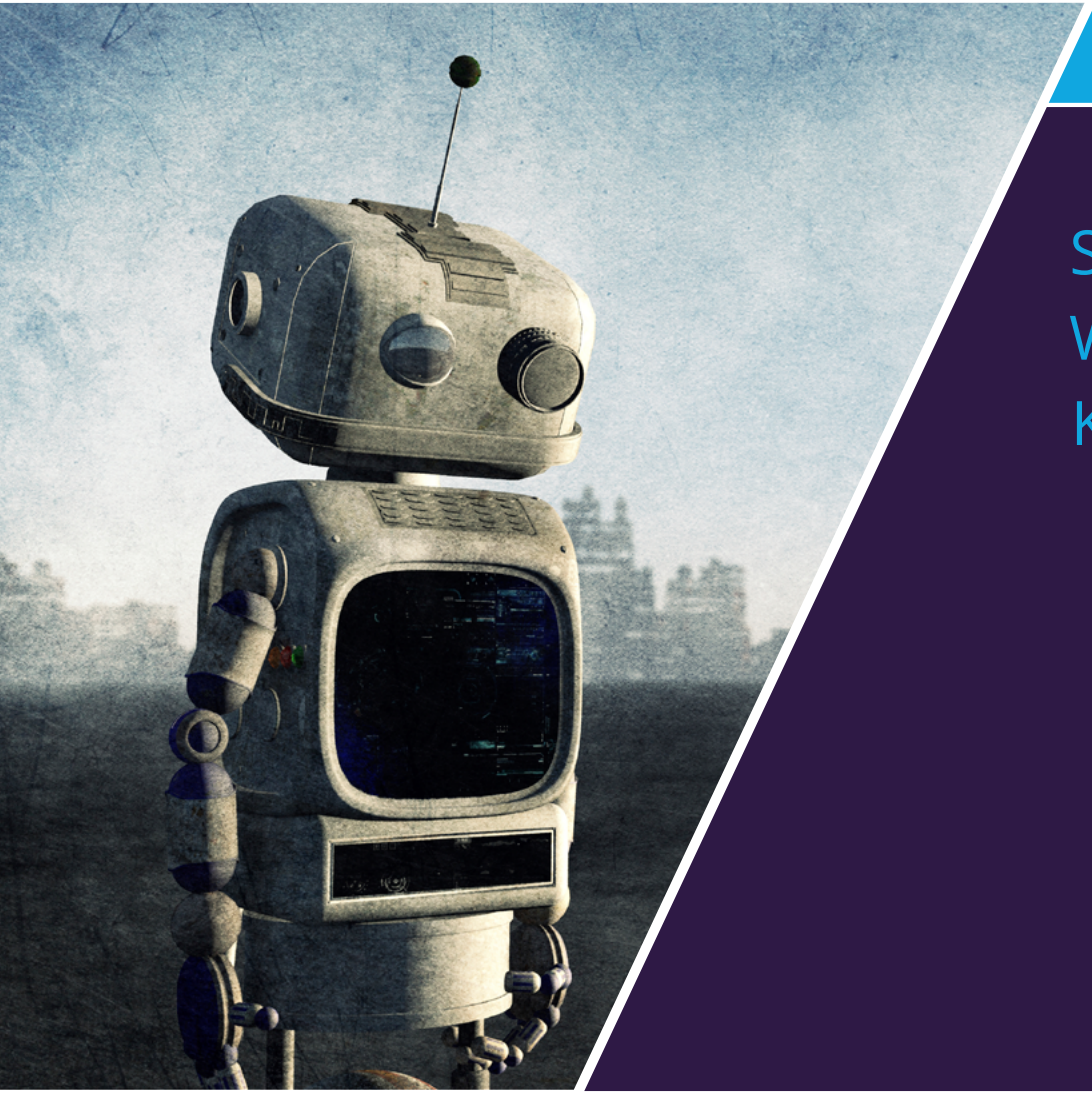
IMPERVA®



E-BOOK

Stop Bad Bots: What Security Experts Need to Know about Defeating Zombies

Content

Put Defeating Zombies on the Top of Your List

Imagine that your transactional website or a critical web application is attacked by a cybercriminal powered by an army of zombie devices, a botnet. For most companies—regardless of industry—such an attack could be extremely costly or even catastrophic. Yet many enterprises have little or no visibility, or control, over malicious web traffic aimed at distributed denial of service (DDoS) attacks, account takeover via credential stuffing, data theft, fraud, and more.

