferred mobile device. And this is the primary way people access the Internet when they're on the go.

Meanwhile, Back at the Datacenter

While moving core business functions to the cloud delivers undeniable business and IT benefits, it also creates new challenges. The old way of delivering secure IT services no longer makes sense in the world of the cloud. IT organizations are forced to re-evaluate their current network infrastructure and established processes for securing IT assets.

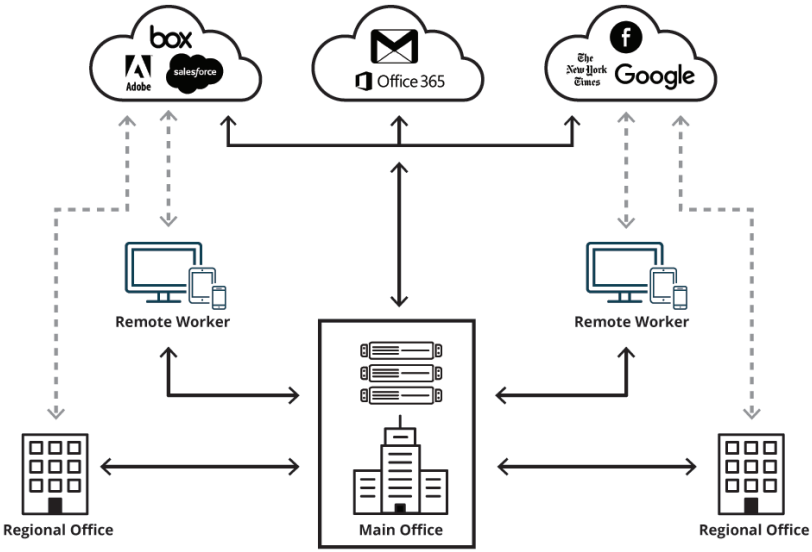

Figure 3-1: With the use of SaaS, it makes sense for traffic to go straight to the Internet, rather than being backhauled to one point.

The cloud's impact on network infrastructure

The cloud has changed the way corporate networks are managed. Traditionally, all Internet traffic is backhauled to one location, and then security is applied at the chokepoint. With the use of SaaS, it makes sense for traffic to go direct to the Internet, as shown in Figure 3-1, thus saving companies the cost of backhauling traffic to one point. This has resulted in the adoption of SD-WAN (software-defined WAN) and a change in traditional network architecture.

The cloud and security

Sending SaaS users straight to the Internet eliminates the chokepoint where organizations previously implemented security controls. It was at this chokepoint that traffic was monitored and run through threat intelligence, and an allow or block determination was made. Bandwidth costs have plummeted since users' devices connect directly to SaaS platforms through the Internet, but security organizations have lost a central point of control.

Cloud security isn't a new concern. From the very start, cloud service providers have insisted that they're only responsible for securing the cloud infrastructure. Everything else is the customer's responsibility. The problem is that organizations simply don't know how to secure their assets in this new environment. As cloud transformation continues to evolve, the pool of available talent fails to keep pace.

Meanwhile, security vendors continue to do what they do best: build more point solutions. But today, they're building solutions designed specifically for cloud infrastructure. Now security organizations aren't just struggling to secure one IT environment—the on-premises datacenter—but two or more as companies adopt multiple clouds. Organizations don't have the time, patience, or budget to duplicate their efforts. And, yet, that's what they attempt to do.

A detect-and-respond approach to security is no more effective in the cloud than it is on premises. Even the most robust, advanced threat intelligence apparatus will only catch and block a certain percentage of threats. Layering a traditional

secure web gateway, URL filtering tool, or a threat intelligence feed on top will buy organizations another percentage point or two. But no matter what they do, organizations will never be able to stop 100 percent of attacks using detect and respond. Attackers are too sophisticated, users are too trusting, and threats move too quickly. As we discussed in Chapter 1, the detect-and-respond approach is broken. Whether in the cloud or on premises, it will and does fail every day.

Security's Time Has Come

A cloud security breach can have dire consequences. Organizations risk loss of data, regulatory compliance violations, cyberespionage, and brand damage. And that's just the start. The security industry can't wait any longer. As organizations continue to figure out their cloud strategies, they should take the time to rethink how to protect their users and IT assets in this rapidly changing world.

Chapter 4

Introducing a New Paradigm

In this chapter

- Read how the cloud can help security organizations improve their cybersecurity defense
- Learn about a new approach to web and email security
- Understand how Internet isolation provides complete protection against cybersecurity threats

It's time to adopt a new approach to cybersecurity defense. No more disparate point solutions. No more alert fatigue. No more cat-and-mouse games. Security organizations need a true solution to the security challenge posed by active content executing on the endpoint—a solution that provides comprehensive protection and reduces their operational burden. Let's discuss what this new solution should look like.

Leverage the Cloud

First and foremost, cybersecurity defense should move to the cloud. Other business and IT domains are enjoying the benefits of the cloud. Now, it's time security organizations follow suit.

Deploying a security solution as a cloud service reduces infrastructure requirements and ensures high service availability and prompt platform upgrades. The cloud service provider is responsible for all of that, which means the pressure is on them to deliver. This provider should be an industry-leading

public cloud service with the resources needed to ensure high availability with a global footprint, geo-redundancy, and routing based on "least latency."

By offloading solution management and monitoring functions to the cloud service provider, security organizations can get some relief from the cybersecurity skills gap and resource shortage they're experiencing. In addition, because a cloud-hosted solution covers every user globally, users are not able to bypass security policies. Universal policy enforcement leads to fewer security incidents. With a security solution that is more effective and less resource intensive, the team can spend less time digging through alerts and more time focusing on initiatives that deliver value to the business.

A cloud-based cybersecurity solution also allows security organizations to be more agile. This flexibility is reflected in the fee model, as shown in Figure 4-1. Organizations can onboard users and offices easily and quickly since there's no need to install software locally or go through lengthy licensing processes. Auto-scaling and bandwidth management ensure that the solution grows smoothly as the organization's needs change—without the additional expense and effort of building out the infrastructure.

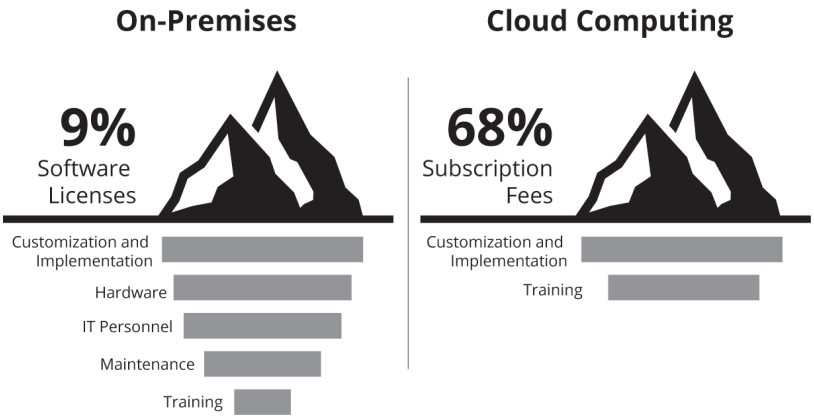

Figure 4-1: Cloud computing allows organizations to shift their budgetary expenditures from capital expenses to operating expenses.

