A CyberEdge Group White Paper

Sponsored by Websense

September 2013

NAVIGATING THE LANDSCAPE FOR NETWORK DEFENSES ... AND KEEPING UP WITH MODERN THREATS

CYBEREDGE GROUP

INTRODUCTION

When it comes to effectively defending their networks, today's enterprises hardly stand a chance. If it's not spam, spear-phishing and worms, then it's drive-by downloads, advanced malware, denial-of-service (DoS) and targeted attacks. Indeed, it seems like every year brings with it one or more new classes of threats.

As the effectiveness of an organization's existing defenses wanes in the face of new threats, the typical reaction is to invest in additional countermeasures. Deciding what to invest in, however, is far from straightforward. In addition to a never-ending stream of new technologies and products to choose from, there is also the difficulty of deciphering how each option works and the degree to which it overlaps with what you already have in place.

And what about the pressure to reduce the complexity and cost of security infrastructure, for example, through consolidation of existing solutions? Once again, there needs to be a clear understanding of precisely what each component of the defense grid does and how they all fit together. That way consolidation can be achieved without compromising effectiveness.

This paper helps address these challenges by providing a taxonomy for evaluating security defenses and better understanding the roles they fulfill based on several defining characteristics, such as the underlying detection mechanisms and technologies they incorporate and the specific stages of the threat lifecycle they each target. The focus is on network perimeter defenses, which – contrary to what some pundits would have you believe – are not going way. The focus is also on threat detection, instead of broad-spectrum preventive technologies such as user authentication and encryption.

This paper can help enterprises answer questions such as:

- How do different perimeter defenses work, and how are they complementary to (or redundant with) each other?
- Which solutions (or components of solutions) does it make the most sense to invest in next to further shore up your defenses?
- What opportunities are available for simplifying and consolidating your perimeter defenses, and which of these should be avoided due to the increased exposure that will result?

WHY BOTHER – ISN'T THE PERIMETER DISSOLVING?

Contrary to what the proponents of "de-perimeterization" seem to be suggesting, the need for network perimeter defenses is in no way diminishing. In fact, a case can be made that the exact opposite is true.

A first point to realize is that the popularized version of de-perimeterization mischaracterizes the actual situation. There is no doubt that user mobility, wireless technologies, cloud solutions and dedicated connections to third parties have degraded the distinction between "internal" and "external" – and, in doing so, have also undermined the strategy of relying on a handful of well-defined and defended points of ingress/egress to a corporate network. But this doesn't mean that these locations in the network should go undefended. Such chokepoints still provide a high-efficiency opportunity to keep a majority of the bad things from ever entering the corporate network in the first place.

What it does mean, however, is that these external boundaries need to be supplemented with internal ones – for example, at high-volume chokepoints deeper in the network and in front of significant aggregations of resources. Specific locations to consider in this regard include significant intersections in your network backbone, the entry/exit point for the corporate data center, and the demarcation point for any high-profile workgroups (e.g., finance, legal, and research and development). In other words, the need for network perimeter defenses is actually expanding.

A second observation is that getting caught up in this notion of de-perimeterization has almost certainly contributed to the situation many enterprises find themselves in today. In particular, while it's certainly appropriate to invest in better security for applications and endpoints, it's clear that many organizations have shifted spending away from perimeter defenses a bit too aggressively. This is supported by the fact that, when it comes to the network perimeter, they have made minimal investments over the years. Instead, they continue to rely almost exclusively on traditional defense technologies, such as stateful inspection firewalls, gateway anti-virus, and legacy intrusion detection/prevention technologies.

The critical point here is that the network defenses for most organizations have not kept pace as threats have evolved. Notable deficiencies, particularly in light of today's advanced threats, include:

- relying too heavily on mechanisms, such as signatures and reputation analysis, that primarily defend against known threats;
- having limited ability to perform the real-time classification and analysis needed to defend against dynamic and zero-day threats; and
- not paying sufficient attention to return-direction traffic.

The bottom line is not only that network perimeter defenses remain an essential component of a defense-in-depth security strategy, but also that, for many organizations, this is an area that deserves renewed attention and investment.