Many IT security teams are overburdened with efforts to protect corporate digital assets, confidential data, intellectual property, and networks. They're focused on endpoint and network security—as they should be. Unfortunately, that often means that websites and applications get less attention because of resource constraints. The result is checking the box and putting "good enough" security in place.

However, those measures are truly no longer good enough. Industry experts report that bad bots and botnets are increasing in frequency, sophistication, and duration. Endpoint, network, and other web defenses can't keep them from stopping your online business in its tracks.

Read on to get the facts about today's bot landscape and understand what enterprises need to do to protect critical web assets from attack.

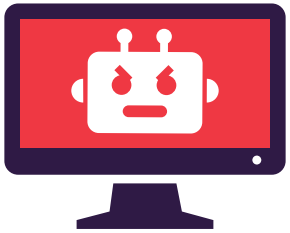
Bad Bots on the Rise

The use of bad bots by cybercriminals has continued to grow by roughly 30% each year between 2012 and 2015.

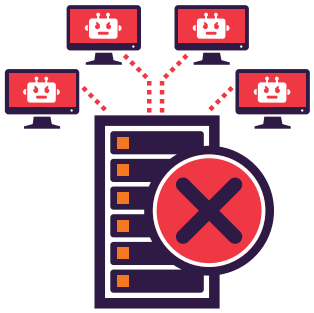
SOURCE: "GLOBAL BOT TRAFFIC REPORT 2015," IMPERVA INCAPSULA, 2016.

IMPERVA®

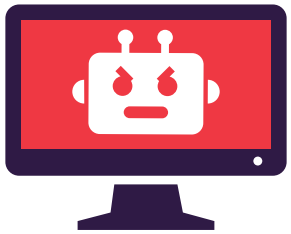
90+% of all security events tracked on the global Imperva Threat Intelligence network are the result of bad bot activity



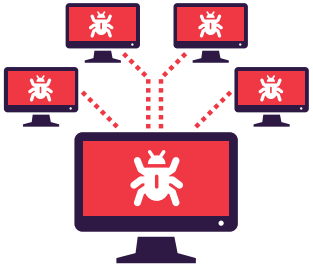
US$9 billion in losses to U.S. victims and over $110 billion in losses globally caused by botnets



200% increase in the number of DDoS attacks from 2014 to 2015



29% of all online traffic in 2015 originated from bad bots



500 million computers are infected globally each year

IMPERVA®

Welcome to Bots 101

Bot

A type of software application (in the case of good bots) or malware (malicious bots) that runs automated tasks over the Internet. Bots can automatically connect to command-and-control servers, which can instruct them to carry out activities, including illicit tasks.

Botnet

Also known as a zombie army, a botnet is a number of Internet-connected devices that, although their owners are unaware of it, have been set up (infected with malware) to take action as instructed by a threat actor using a command-and-control infrastructure. Building these networks of bots, or botnets, has become a lucrative business for botnet operators, who rent out their botnets at very affordable rates—DDoS attacks can be purchased on the hacker underground for as little as US$5 per hour.[1]

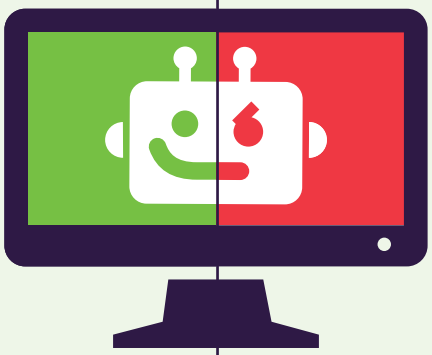
Good Bot Versus Bad

GOOD BOTS

Assisting in the evolution and growth of the Internet, good bots are owned by legitimate businesses that use them for automated tasks such as search engine indexing.

Examples include:

- Search-engine crawling bots:
  - Googlebot
  - Yahoo
  - MSN Bot/BingBot
- Website health monitoring
- Vulnerability scanning
- Fetching content
- Powering APIs



BAD BOTS

Bad bots are used by bad actors or anyone with a credit card looking to do harm to a target company.