Change the Way You Think About Web and Email Security

As we explained in Chapter 1, past efforts to eradicate email and web security threats have failed to provide complete protection. Given what's at stake if a company experiences a security breach, security organizations can no longer settle for less than 100 percent protection. That said, it's time to change the way we think about email and web security. It's time for a new approach that leverages the benefits of the cloud.

Introducing Internet isolation

Internet isolation is a relatively simple concept that has significant ramifications for email and web security. The goal of Internet isolation is to keep all browser infections and browser-related attacks away from the endpoint. This is achieved by removing the browsing process from the endpoint and moving it to the cloud, effectively creating an air gap between the enterprise network and the public web.

Internet isolation assumes a *default deny* approach, meaning that unless it's specifically allowed, all content is denied. Internet isolation also assumes that all Internet content has the potential to be malicious. Users are still able to access the Internet using an isolated remote web browser that mirrors safe content down to the browser on the endpoint. Email attachments or other documents are also rendered in the cloud, keeping the endpoint completely safe. This browser-to-browser content mirroring is achieved using a technology that's highly secure and carries only rendering updates to the endpoint and returns user input to the isolated browser. Thus, attacks are completely isolated in the cloud, and users access the public web from an air-gapped network environment.

And, guess what? It works! Internet isolation can provide 100 percent protection against web-based threats. Unlike other web and email security technologies, Internet isolation embraces a zero-trust Internet strategy. Instead of attempting to distinguish safe content from malicious content, Internet isolation treats all web-based traffic equally. That is, it's all considered risky and is by default isolated. As a result, end-user devices are isolated—and protected—from *all* browser-based threats, even the nastiest ones like phishing attacks.

Requirements for Internet Isolation

Internet isolation isn't entirely new. Virtual desktop infrastructure, client virtualization, and application virtualization all seek to isolate the endpoint from threats that can be transmitted through vulnerable software. However, as shown in Figure 4-2, these technologies fail to meet the demands of a modern workforce. In addition, leveraging virtualization technologies as an approach to Internet isolation can easily lead to high costs, as a virtualized infrastructure requires a lot of compute and infrastructure resources. End users also experience degraded compute performance because virtualization requires an agent on each machine. The user experience is further degraded due to the loss of native features, such as copy/paste and print.

Just as it's necessary to change the way you think about web and email security, it's also important to update your understanding of isolation technology. Let's look at what differentiates Internet isolation from other types of isolation solutions.

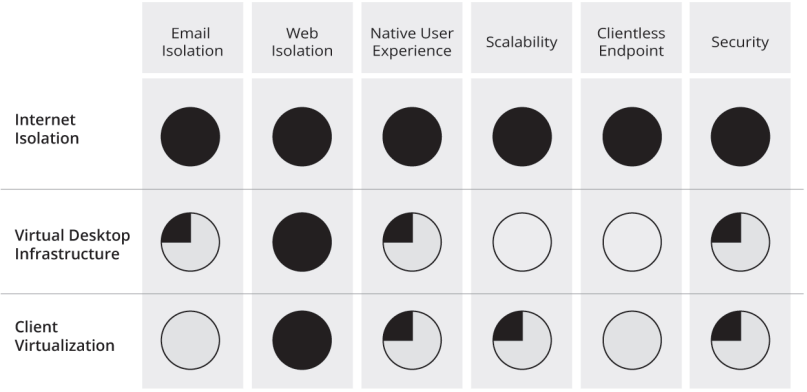

Figure 4-2: Not all isolation technologies are created equal.

Clientless deployment

The last thing security organizations need is another piece of software to install on each and every desktop, laptop, smartphone, and tablet device. Clientless deployment reduces the burden on IT as well as the risk of destabilizing the endpoint.

When consumed as a cloud-based service, Internet isolation solutions can be deployed companywide without the use of client software.

Native-like user experience

End users have a tendency to circumvent security controls that inconvenience them in any way. To avoid becoming a roadblock in the user's workflow, an effective Internet isolation solution delivers a user experience as close to native as possible. In other words, users don't notice any difference between browsing the web locally on their device and browsing the web via Internet isolation technology. There aren't any changes to the browser that can serve as distractions or any need for users to change the way they work. Perhaps most important, rendering speed and quality for a broad range of media types are identical to those of local browsing.

Scalability

Scalability must be effortless to accommodate the growing number of endpoint devices and web requests. As security organizations undergo their cloud transformation, the number of web requests will only increase. They can't be constantly worried about whether the Internet isolation solution will handle the growing demand. Thanks to the cloud, it just does.

One piece of a larger solution

To optimize the benefits of Internet isolation (which we'll cover in Chapter 5), the technology should be delivered via a cloud platform that provides a variety of other features and capabilities, including access control and data loss prevention, and web and email security. This complete solution reduces the need for myriad point products and the overhead associated with managing them separately. It also helps reduce the risk that policies will not align and threats will still get through.

Cost Comparison: Detection & Response vs. Isolation

Cost is an important factor in any purchasing decision. So how does Internet isolation technology stand up against detect-and-respond in terms of cost? Consider the following:

Malware containment

According to Menlo Security's customer data, the average enterprise spends more than 600 hours a week on malware containment. Considering the hourly average cost of a security operations center engineer is $82, the cost of malware containment comes to more than $2.5 million annually.

Internet isolation eliminates that expense. By preventing all web content from ever reaching the endpoint, Internet isolation technology eliminates the risk of malware infection.

Malware false positives

According to the Ponemon Institute, two-thirds of the time that security staff spend responding to malware alerts is the result of faulty intelligence and false positives, costing organizations an average of $1.27 million annually.

Internet isolation eliminates the expense associated with false positives. Internet isolation stops attacks before they reach the network perimeter, where an alert would be generated. No alerts mean no false positives.

Reimaging machines

Some organizations choose to regularly reimage machines as a way to stop pervasive attacks. However, Menlo Security has found that reimaging just eight devices per week could cost $3-4 million per year—not including productivity loss resulting from the planned downtime.

Internet isolation eliminates that expense. There's no need to sanitize machines because Internet isolation prevents the possibility of infected endpoints. Furthermore, Internet isolation reduces the urgency around patching machines for browser and plug-in vulnerabilities.

Help desk requests

When security organizations ramp up their blocked content policies, help desks become overwhelmed with requests from users who are blocked from accessing websites they need to do their jobs.

Internet isolation eliminates that expense. Internet isolation allows security organizations to give users access to any site they want without the risk of a malware infection.

As you can see, Internet isolation eliminates much of the financial burden associated with a detect-and-respond approach to cybersecurity threats. Not only does Internet isolation provide complete protection against web-based threats, it also enables security organizations to recoup their costs and reallocate budget to other, more-strategic IT projects.

Chapter 5

Digging Deeper into Internet Isolation

In this chapter

- Learn how web pages are delivered to endpoint browsers
- Understand the technologies that make Internet isolation work
- Explore the benefits of Internet isolation

At this point, Internet isolation may sound too good to be true. After all, the security industry has spent decades building and managing complex solutions with little effect. Why would you expect anything else? Let's take a look at how modern isolation works so you can see for yourself how it can virtually eliminate web-based attacks. But before we do that, it's necessary to understand how a web browser works.