GETTING STARTED

The trick is figuring out which of the countless potential investments available to your organization make the most sense. The high level answer is whichever ones provide the biggest "bang for your buck" – or greatest boost in effectiveness *in your environment* for the total investment required. The emphasis here highlights the fact that the answer will not be the same for every organization; after all, it depends on factors as diverse as the nature of your business, your organization's overall tolerance for risk, the particulars of your network, and what defenses have already been deployed.

To arrive at a more specific answer, IT Security decision makers should also evaluate several other dimensions of the problem and any solutions intended to address it. For example, two considerations to start with are the types (or classes) of threats that require attention and the communication vectors they typically employ.

Relevant classes of threats include: social engineering, eavesdropping (aka sniffing), malware (e.g., viruses, worms, and trojans), DoS attacks, intrusions, man-in-the-middle attacks, and internal threats.

Potential vectors or communications channels over which these threats might operate include: web, email, dedicated network connections for partners and service providers, portable media, mobile devices such as smartphones and tablets, and shared storage.

The point of reviewing these dimensions is not complicated. It's simply about ensuring there's coverage for all the areas that require it. If one technology only protects against malware, then others are needed to cover the other classes of threats. Similarly, if one solution only covers web communications, then other investments are needed to account for each of the remaining vectors that are applicable for a given organization.

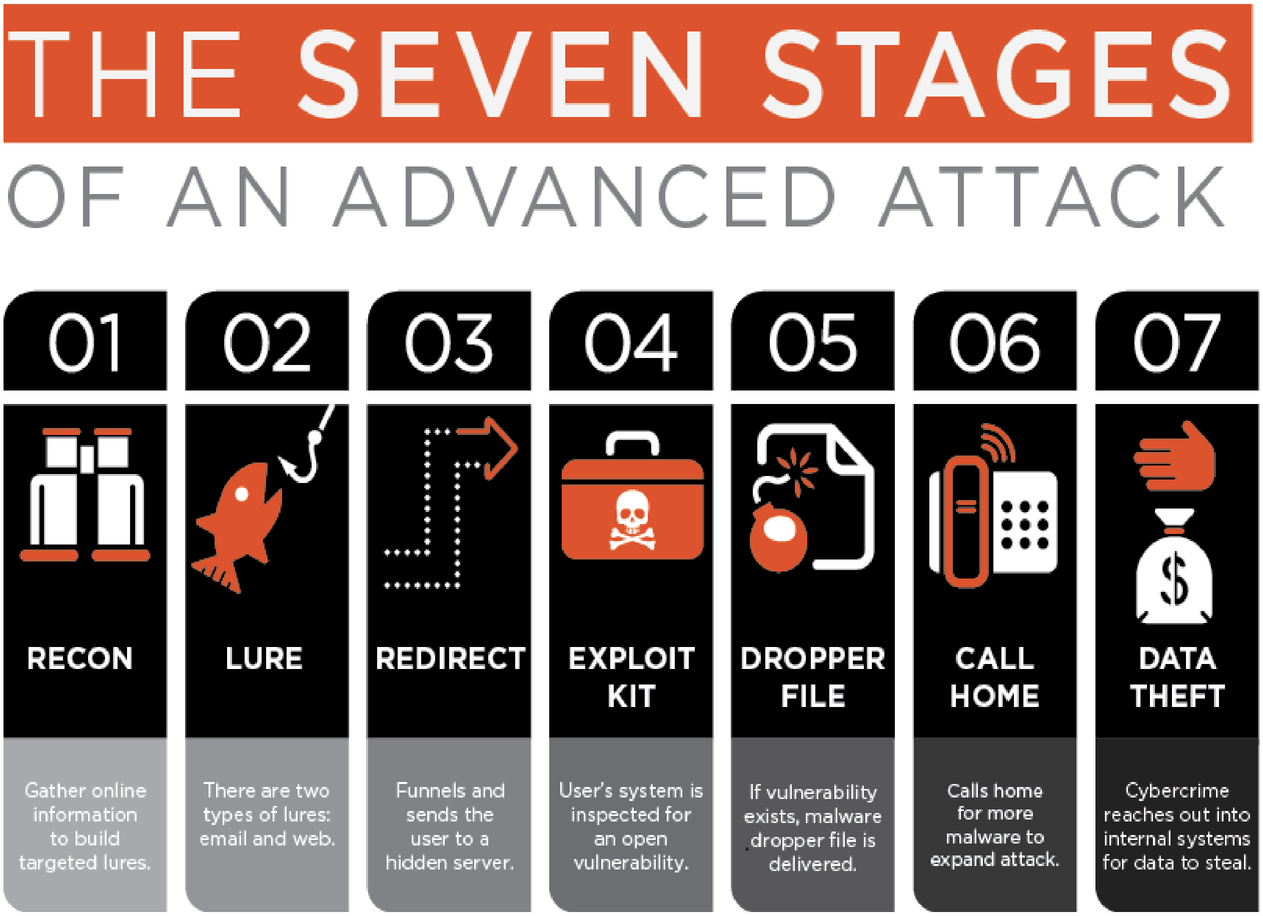
Other dimensions of existing and prospective defenses that also demand close attention are covered in the following sections. These include:

- the stages of the threat lifecycle that are addressed;
- the specific detection/protection mechanisms that are employed;
- the essential technologies each defense incorporates;
- how these technologies are packaged/bundled into solutions;
- deployment options and locations that are supported; and
- alternate prevention and mitigation solutions the organization may be using.

THREAT STAGES – UNDERSTANDING THE KILL CHAIN

Modern threats – in particular the advanced malware and targeted attacks that are causing today's organizations so much trouble – are characterized by a series of steps through which they progress to initially gain access to a network, spread within it, and eventually liberate data. For better or worse, this has become known as the "kill chain."

A generic, four-step version of this threat lifecycle is: infiltration, infection, propagation, and exfiltration. However, an updated alternative that better accounts for some of the underlying nuances associated with advanced threats is depicted in Figure 1, courtesy of Websense, Inc.



Gather online information to build targeted lures.

There are two types of lures: email and web.

Funnels and sends the user to a hidden server.

User's system is inspected for an open vulnerability.

If vulnerability exists, malware dropper file is delivered.

Calls home for more malware to expand attack.

Cybercrime reaches out into internal systems for data to steal.

Figure 1 – Websense Seven Stage Threat Model

For a comprehensive treatment of each of the stages shown here, readers are referred to the resources listed at the conclusion of this paper.[1] Without getting into all the related details, some key points to take away with regard to this dimension of the perimeter defense problem are as follows:

- In general, effectiveness of an organization's defenses can be enhanced by establishing coverage across the entire kill chain.
- Security technologies, and consequently enterprise investments, have historically focused primarily on stage 5 – and to some extent on stage 1, if you credit firewalls for being able to thwart certain types of reconnaissance efforts.2 This suggests concentrating future investments on the ends of the lifecycle. Candidate technologies that offer a good fit in this regard include comprehensive packet capture with associated traffic analysis (stages 1 and 6), spear-phishing protection (stage 2), real-time content and security analysis (stages 3 and 4), outbound traffic monitoring/analysis (stage 6) and gateway data loss prevention (DLP) (stage 7).
- Although they are not classified as proactive, tools that operate in the final two stages are nonetheless crucial to success. In fact it might soon be time to redefine what "proactive" means in the context of information security. After all, at the end of the day, what matters most is preventing the exfiltration of data.

UNDERLYING DEFENSE MECHANISMS

Turning more to the solution side of the equation, it is essential that IT Security decision makers also have a firm grasp of the underlying technical mechanisms at work within any given threat defense. All mechanisms have their strengths and, conversely, weaknesses. And some mechanisms are better at counteracting certain types or categories of threats than others. Maximizing effectiveness depends on establishing a perimeter security infrastructure with representation across the entire spectrum of defense mechanisms.

Rules. With rules, the flow of network traffic is controlled based on matching a predefined combination of attributes, such as the source and destination IP addresses, TCP/IP port, and protocol associated with the individual packets. Unlike with the other mechanisms discussed below, the protection this provides is indirect. Rather than attempting to identify actual threats, a blanket approach is taken that reduces an organization's attack surface by minimizing – but not eliminating – the potential paths by which threats can enter a network.

Signatures. Conventional threat detection signatures work by matching a bit pattern found in a traffic stream to the bit pattern of an exploit. The obvious limitation is that this mechanism only works for known threats. So-called vulnerability-based signatures operate by detecting triggering actions required to take advantage of known vulnerabilities – and, as a result, have the potential to also thwart unknown threats. Strictly speaking, though, the underlying mechanism in this case is more of a heuristic than an ordinary signature.