A Crash Course in Web Browsing

It's easy to take the web for granted. One click, and there it is: a web page in all its glory. But there's a lot happening behind the scenes. Various components on the device itself work together to enable the web experience. These include operating system, application, and web browser components. For our purposes, our focus is on the web browser.

Three core functions deliver a web page to a web browser on the user's device:

1. Fetch. When a user clicks on a link, the web browser fetches a data stream—code served from web servers.

The data stream includes all of the content that makes up the web page. This includes fonts, images, and active content.

2. Execute. The fetched data is executed in the web browser on the user's device. Execution transforms the data stream from bits into content, such as video, music, articles, advertisements, and more.
3. Render. The web browser then renders the pixels, delivering the content in the viewable and interactive format of a web page.

Complexity—and risk—increase exponentially when you take a closer look at the code that the web browser fetches. Reports show that many common websites accessed by users on a daily basis run vulnerable code on their web servers, making the servers ripe for attack or hijacking.

What's more, the security issue isn't limited to one website at any given time. The user may initialize a single request on a web page. However, the website they access may connect to an average of 25 different other sites in the background. These "background sites" fetch any variety of content components. Think of the latest viral cat video from a content delivery server, or a diet pill advertisement from an ad delivery network.

Each of these fetch functions exposes the end user's device to a potentially vulnerable data stream. Of course, these actions are occurring behind the scenes, unbeknownst to the user. The problem is that the fetch function is largely invisible to current malware protection solutions like antivirus and web filtering software, as well. That means a background site that delivers malware-infested code or active content can still infect the end user's device.

What's Different About Internet Isolation

Now, let's look at a web browsing scenario where Internet isolation technology is implemented. Internet isolation moves the fetch and execute functions to a remote cloud environment, as illustrated in Figure 5-1. Only the rendering function runs in the user's web browser.

At a high level, here's what that looks like:

1. Fetch. The user clicks on a link and the web browser fetches the data stream, which is sent to the isolated cloud. There's no attempt to determine whether the traffic contains malware or any other threat. All web code is assumed to be infected and is isolated in the cloud environment.
2. Execute. All of the web code is executed in the cloud. It doesn't matter whether the web page contains active content, or if all of the content is malware-free. Everything is executed away from the endpoint.
3. Render. The rendering, and all the functionality that goes along with it, runs in the user's web browser. The page looks and feels identical to the existing web page. The only thing that's missing is the risk of a malware infection.

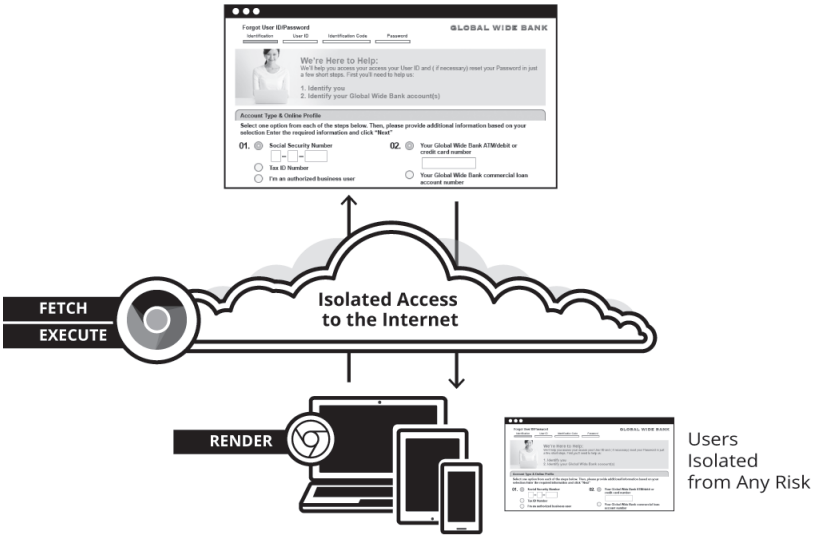

Figure 5-1: Isolation technology moves fetch and execute functions to a separate cloud environment.

The power is in the rendering

On a conceptual level, isolation is all about fetching, executing, and rendering content. Out of those three functions, rendering is arguably the most difficult to achieve. Rendering is also the important function in terms of maintaining a native-like user experience.

Most isolation solutions perform fetch and execute in the cloud and mirror all content back to the client. This approach isn't adequate. Instead, a modern isolation solution should leverage a rendering engine that adapts its approach based on the content type. The Internet is dynamic. To maintain a native-like user experience, the rendering capabilities must be dynamic, as well.

The rendering technology is also responsible for carrying clicks and keystrokes from the user's device back to the cloud. This is all accomplished without the need for any endpoint software or plugin. The result is a native-like browsing experience, minus the risk of malware infection, on a clientless architecture, as shown in Figure 5-2.

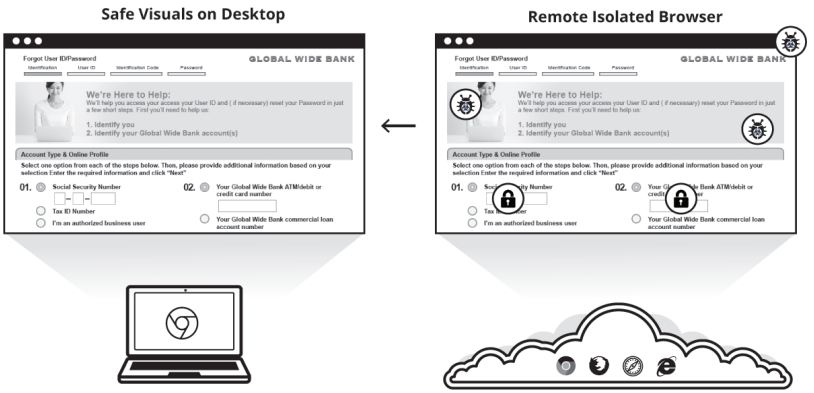

Figure 5-2: The endpoint browser loads a safe, transcoded version of the original web page that interprets rendering updates coming from the isolated browser and relays input events back to it.

Sometimes users have multiple websites and browser tabs open simultaneously. Internet isolation technology can handle that, too. When a user opens a new browser tab, a new cloud isolated browsing instance is allocated to the request. If the user navigates to a new domain in an open tab, the existing cloud browsing instance is destroyed and a new one is created. This helps prevent malware from persisting from one session to another.

The rendering technology can perform additional functions as well. For example, it can identify differences between the user's local rendering and the rendering generated by the session in the cloud browsing instance. A difference could indicate that malware on the endpoint is attempting to commit fraud by hijacking the user's local session.

The web page loaded by the user's browser is a transcoded version of the original page. Upon loading in the user's browser, the web page establishes an SSL-encrypted communication channel to a freshly allocated cloud browsing instance. The web page then applies rendering updates from the cloud browsing instance and relays user inputs back to it.

Adaptive rendering also offers other benefits. It allows web browser functions such as CSS reflow to be performed on the endpoint just as they would be performed natively. This results in fast page loads, smooth scrolling and animations, and crisp video playback. In addition, rendering can be semantically aware. This capability enables the endpoint browser to apply native fonts and UI widgets. Users enjoy a native-like experience regardless of the browser or platform they're using.

Workflow operations like copy-paste, find-replace, and printing are difficult to emulate using traditional pixel mirroring. Adaptive rendering technology provides the endpoint browser's workflow mechanisms with all the necessary information, avoiding the need to emulate the operations. As a result, workflow operations function the way users expect them to.

Isolating Documents

Document applications like Microsoft Office and PDF viewers also pose a risk to end users. Active content embedded within a malicious document can exploit vulnerabilities in the host application. It's therefore important to ensure that documents downloaded off the web or sent via email are also protected. Internet isolation can help here, too.

When a user downloads a malicious document through the isolated browser, the Internet isolation solution uses adaptive rendering technology to transcode the document into HTML5. The layout is preserved, but any malicious content is not. The rendering technology loads the transcoded content into the isolated browser. The Internet isolation solution then uses advanced mirroring mechanisms to deliver a safe PDF of the document to the endpoint.

Security Mechanisms

Adaptive rendering technology employs its own security mechanisms that, when used together, provide a strong defense against even the most determined adversaries:

1. **Active content blocking and transcoding.** All <script> elements are dropped while <object> elements are replaced with a safe remoting widget. As an extra layer of protection, the safe page itself can employ a content security policy that blocks all active content executions at its strictest setting.
2. **Protocol checking and enforcement.** In the case that an infected isolated browser sends malformed updates to a safe page, it is important that controls be in place to prevent the safe page from executing active content. Protocol checking and enforcement ensure that a safe page will not accept malformed updates and that outgoing messages adhere to a simple user-input protocol.
3. **Safe page integrity preservation.** Mechanisms in the Internet isolation solution ensure that the safe page maintains its integrity and is truly trustworthy. For example, the safe page is always served via an SSL connection with high-grade encryption. Further, it is served from a portion of the solution that is itself trusted and highly protected, and never comes into contact with isolated browsers.

Benefits of Today's Isolation Technology

As you can see, Internet isolation offers a different approach to providing secure web and email access. As such, it delivers real benefits that can transform how organizations think about security.

Internet isolation works

First and foremost, Internet isolation does what it sets out to do. Internet isolation protects endpoints against malicious file downloads and malicious content on websites, as well as malicious email links and attachments.

By taking a zero-trust approach to web content and executing active content away from the endpoint, Internet isolation eliminates the risk of malware infection while providing comprehensive phishing protection. All of this is achieved without signatures, which means no patient zero.

Preserves the user experience

When it comes to eliminating the risk of security threats, unplugging from the Internet is 100 percent effective—except for one little problem: the end user. No security solution can be considered effective if it disrupts the user experience or drives the user to implement a workaround.

Modern Internet isolation is designed to replicate the native web browsing experience, regardless of the user's browser or endpoint platform. Users still enjoy:

- ☑ Fast page loads
- ☑ Smooth scrolling and animations
- ☑ Crisp, high-quality video
- ☑ Natively available fonts and user interface widgets
- ☑ Functioning workflow operations like copy-paste and print

In addition, Internet isolation is completely transparent to the end user. The entire process of fetch, execute, and rendering takes place behind the scenes, and users are none the wiser, whether they're browsing the web or clicking on a link in an email.

Reduces IT overhead

A security solution's impact on the IT organization is as important as its impact on the end user. And Internet isolation delivers.

Because Internet isolation does its job—and does it well–the IT organization has fewer trouble tickets and fewer security alerts to respond to. It also has fewer security incidents to clean up after. And with a cloud-based solution, there's no patching or other maintenance tasks required. All of this adds up to better protection while requiring fewer resources, which means when a problem does arise, the IT organization actually stands a chance of reducing its detection and response times.

Chapter 6

Reimagining Cloud Access

In this chapter

- Learn how an Internet isolation cloud platform provides secure access to the web
- Review the features and functionality of an Internet isolation cloud platform that help prevent advanced cybersecurity threats
- See how an Internet isolation cloud platform protects users from advanced email-based and web-borne attacks in one platform

An Internet isolation cloud platform combines email security, web security, and phishing and security awareness training into a single platform. Tried-and-true technology like URL filtering and data loss prevention come together with Internet isolation to create a robust security solution. Because everything's under one hood, security organizations can reduce their overhead and ensure policy alignment across all of their controls.

Email Security

A detect-and-react strategy is ineffective at protecting users against malware and sophisticated phishing attacks. Instead of trying to improve upon a strategy that doesn't work, an Internet isolation cloud platform takes an altogether different approach. It applies a zero-trust strategy to protect endpoints against advanced cyberthreats.

Email link isolation

It doesn't matter who emails a link or under what pretext–it could be included in a promotional newsletter from a business partner or part of competitive information sent by a colleague. Any link users click on is opened in an isolated browser. This protects against targeted spearphishing and drive-by exploits without relying on error-prone threat detection.

As an added measure of protection, administrators can configure an Internet isolation cloud platform to grant read-only access to websites. This means users can only view websites. They are prohibited from submitting information in web forms. This measure provides protection against credential theft.

Email attachment isolation

An Internet isolation cloud platform also isolates email attachments. Any document the user clicks on is opened on a remote, cloud-based server. This eliminates the risk of weaponized email attachments infecting user endpoints.

Administrators can allow users to download safe PDF versions of document attachments. The Internet isolation cloud platform removes all dynamic content from the documents, and then creates a safe version in Adobe Acrobat.

There may be some instances where users need to download documents in their original form. In these cases, administrators can allow users to do so on a policy-controlled basis. (For example, per user, per group, per domain, etc.)

Antivirus scanning and sandboxing options help ensure that any documents downloaded in their original form are safe. If a user requests an original attachment, the Internet isolation cloud platform performs an antivirus scan on the document. If no malware is found, then the document is further analyzed in a sandbox to ensure it is not a threat. Even password-protected documents contained in ZIP files can be scanned and inspected.

Integration with existing email infrastructure

An Internet isolation cloud platform can integrate with a variety of existing email server infrastructures, both in the cloud and on premises. They include Microsoft Exchange, Gmail, and Office 365. What's more, this integration doesn't require endpoint software or network appliances.

As a result, an Internet isolation cloud platform...

- ☑ significantly reduces deployment and installation time
- ☑ decreases management overhead time and expense
- ☑ mimics the native user experience (users don't have to deal with changes to their workflows)
- ☑ preserves system performance—there's no perceptible delay when viewing a safe version of attachments

Web Security

Web security requires a three-pronged approach that includes access control, threat prevention, and data protection. An Internet isolation cloud platform incorporates features and functionality to address each of these needs, in addition to isolating websites.

Access control

An Internet isolation cloud platform provides a number of features that ensure safe access to the web.

URL filtering and acceptable use policy

An Internet isolation cloud platform allows organizations to enable, isolate, block, and restrict access to the web using categorization and exception-based policies, while controlling employee web browsing via granular policies like user, group, or IP. Administrators can also limit user interaction with specific categories of websites, as well as deploy a block or isolate acceptable use policy.