Heuristics. Sometimes referred to as a heuristic signature, this mechanism works by identifying a specific pattern or loosely coupled collection of events (rather than bits) in relative proximity to one another. Another way to think about it is that a heuristic is basically a predefined correlation – for example, if A, B, and C occur in sequence, then that is indicative of a threat. Although the core mechanism is best suited to identifying minor/predictable perturbations of known threats, more advanced implementations that employ additional algorithms and analytics can extend coverage further into the realm of the unknown.

Reputation. With a reputation-based mechanism, trust, validation and track record data are weighed to help reach a decision of whether or not to block an information source, sender, or file. Overall, the approach of using past behavior as an indicator of present behavior is fairly reliable, at least when it comes to stopping known, consistently bad actors. However, it breaks down when historically reputable sites and senders are compromised and become intermediate sources of threats.

Anomaly/behavior. This type of mechanism works by identifying significant deviations from specifications (e.g., for protocols) or baselines (e.g., for types and amounts of traffic). It can definitely pick out unauthorized activity on a network, but requires increasingly diligent tuning or a high tolerance for false positives to compensate for today's highly dynamic computing environments. Credentialed and well-obfuscated attacks can also be problematic.

Correlation. This mechanism involves using analytics, visualization techniques, and highly knowledgeable operators to uncover previously unknown relationships between events typically gathered from disparate resources that are eventually revealed to be indicative of a threat. A resource-intensive approach, correlation is best suited to detecting complex, multi-stage threats, and is not really appropriate for simpler, known threats.

Composite scoring. Essentially an extension of basic heuristics, composite scoring uses intelligent weighting of a collection of events or observed characteristics to come to a conclusion about the presence of a threat. For example, by itself the presence of JavaScript on a website probably doesn't mean much. However, when considered in combination with other factors – such as the use of a potential obfuscation technique, reputation of the website, URL classification, and anti-malware scanning results – it might be appropriate to conclude that malware has been injected into the site.

Additional points to consider when it comes to underlying technical mechanisms include the following:

- The adjunct ability to inspect SSL-encrypted traffic is becoming crucial. Without the ability to decrypt and subsequently re-encrypt such traffic, many of the aforementioned mechanisms will be rendered useless for a substantial portion of most organization's network traffic. According to the NSS Labs SSL report from June 2013, 25 to 35 percent of enterprise traffic is currently SSL, and it is expected that this will grow by an average of 20 percent annually.
- Discounting mechanisms such as signatures and reputation may in fact be warranted, but eliminating them altogether from your network defense portfolio is not. Although such mechanisms are poorly equipped to address the new breed of highly dynamic, previously unknown threats, they remain the most efficient and effective way for dealing with the vast collection of known ones.
- As the once clear delineation between "good" and "bad" continues to fade for many aspects of IT – for example, as is the case with social networking applications that can be used for many different purposes – assessing the context around individual events becomes increasingly important to achieving high detection accuracy. Accordingly, contextual analysis, which is not an underlying mechanism per se, should be sought out as a key capability. This in turn suggests concentrating new/additional investments on products involving correlation and composite scoring mechanisms – assuming, that is, that they include significant context/contextual analysis components to feed into the correlation and scoring engines.

A COCKTAIL OF ESSENTIAL TECHNOLOGIES

One step up from the underlying detection and prevention mechanisms are the technologies that employ them. This area can be a source of much confusion, particularly given the constant proliferation of new security technologies. Although this sort of innovation is absolutely necessary to keep pace with the changing nature of threats, it nonetheless makes it difficult to stay on top of which technologies do what, the limitations they each have, and how they can best be puzzled together to establish an effective perimeter security infrastructure.

The objective with the following three sections is twofold: (1) to alleviate confusion by providing a brief synopsis of several key technologies, and (2) in doing so, to convey the recipe for a "cocktail" of essential perimeter-oriented security technologies. The covered technologies are organized into three categories not only to highlight their emergence over time, but also to better focus attention on the more recent additions to the defense landscape – where the need for new/additional investments is greatest.

CC

THE CLASSIC CORE

This core group of network security technologies has already been present in most enterprises for quite some time. And although they are incapable of providing much protection against the latest breed of dynamic and zero-day threats, this shouldn't be interpreted as diminishing the role they play. For most environments, these core technologies continue to carry the bulk of the defensive load – at least in terms of the percentage of the total volume of threats typically encountered.