Application control

An Internet isolation cloud platform also gives administrators the ability to control which web-based applications users can access and the features they can use within those apps. For example, access to Facebook may be limited to marketing employees, and their ability to use messaging functionality is blocked.

Security organizations can use application control to ensure that people only use the cloud services that have been approved. For instance, users may be given access to Dropbox but blocked from OneDrive, Google Drive, and Box. This helps prevent shadow IT–the adoption of unsanctioned cloud services.

File control

Access control also extends to documents. An Internet isolation cloud platform can support a wide variety of file types. Administrators can configure granular policies to limit document access based on file type and user. In addition, documents can be downloaded in their original form or as cleaned versions processed by the Internet isolation cloud platform. Administrators can also configure the solution to prevent users from uploading documents to the Internet.

Threat prevention

An Internet isolation cloud platform provides protection against advanced cybersecurity threats that are known to bypass preventative controls.

Cloud sandbox

An Internet isolation cloud platform can leverage a cloud sandbox at the time a request is made by the user to access an original file. Suspicious files are opened in the cloud sandbox, where they undergo a content and malware analysis.

Antivirus

When users encounter known-bad malware, there's no need to go through the isolation process. Antivirus capabilities within the Internet isolation cloud platform can stop malware, while resources are reserved for other risks.

Threat feed integration

Similar to antivirus, threat feed integration helps stop known threats. There's no need to spend valuable resources isolating something that the industry has already identified as bad.

Data protection

There are many ways data can leave the organization. Isolation helps stop attackers from gaining a foothold in the organization via the web and stealing data that way. Additional data protection mechanisms are necessary to stop users from giving up data, as shown in Figure 6-1.

Data loss prevention (DLP) integration

An Internet isolation cloud platform not only integrates with existing DLP solutions, it also enhances their visibility and effectiveness. The key is in how data is presented: in a consistent and simple format that any DLP solution can understand. In addition, administrators can control the data that's transferred in HTTPS streams. HTTPS form data is intercepted and DLP policies are applied without a break in the HTTPS connection.

Cloud DLP

Cloud DLP functionality helps prevent users from uploading sensitive information to or downloading it from the cloud. For example, users may be blocked from entering financial data or a Social Security number.

SaaS application visibility

An Internet isolation cloud platform also gives security organizations the visibility needed to control user access to web-based applications. CASB capabilities provide deep visibility into and control of cloud and SaaS traffic, thus protecting data and ensuring compliance.

An Internet isolation cloud platform integrates with existing third-party CASB solutions.

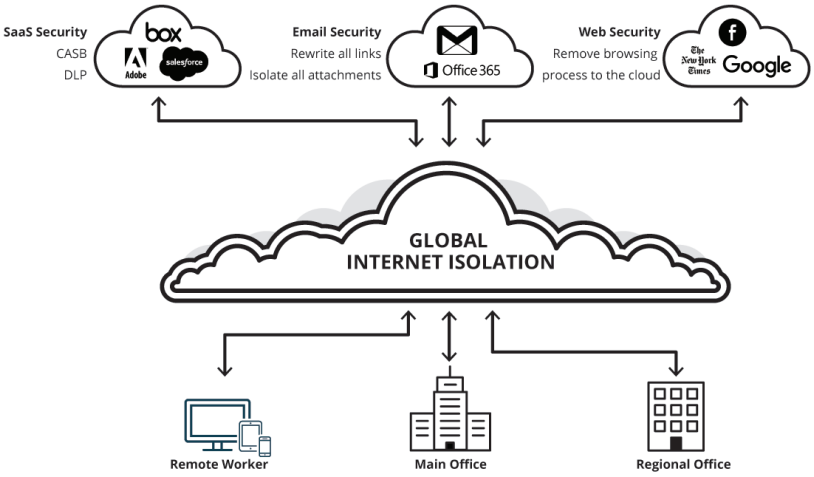

Figure 6-1: An Internet isolation cloud platform incorporates URL filtering, DLP and CASB functionality, and email security in one platform.

Security Awareness Training

Security awareness training remains an important component of any security program, regardless of the security controls an organization has in place. An Internet isolation cloud platform can help here, too. The platform can provide visibility into user behavior so that administrators can identify which users are clicking on risky links and need additional training. (Note: Even if a user does click on a malicious link, all sites are isolated, so no harm is done.) Administrators can configure real-time warning messages to reinforce training during the user's workflow—when it's needed most and when it's most likely to resonate.

Chapter 7

Exploring Use Cases

In this chapter

- Review how IT organizations can put a stop to phishing and advanced email attacks
- Learn how an Internet isolation cloud platform enables a secure cloud transformation
- Explore how IT organizations use an Internet isolation cloud platform to grant safe access to all websites

An Internet isolation cloud platform provides the cybersecurity protection that companies have long sought. But where does an IT organization start? In this chapter, we look at several use cases for an Internet isolation cloud solution so that readers can begin to envision how to apply the technology in their own organizations.

Use Case: Preventing Phishing and Attachment-based Email Attacks

Email continues to be a primary attack vector due to the success of phishing and ransomware. Traditional and even most modern security solutions fail to identify phishing emails, making users the last line of defense. As shown in Figure 7-1, an Internet isolation cloud platform removes this burden from users and effectively puts an end to phishing and ransomware attacks.

Instead of looking for phishing and other email threats, an Internet isolation cloud solution automatically isolates all web links and attachments sent via email. Whether the link is safe or infected with malware, it's executed away from the end-point. If the link does go to a website infected by malware, that malware is contained on the isolated remote browser. In addition, administrators can prevent users from submitting information to websites, eliminating the risk of users' giving up their access credentials or other sensitive data to an attacker.

Email attachments are wrapped such that they open in the Internet isolation cloud. Administrators can configure the Internet isolation cloud platform so that attachments can be viewed as a safe PDF or downloaded in their original format.

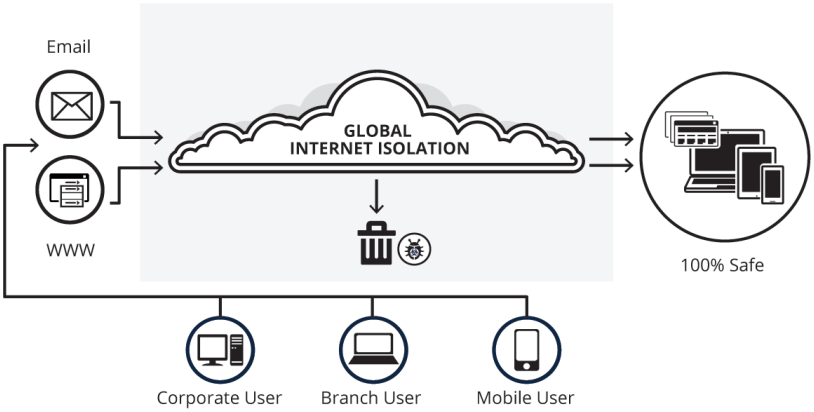

Figure 7-1: An Internet isolation cloud platform protects end users against advanced email and web-borne attacks.

Use Case: Achieving Secure Cloud Transformation

Security remains one of the top concerns IT and business leaders express about moving to the cloud. With each new cloud service a company adopts, its IT environment and threat landscape expand, increasing the risk of malware infection, data loss, and network infiltration.

What's more, simply moving services to the cloud does nothing to improve security. Organizations reduce the cost and complexity of managing those services, but the security challenges that existed on premises still exist in the cloud. An Internet isolation cloud platform supplies security that's missing in a cloud environment, enabling organizations to undergo a secure cloud transformation.

Use Case: Protecting Against Malicious File Downloads and Web Content

A Fortune 50 financial services organization researched the source of all malware that reached its network and found that more than 60 percent of infections came from uncategorized websites. This finding poses a dilemma for organizations. End users need access to the Internet to do their jobs, but it's impossible to categorize every site on the web. Even if it were possible, a known good website can become bad overnight. Plus, liberally blocking websites can increase the burden on the help desk when users want access to a benign site.

An Internet isolation cloud platform enables users to safely browse the web while giving IT organizations the peace of mind that threats from uncategorized websites will not infiltrate their private network. The Internet isolation cloud replaces legacy web proxies and provides an air-gapped execution environment for web browsing sessions. Administrators can block designated content categories and prevent users from posting on social media websites or uploading documents. They can also disable Java and Flash on endpoints, eliminating the risk of attack from these vectors.

However, even if users visit a website that isn't categorized, any malicious content or payload is confined to the isolated remote browser. The endpoint remains safe and secure, and the help desk doesn't have to categorize or reclassify sites. Meanwhile, the Internet isolation cloud provides administrators with the visibility and reports they need to monitor users' web activity.

Internet Isolation Technology Reunites Employees with the Web

A global insurance company discovered that 80 percent of its web malware infections were caused by employees accessing uncategorized websites. Desperate to put an end to web-based malware and phishing attacks, the company tried everything–even preventing user access to any uncategorized website.

The company knew that limiting web access would cause an explosion in help desk requests, but that was just the beginning. Many frustrated users decided to circumvent the new security measures. This left the company in even more dangerous waters.

After learning about Internet isolation and the cloud-based Menlo Security Isolation Platform, the company decided to try it out. They conducted a proof-of-concept deployment and found that isolation alleviated the need to limit web access–even to uncategorized websites. There was no doubt that isolation could address employees' web-based malware challenges, but there was still the issue of cost.

The organization decided that cost efficiency would be the determining factor in whether to acquire the Menlo Security Isolation Platform. They tallied their current costs associated with remediating malware-infected devices and responding to help desk requests, together with reduced employee productivity and the ongoing risk of becoming infected or suffering a data breach. This total was compared to the cost of obtaining and deploying the Menlo Security Isolation Platform.

In the end, it was a no-brainer. The company's costs would be significantly decreased by deploying the Menlo isolation solution.

Isolation has since put an end to successful web and email attacks while increasing employee satisfaction and maintaining a familiar user-accepted experience. Employee productivity is up, help desk requests are down, and devices are safe–all because of isolation technology.

Chapter 8

Preparing for the New Regulatory Environment

In this chapter

- Learn how a single phishing email resulted in Singapore's largest security breach
- Understand the difference between network separation and Internet isolation
- Explore how Internet isolation can help organizations meet the Singapore government's recommendations for cybersecurity

In June 2018, Singapore's biggest health network experienced the largest breach in the country's history. The attackers, dubbed Whitefly, stole the personal data of more than 1.5 million patients, including prescription data for the prime minister. A joint investigation by SingHealth and the government resulted in a report outlining 16 recommendations for avoiding future attacks. These recommendations, which include network isolation, have the attention of legislators and governments around the world.

The Phish that Started It All

The SingHealth data breach started with a highly targeted phishing email. According to the Cybersecurity Agency of Singapore, an attacker obtained access to a front-end computer at Singapore General Hospital by conning an end user into clicking a link in an email. The link automatically

installed custom malware on the computer, which gave attackers access to the system. But the attackers didn't act right away.

After several months the attackers started distributing malware and stealing credentials, including those that gave them access to the electronic medical record (EMR) database. They avoided secondary targets that could have given them away and destroyed evidence of their presence.

In January 2019, the Singapore government issued a report on the lessons learned from the attack. The report outlined 16 recommendations that range from improving incident response processes to creating better antiphishing education for users. Seven of the recommendations were labeled a priority.

A poor decision made in haste

Before the report was issued, SingHealth made a rash decision to disconnect healthcare systems from the Internet. It's easy to see why, given the extent of the breach. Plus, network separation had already been applied to government systems, so there was precedent for it. In light of the SingHealth breach, some government officials were calling for the same practice to be applied to healthcare networks.

Unfortunately, network separation causes more headaches than it's worth. The Singapore government's intent was good but misguided because, contrary to popular belief, network separation does not provide complete protection against web-based threats and attacks. Adversaries can use advanced attack techniques, like those explained in the sidebar, to steal data and infiltrate devices over air-gapped networks.

Network separation also creates productivity and workflow issues for security organizations end users alike. IT has to maintain and monitor two separate networks to ensure that devices on the health network aren't connecting to the Internet. At the same time, users need access to web-based tools and information for reporting and research. The trade-off—improved but incomplete protection in exchange for a poor user experience and added IT overhead—just wasn't worth it.

Network Separation Doesn't Cut It

In an effort to protect their networks and IT assets, some government and military organizations have adopted network separation. The idea is that if a device can't access the Internet and web, then it can't be compromised. While this approach does reduce the risk of compromise, it doesn't eliminate it. To be clear: endpoints don't have to be connected to the Internet to be compromised. Consider the following threats:

- Data downloaded from the Internet can be transferred to a network-connected device via a USB drive.
- Cellphone-based malware can use electromagnetic waves to poach data from network-separated systems.
- With acoustic signaling, attackers can use an acoustical mesh network to circumvent network separation and steal data.
- Airhopper is malware that uses FM frequency signals from a nearby mobile phone to infiltrate network-separated devices.
- BitWhisper is an attack method that uses thermal manipulation to steal data using a covert signal.
- GGMem uses cellular frequencies produced by a standard internal bus to convert an isolated device into a cellular transmitter antenna to steal information via GSM frequencies.
- Magneto is another technique for passing data from network-separated computers to smartphones using electric fields.
- Fansmitter is malware that uses fans in network-separated computers to send acoustic data.

A Better Approach than Separation

It's not necessary to completely separate Internet-connected devices from the rest of the corporate network to protect end users against phishing and other advanced cyberthreats. Security organizations only need to isolate web-based activity, including web content accessed from email links. By doing so they can protect end users and preserve the native web browsing experience. An Internet isolation cloud platform also offers a number of other benefits, as shown in Figure 8-1.

Physical Internet Separation	Internet Isolation Platform
• Malware can be downloaded through other means • Users having to use two computers disrupts work flows • Limited access to Internet saps productivity • Additional capex and opex costs for separate devices • Devices reserved for "Internet use" still at risk	• Web content is fetched and executed in a cloud-based browser, preventing malware from accessing users' devices • Web content is rendered in HTML5, giving users a consistent browsing experience • No client or special browser to install • No pixelated pages or noticeable latency • Preserve web functions such as copy, paste, and print

Figure 8-1: An Internet isolation cloud platform offers distinct advantages over physical network separation.