Stateful inspection firewalling. Initially introduced in 1994, stateful inspection firewalling is a refinement to basic rule-based access control that operates by maintaining awareness (i.e., the state) of allowed connections. Once a connection is evaluated against the firewall's rule set, all subsequent inbound and outbound packets from that connection are allowed to pass with no/minimal inspection. Although advantageous from a performance perspective, this approach is susceptible to threats that exploit return-path communication streams. Insufficient granularity of the governing rules can also be an issue and is the reason modern implementations have steadily extended the set of attributes that can be filtered on – for example, by incorporating greater degrees of application, user, and device awareness.

Gateway anti-virus (AV). Historically dependent on signatures, most network-based anti-virus implementations have been adapted over time to also incorporate a smattering of heuristics. Nonetheless, the focus – and primary benefit – is still on detecting/blocking known viruses and other forms of malicious code found in files traversing the network via common protocols, before they're able to reach an organization's endpoints. This is a particularly important defense for endpoints without host-level AV/protection (e.g., employee-owned mobile devices and networked medical or process control equipment), and is otherwise considered a best practice from the perspective of establishing defense in depth.

Intrusion detection and prevention. While gateway AV focuses on files, network intrusion detection and prevention systems directly monitor the network traffic stream itself for signs of malicious activity. Mechanisms typically used to accomplish this include signatures, protocol and statistical anomaly, and heuristics (in the form of vulnerability-oriented signatures). Modern implementations seek to overcome the deficiencies characteristic of these mechanisms and to also minimize false positives by adding increasing amounts of contextual awareness, such as knowledge about users, vulnerabilities, and the specific devices/systems being protected.

URL classification/filtering. Essentially a rule-based technology, URL filtering leverages an extensive database of URLs that are categorized based on periodic evaluation via a combination of automated and manual techniques. The security benefit is derived by setting policies to minimize the exposure of users to websites that are deemed undesirable, unsafe, or simply unnecessary to the performance of their jobs. Besides the impossibility of classifying the entire web, another limitation of this technology is the inability to keep up with rapidly changing conditions and the growing tendency of modern threats to also involve the compromise of otherwise reputable sites.

Reputation-based filtering. Implementations are commonly available for web/URL, email/senders, and files and utilize the basic reputation mechanism discussed previously. Effectiveness varies, often in relation to both the number of parameters that are evaluated to score an entity's reputation and the size of the network from which track-record intelligence is gathered. Because the output is typically a score versus a definitive indication of threat/no threat, these technologies are often most useful in a complementary role – for example, to help identify blended threats, or to eliminate low-hanging fruit in the case of anti-spam solutions.

SECOND GENERATION TECHNOLOGIES

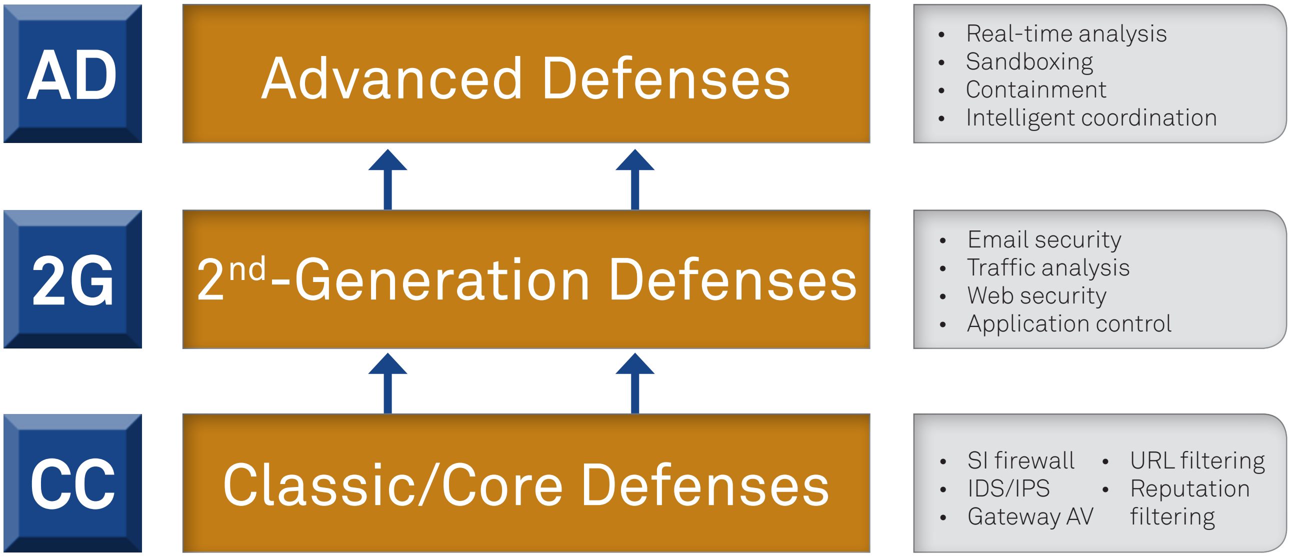
These second/next generation (2G/NG) technologies also have relatively high penetration, but are not nearly as pervasive as the classic core. In general, they fill some of the gaps left by the core technologies – for example, by providing comprehensive coverage for key communication vectors and introducing new/different implementations of underlying detection mechanisms. Another distinguishing characteristic is their ability to provide incrementally greater protection against unknown threats.