Web isolation, when deployed as part of an Internet isolation cloud platform, helps organizations meet a number of the recommendations established by the Singapore government to protect against web-based threats:

- ☑ Improve staff awareness of cybersecurity
- ☑ Secure domain controllers against attacks
- ☑ Improve incident response processes
- ☑ Implement a robust patch management process
- ☑ Implement an Internet access strategy that minimizes exposure to threats

Let's take a closer look at each of these recommendations and how web isolation can address them.

Improve staff awareness of cybersecurity

The Singapore government advises organizations to improve staff awareness of cybersecurity in order to better prevent, detect, and respond to security incidents. This includes:

- ☑ Improving the level of cyber hygiene among users
- ☑ Implementing a security awareness program to reduce organizational risk
- ☑ Equipping IT staff with sufficient knowledge to recognize the signs of a security incident

An Internet isolation cloud platform ensures that phishing attacks are mitigated and users are educated on identifying the characteristics of a phishing website. Any time a user clicks on a link in an email, the browsing session is started in an isolated remote cloud environment. Once the phishing site is isolated, a custom banner can warn users about it. Administrators can also prevent users from submitting data via a web form.

Secure domain controllers

The Singapore government recommends that organizations better secure their domain controllers against attacks. This effort includes:

- ☑ Regularly updating operating systems for domain controllers to protect them against the risk of cyberattack
- ☑ Limiting login access to administrators
- ☑ Requiring two-factor authentication for administrative access

With an Internet isolation cloud platform in place, all browser traffic from the domain controller is isolated in the cloud. No active content, whether good or bad, is executed locally. As a result, malware doesn't have a chance to execute on the domain controller.

Improve incident response processes

To enable a more effective response to cyberattacks, the Singapore government recommends that organizations improve their incident response processes. Specifically, organizations should:

- ☑ Frequently test response plans to ensure effectiveness
- ☑ Strike a balance between containment, remediation, and eradication and the need to monitor an attacker and preserve critical evidence
- ☑ Ensure the availability of information that's needed to investigate an incident
- ☑ Establish an advanced security operations center or cyber defense center to improve intrusion detection and response

An Internet isolation cloud platform prevents web-based threats from reaching the network perimeter, the point when an alert is typically generated. As a result, the Internet isolation cloud platform significantly reduces the number of false positives that incident response teams have to investigate. Incident response teams benefit from reduced alert fatigue and more time to focus on actual threats.

Implement a patch management process

The government recommends that organizations implement a robust patch management process to address vulnerabilities. To this end, organizations are advised to:

- ☑ Formulate and implement a clear policy on patch management

While patch management is important for reducing cybersecurity risk, the effort consumes considerable resources. Security organizations must first test patches and then coordinate their rollout across multiple departments, all the while hoping that a patch doesn't cause an outage.

An Internet isolation cloud platform can help reduce the overhead associated with patch management. Because active web content is executed away from the endpoint, attackers are unable to exploit vulnerabilities on the endpoint's web browser. Security organizations can thus de-prioritize browser patching and focus on more-urgent vulnerabilities first.

Implement an Internet access strategy

The Singapore government advises organizations to implement an Internet access strategy that minimizes exposure to external threats. More specifically, organizations should:

- ☑ Consider their Internet access strategy afresh
- ☑ If in the healthcare sector, consider the benefits and drawbacks of Internet surfing separation and Internet isolation technology, and put in place mitigating controls to reduce residual risks

Internet isolation ensures that all web-based user activity is executed in a secure, trusted environment in the cloud. Since no web pages are actually executed on the device, users cannot inadvertently unleash malware on their own device or any devices they're connected to throughout the network.

When security organizations deploy Internet isolation as part of an Internet isolation cloud platform, they benefit from additional capabilities that help protect against any residual risk. For example, URL filtering and acceptable use policy help prevent users from visiting sites that are inappropriate for the workplace. DLP and CASB capabilities help prevent the loss of sensitive data and provide visibility into SaaS applications.

Looking forward

Given the severity of the SingHealth data breach and the effectiveness of Internet isolation in preventing phishing attacks, it's likely other governments will consider adopting similar recommendations. In the interest of protecting the privacy of their citizens, it's even likely that the recommendations will become regulatory requirements in the future.

Chapter 9

Evaluating Internet Isolation Cloud Platforms: 10 Must-have Features

In this chapter

- Learn what features and capabilities to look for in an Internet isolation cloud platform
- Explore deployment options for an Internet isolation cloud platform
- Read about one company's success in eliminating web-based malware with an Internet isolation cloud platform

An Internet isolation cloud platform changes the way security organizations approach web and email security. At last, they can proceed with their cloud transformation with the assurance of complete protection against web-based threats as well as robust protection against data loss. As organizations begin evaluating Internet isolation cloud platforms, it's important they keep these 10 features front-of-mind to ensure that they get the functionality they need.

Web Isolation Technology

Web isolation technology is the heart of an Internet isolation cloud platform. Organizations should look for a solution with technology designed to protect users and endpoints from all active and malicious content, whether it's a link sent via email or a site that's been previously categorized as "good" or "safe"

by the organization. The technology should also make efficient use of endpoint and network resources to avoid impacting compute performance or increasing network latency.

Protection Against Phishing and Other Email Threats

An Internet isolation cloud platform should include and integrate email security. Internet isolation is an effective means of countering phishing and other advanced email threats. It's also the only way to achieve complete protection. The links and attached documents users click on in emails should be isolated in the provider's cloud sandbox, and users should be prevented from filling out suspicious web forms that could be collecting sensitive information.

Global Elastic Cloud

The Internet isolation cloud should provide universal access. This ensures that users can safely access web-based resources from any location and on any device.

The cloud service a provider uses will impact service delivery. Organizations should consider a platform that's hosted on a global elastic cloud with autoscaling and least-latency-based routing. These features, along with an industry-standard service-level agreement (SLA), will ensure high availability and high performance. A global elastic cloud should support thousands of users, enabling organizations to support a rapidly growing user base instantly.

When considering the provider's cloud, ask the following questions:

- ☑ Does the service run on an architecture built for high availability?
- ☑ Does the vendor use full virtual machines or containers for the browser sessions?
- ☑ Is the browser session set back to a known good state for each new user session? How about for each tab opened within a given user session?
- ☑ How strong and secure is the isolation architecture?

Advanced Threat Protection

Advanced threat protection requires a zero-trust approach. The Internet isolation cloud platform should assume that all content is risky, including content that was previously benign. If a solution categorizes content, then the organization can't be certain that it will protect against advanced threats.

Product evaluators should ask the vendor what percentage of threats is known to get past their solution. An Internet isolation cloud platform should provide 100 percent protection against all web- and document-borne threats, including zero-day malware. If a vendor cannot attest to zero endpoint infections, then organizations should move on to the next solution.

Deployment Options

An Internet isolation cloud platform should provide flexible deployment options. Many IT organizations are adopting software-defined WAN (SD-WAN) technology. That being the case, it is wise to consider an Internet isolation cloud platform that will integrate with SD-WAN.

Clientless Architecture

Clientless deployment is key to delivering a native-like user experience and minimizing the impact on the IT organization. With devices proliferating almost daily, IT organizations don't have the resources to deploy clients on every endpoint. They should look for a platform that supports a clientless architecture.

When evaluating a platform's architecture, ask providers the following questions:

- ☑ Is a local client/agent required?
- ☑ How is web video content, such as YouTube, handled?
- ☑ How are mobile users handled?
- ☑ Does the vendor have a secure web gateway offering or a partnership for traffic that can't be isolated?
- ☑ Does the solution impact CPU performance?

More Than Isolation

Complete protection against web-based threats is great, but an Internet isolation cloud platform can do even more. Organizations should look for a solution that provides additional capabilities as part of the platform. This approach will enable the organization to consolidate must-have security controls, including:

- ☑ Antivirus
- ☑ URL filtering
- ☑ Data loss prevention
- ☑ Logging, analytics, and reporting
- ☑ User/group policy and authentication
- ☑ Encrypted traffic management
- ☑ Cloud access security broker
- ☑ Email link and attachment protection

Deep Insights

In order to effectively remediate threats and prevent future attacks, a security organization must know exactly what users were doing the moment an attack occurred. An Internet isolation cloud platform can provide deep insights into and context for threats and vulnerabilities, as well as users' web and email behavior.

Organizations should consider a solution that enables them to monitor user access to websites and documents residing on the Internet. The ideal solution also generates detailed reports that provide insights into threats, vulnerabilities, and email and web activity for improved security investigations, remediation, and regulatory compliance.

Native-like User Experience

An Internet isolation cloud platform should have minimal impact on the user experience. If users notice any difference at all, it should be the lack of security incidents that previously derailed their workday. The platform vendor should intentionally design the product with the end user in mind. That means using sophisticated technologies like adaptive rendering that preserve as much of the native user experience as possible. Users should be able to use their favorite plug-ins and short cuts, with no impact to performance.

To help you assess the user experience of an Internet isolation cloud platform, ask providers the following questions:

- ☑ How does the browser service support plug-ins? Which plug-ins does it support?
- ☑ How well does the remote browser support cloud SaaS applications such as Office 365 or G Suite?
- ☑ Does the browser service provide a remote viewer for safely viewing file objects encountered on the public Internet?
- ☑ Does the service scan files before users download them from the public Internet?
- ☑ When the user wants to cut/paste data from the Internet, what happens?

Reduced TCO

One of the benefits of using a cloud-based solution is the subscription-based pricing structure. Security organizations should look for an Internet isolation cloud platform that enables them to categorize the technology as an operating expense with per-user pricing, rather than a capital expense. This will help with cost management and reduce the total cost of ownership (TCO).

High-risk Target Eliminates Web-based Malware Exploits with Internet Isolation

With millions of customers worldwide and trillions of dollars in assets, a leading global investment firm was a high-profile target for cybercriminals. Nearly every aspect of its infrastructure was under constant attack. A layered defense protected the organization against a broad variety of threats, but email phishing attacks were becoming an increasingly serious threat. Something had to be done.

To combat email threats, the organization deployed multiple layers of security. The architecture included cloud and on-premises versions of antispam, antivirus, data security, encryption, and sandboxing solutions. But it just wasn't enough. Spearphishing attacks and drive-by malware exploits were still a significant risk. It would only take one successful attack to cause billions of dollars' worth of damage.

The IT team knew it needed a new approach to protecting its end users against phishing and drive-by malware exploits. Having successfully deployed the Menlo Security Next-Gen Secure Web Gateway to eliminate web-borne malware from uncategorized websites, the organization decided to add isolation to its email security strategy. The Menlo Security Email Isolation service is designed to protect end users from malicious email links that cause malware infections or lead to phishing sites.

Today, all web sessions pass through the isolation platform. Visibility into user behavior enables administrators to identify who is clicking on potentially malicious links and needs further security training. When users do click on malicious links, all sites are safely isolated and have input-field restrictions. By isolating all email links, Menlo Security Email Isolation protects the firm against credential theft, while eliminating 100 percent of drive-by malware exploits.

Moving Forward

An Internet isolation cloud platform is the first of its kind. Its the first security solution to deliver complete protection, in the cloud and on premises, against advanced email and web-borne threats. With an Internet isolation cloud platform, security organizations can finally rest assured that users are protected against phishing attacks and that a random Internet click won't lead to infection or data loss. By choosing a platform that meets the previous criteria, security organizations can finally shift their focus to more strategic endeavors.

Glossary

active content: interactive or dynamic website content that executes in a web browser.

advanced persistent attack: a highly targeted attack in which adversaries seek to maintain network access, move laterally across the network, and exfiltrate data, all the while evading detection.

air gap: created by removing any physical or digital connections between two or more IT assets or networks.

cloud computing: a pool of on-demand compute resources that are consumed as a service.

cloud sandbox: an isolated server in a service provider's cloud.

cloud transformation: the process of moving and rearchitecting on-premises systems and applications to run optimally in the cloud.

default deny: an approach to security that assumes all traffic or content is potentially malicious and is therefore denied access unless specifically allowed.

defense in depth: a security strategy that calls for implementing layers of defensive technologies so that if one fails to stop a threat, another security control will be in place to potentially thwart it.

Internet isolation cloud platform: a cloud-based security solution that combines isolation technology and web security, email security, and phishing and awareness training into a single platform.

phishing: a type of attack in which an adversary poses as a trusted company or individual and sends a message to a recipient with the intent of manipulating him/her into sharing sensitive information, downloading a document, or clicking on a link that is infected with malware.

ransomware: a type of malware that locks the user out of their device or files and threatens to publish the victim's data or permanently block access to it unless a ransom is paid.

shadow IT: applications, often web-based, which are adopted by users without the IT organization's approval.

spearphishing: a form of phishing attack in which the adversary targets an individual and includes personal information in the message to gain the recipient's trust.

software as a service (SaaS): applications hosted and managed in the cloud by a service provider.

zero-day threat: a previously unknown cybersecurity threat that exploits an unknown vulnerability.

zero-trust Internet: a default-deny approach to security that assumes everything on the Internet is a potential threat.

Discover how Internet isolation revolutionizes security to eliminate the risk of phishing attacks and malware-infected endpoints for a secure cloud transformation.

Organizations can't afford anything less than 100 percent protection against phishing attacks and web-based threats. Yet, that's exactly what the security industry has delivered—until now. Learn about a new approach to security that doesn't involve resource-intensive detection and response. Internet isolation transforms security to provide complete protection where other technologies fail.

- Understanding the security industry's failure to stop threats—learn how organizations are giving up more ground to cyberattackers
- Learning how the Internet has changed—examine the impact of our growing dependence on cloud and web-based apps
- Introducing a new paradigm—explore how Internet isolation transforms security to provide complete threat protection
- Reimagining cloud access—understand Internet isolation's role in a secure cloud transformation
- Evaluating platforms—know what to look for when choosing Internet isolation technology

About the Author

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-90-4