Email security. Actually a collection of technologies, email security combines multiple countermeasures to provide protection from a broad spectrum of email-borne or email-facilitated threats, including spam, malware, spear-phishing, and data leakage. Underlying mechanisms center on signatures, reputation, and heuristics.

Web security. Analogous to the previous item, web security delivers a cocktail of multiple countermeasures all focused on the web channel of communications. Typical implementations combine web-centric AV and URL and reputation filtering with several more advanced capabilities, such as social media controls, proxy-enabled SSL inspection, and web DLP.

Network traffic analysis. This technology involves capturing and analyzing network traffic for patterns, anomalies, and other events that are potentially indicative of malicious activity. Related solutions often support DoS detection/prevention and identifying unknown threats that are relatively "noisy" in terms of the network traffic they generate. Although reactive in nature, out-of-band variations can typically leverage data from both dedicated and standard traffic capture infrastructure (e.g., NetFlow sources), and also benefit from advanced analytics and data-mining techniques.

Application classification and control. App whitelisting and control are basically extensions of URL filtering and stateful inspection firewalling, respectively. As with the original technologies, they're primarily intended to limit exposure to/from unnecessary or unsafe Internet-based resources. The difference in this case is substantially increased granularity enabled by in-depth application awareness and the ability to discern how popular protocols, such as HTTP, are being used in any given instance.


AD Advanced Defenses

- Real-time analysis
- Sandboxing
- Containment
- Intelligent coordination

2G 2nd-Generation Defenses

- Email security
- Traffic analysis
- Web security
- Application control

CC Classic/Core Defenses

- SI firewall
- IDS/IPS
- Gateway AV
- URL filtering
- Reputation filtering

Figure 2: A Layered Model for Network Perimeter Defenses

AD ADVANCED DEFENSES

This final group of technologies represents the latest and greatest attempts to counteract the latest and not-so-greatest threats to emerge on the scene. For those organizations that have been steadily evolving their perimeter defenses over the years, these are the areas that require attention next. All others should consider filling remaining gaps from the lower tiers before proceeding to these more-advanced defenses.

Real-time analysis. This class of technology combines advanced heuristics and other proprietary algorithms to dynamically classify web content and inspect files, scripts, and traffic streams in real time for the presence of previously unknown threats. It is typically used to enhance traditional web and email security solutions, and is becoming increasingly imperative given the dynamic nature of today's web content, the relative ease of injecting malcode into websites, and the proliferation of customized and targeted malware. Because related solutions are operated in-line, they are also dependent on a high-performance architecture.

Sandboxing. With this technology, an out-of-band virtual execution environment is used to open unknown files, trigger embedded code, and watch for a litany of catalogued "bad behaviors." Although this approach is extremely useful for detecting never-before-seen threats, implementations ideally need to utilize more than just ordinary signatures and heuristics. IT Security teams should also evaluate related solutions for both the breadth of file types supported and the presence of refinements that compensate for virtualization-aware malware (i.e., malware that will remain dormant when it determines it is running in a virtual environment).

Containment. The technologies in this category are focused on detecting attempts made by entrenched threats to "call home" or exfiltrate sensitive data. In the first case, the technology is essentially a specialized version of network traffic analysis that looks specifically for command and control communications, suspicious DNS traffic, and other telltale characteristics. In the second case, it's gateway-based DLP. Leading implementations go well beyond basic fingerprinting techniques to also include advanced mechanisms designed to account for the various exfiltration tricks and techniques employed by modern malware – such as detection of password files, drip/slow leaks, use of proprietary encryption protocols, and image-based data.

Intelligent coordination. Modern threat actors are not confined to a single communications vector and are forever finding innovative ways to avoid commonly deployed defenses. For example, a particularly crafty spear-phishing tactic capitalizes on timing:

1. an email with an embedded URL is sent during non-working hours;
2. instead of compromising the associated website in advance, this part of the attack is delayed until just before the start of the next work day;
3. as a result, the organization's content security gateways find no issues with the email and its embedded web links at the time of receipt;
4. but, when the target eventually clicks on the link, the associated page is now hosting malware.

This points to the need not only for real-time analysis capabilities, but also intelligent coordination among different technologies – in this case, various elements of email and web security. What enterprises should look for in this area is a layer of management technology that bridges multiple, domain-specific technologies with advanced algorithms and mechanisms that deliver cross-technology analysis and response.

COMBINING DEFENSES FOR MAXIMUM EFFECTIVENESS AND EFFICIENCY

At the end of the day, enterprises don't buy individual mechanisms and technologies; rather they purchase solutions that are aggregations of these former elements. Unless key decision makers understand the underlying mechanisms and technologies, though, it's often difficult to distinguish one solution from the next. This can lead to unfortunate choices that result in poor overall effectiveness, such as:

- trying to defend one's network solely with next-generation firewalls, which, while highly capable, are not sufficient protection against modern malware; or,
- purchasing a collection of solutions that overlap excessively or still leave several areas undefended.

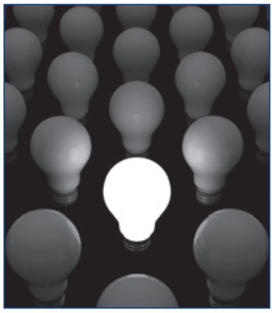
To this end, the following table shows one example of how the various dimensions of the network perimeter security problem can be used to map out both existing and candidate solutions. The result is a better understanding of how different solutions fit together and where critical gaps might remain in an organization's perimeter defenses.

This table further reveals that there are two centers of gravity that deserve close attention when it comes to network perimeter defenses, namely next-generation firewalls and unified content security solutions. And although the third category of product covered here seems destined for consolidation, given the magnitude and complexity of the problem it's addressing, the possibility of advanced malware defenses eventually coalescing into its own center of gravity should not be counted out. Either way, however, it is an area that definitely requires attention from today's enterprises.

Tier	Technology	Product/Solution			Primary Mechanism	Stages
		NGFW	UCS	AMD		
CC	SI Firewall	✓			rules	1*
CC	IDS/IPS	✓			signatures	4,5
2G	Traffic analysis	✓			anomaly	1,6,7
2G	Application control	✓			rules	1,2,3
CC	Gateway AV	✓	✓		signatures	4,5
CC	URL filtering	✓	✓		rules, reputation	1,2,3
CC	Reputation filtering		✓		reputation	4,5
2G	Email security		✓		signatures. reputation, heuristics	most
2G	Web security		✓		signatures, reputation, heuristics	most
AD	Real-time analysis		✓		heuristics	4,5
AD	Gateway DLP		✓		signatures, rules	1,7
AD	Call-home	✓	✓	✓	anomaly	6
AD	Sandboxing			✓	anomaly/behavior	5
AD	Intelligent coordination		✓		correlation, composite scoring	2,3,4,5

Notes:
NGFW = next-generation firewall
UCS = Unified content security
AMD = advanced malware defenses
* refer to Footnote 2 below

ADDITIONAL CONSIDERATIONS



Additional dimensions to evaluate when architecting one's network perimeter defenses include each solution's deployment options and locations, and the presence of other compensating techniques and controls that may offset the need or urgency for making certain investments.

Deployment options and locations. Besides having full functional coverage in terms of mechanisms and technologies, it's also necessary to have comprehensive physical coverage. This involves having appropriate form factors (e.g., software, hardware, and virtual appliances) and sizes (e.g., in terms of feeds and speeds) for all potential perimeter deployment locations: internet gateway, network core, data center edge, branch offices, and the cloud. Depending on the location, network design, and type of countermeasures involved, it might be necessary to also consider different configuration options, such as in-line versus out-of-band. Finally, the direction in which a given solution provides protection is also of paramount importance. As demonstrated by the kill chain, the days of getting by inspecting traffic in only one direction are in the rearview mirror; but, unfortunately, not all of the tools and products out there have adjusted to this new reality.

Compensating controls. Do you really need the latest and greatest product featuring the latest and greatest technologies right now? Or can you wait until it's matured a bit – or better yet, until it's been bundled into one of your existing solutions? Do you really need to fill the one little gap remaining in your core defenses? Perhaps not. The point is that any decision to invest in or otherwise change your perimeter defenses should also account for other countermeasures that have been implemented – not all of which may be network-perimeter oriented. In particular, a combination of any of the following defenses common to most organizations may provide sufficient coverage to defer certain investments, especially those with marginal benefits:

- Comprehensive vulnerability and patch management practices (which deliver a broad-spectrum reduction to an organization's attack surface);
- A network architecture featuring a high-degree of segmentation/zoning (which enables the organization to only deploy advanced countermeasures where they're needed most); and,
- Extensive use of encryption technology for data in transit and at rest (which can help offset the need for certain containment technologies).

CONCLUSION

Today's enterprises still need to invest in network perimeter defenses. For some this need is born out of years of de-emphasizing perimeter security in favor of investments in other areas (e.g., endpoint and application security). For others it's based on recognizing that the real impact of de-perimeterization is that there are now more locations in the network that require protection, not fewer. And for still others it's an inherent consequence of the never-ending chore of trying to keep pace with modern threats.

Deciding which specific security solutions to invest in next, however, can be tricky. Not only is there a plethora of options from which to choose, but all too often it's unclear what capabilities each solution brings to the table and how these compare to the defenses you already have in place.

The key to success in this regard is having a thorough understanding of each of the many dimensions that characterize both the threats being encountered and the solutions being proposed to thwart them. Subsequently mapping available countermeasures against these dimensions – especially the stages of the threat lifecycle and underlying defense mechanisms and technologies that are applicable – should help not only to reveal which combinations of solutions make the most sense, but also where more attention is still needed.

Footnotes/Resources:

1. For further details on the threat/malware kill chain, please see the **Websense 2012 Threat Report** (at http://www.websense.com/content/websense-2012-threat-report-download.aspx) and **The 7 Stages of Advanced Threats and Data Theft** (at http://www.websense.com/content/7-stages-of-advanced-threats-and-data-theft.aspx).

2. The nature of reconnaissance has changed considerably in recent years. Traditionally this activity centered on "sniffing" an organization's traffic from within or intercepting useful tidbits of information (e.g., operating system flavors and version numbers) through both legitimate and illegitimate interactions with an organizations applications and systems. These days, however, a considerable amount of reconnaissance occurs beyond the corporate perimeter, for example, by leveraging social networking sites and services. To be clear, this modern-day approach to reconnaissance is beyond the scope of this paper. Therefore, all references made herein to capabilities that support stage 1 are referring solely to the ability to address traditional reconnaissance techniques.

About Websense

Websense, Inc. is a global leader in protecting organizations from the latest cyber attacks and data theft. Websense TRITON comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware using real-time defenses and advanced containment and sandboxing technologies. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON solutions.

About the Author

Mark Bouchard, CISSP, is a Co-Founder and the Vice President of Research at CyberEdge Group, an award-winning research and consulting firm serving the needs of high-tech organizations worldwide. Mark's areas of specialization include information security, compliance management, application delivery, and infrastructure optimization. A former META Group analyst, Mark has analyzed business and technology trends across a wide range of information security and networking topics for more than 15 years. During this time, he has assisted hundreds of organizations worldwide with both strategic and tactical initiatives, from the development of multi-year strategies and high-level architectures to the justification, selection, and operation of security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about ensuring the success of his clients.

CYBEREDGE GROUP

CyberEdge Group, LLC
1997 Annapolis Exhange Pkwy
Suite 300
Annapolis, MD 21401

800.327.8711
info@cyber-edge.com
www.cyber-edge.com

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of CyberEdge Group, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.