There are many uses for bad bots, including:

- Automate spam campaigns, including comment spam and search engine optimization spam
- Launch DDoS attacks
- Test out stolen account credentials at volume (also known as credential stuffing)
- Spy on competitors
- Conduct site scraping
- Execute vulnerability scans to compromise websites

[1] "Underground Hacker Markets, Annual Report," Dell SecureWorks, April 2016.

Application DDoS attacks by the numbers

- **101 days:** The longest application DDoS attack
- **44.7%:** Targets that were attacked more than once
- **10.7%:** Targets attacked more than 10 times

SOURCE: GLOBAL DDOS THREAT LANDSCAPE Q4 2015, IMPERVA INCAPSULA, JANUARY 28, 2016.

Know the Risks

Any business with a web presence is at risk for bot-led attacks such as:

- DDoS attacks: DDoS attacks are bigger, smarter, and more dangerous than ever. Given today's threat landscape and the availability of inexpensive, do-it-yourself DDoS tools, businesses need to take DDoS threats seriously. These attacks can cripple a website in minutes, resulting in lost revenues, reputation damage, and reduced customer confidence. The average cost to a business attacked using DDoS is $40,000 per hour according to a survey of North American organizations conducted by Imperva.[2]
- Application DDoS attacks: Some DDoS attacks are targeted at overwhelming a web server, application server, or database resources instead of an organization's Internet connection. These threats (also known as application-layer DDoS attacks or Layer 7 DDoS attacks) are more sophisticated and much more challenging to stop than traditional DDoS attacks. Application DDoS attacks usually bypass most traditional network security devices because attack traffic often mimics regular traffic, is protocol compliant, and cannot be identified by network-layer anomalies (such as an extreme volume of traffic or connection requests).
- Credential stuffing and account takeover: According to the 2016 Verizon Data Breach Investigations Report, 63 percent) of confirmed data breaches in 2015 involved weak, default, or stolen credentials.[3] A bad actor can purchase a hacked U.S. social media account for $129 or a corporate email account for $500. Banking credentials can be purchased for as little as 1 percent of the account balance.[4] Account takeover attacks typically include the following elements: harvesting credentials, testing credentials using bot networks, gaining access, and stealing assets. Losses from related fraudulent activities tally in the billions of dollars per year and extend well beyond the retail and banking sectors.

[2] "DDoS Impact Survey Reveals the Actual Cost of DDoS Attacks," Imperva Incapsula, November 12, 2014.

[3] "2016 Data Breach Investigations Report," Verizon, April 2016.

[4] "Underground Hacker Markets, Annual Report," Dell SecureWorks.

Understand Your Security Gaps

Botnet strategies, technologies, and attack techniques are constantly evolving. While simpler bots may make little attempt to hide what they are, more sophisticated bots closely mimic human behavior. Typical security solutions can't detect the most sophisticated bots.

Here's why:

SECURITY SOLUTIONS	WHY THEY FAIL AGAINST BAD BOTS
Endpoint and network protection solutions	• Botnets use anonymizing systems (e.g. proxy servers and Tor relays) to hide their source IP address. Endpoint and network security solutions that only rely on blacklists cannot detect bots. • By posing as authorized users of target applications and services, bots can pass through perimeter and access control defenses. Endpoint and network security solutions do not have sufficient visibility into application-layer (Layer 7) traffic or context into which webpage is being targeted.
Obfuscation-based or polymorphic code solutions	• A solution that changes code for web pages on the fly, these products can only inspect headers and cookies, and are not focused on detection. • They can also wreak havoc on downstream and upstream application optimization and security solutions because the code changes with each request.
Application delivery controller (ADC) appliances	• A solution that changes code for web pages on the fly, these products can only inspect headers and cookies, and are not focused on detection. • They can also wreak havoc on downstream and upstream application optimization and security solutions because the code changes with each request.

Put the Right Defense in Place

There is a way to protect your website and applications from attacks by bad bots: deploy a sophisticated web application firewall (WAF) with a robust bot classification system and comprehensive, real-time threat intelligence.

WEB APPLICATION FIREWALL	THREAT INTELLIGENCE
• Analyzes all incoming traffic to your websites and applications • Distinguishes between human and bot traffic, good versus bad bots • Blocks newly discovered bad bots	• Collects global attack data, including: – Known malicious IP addresses • Known bad IP addresses • Anonymous proxies • Tor networks • Phishing sites/URLs – Known malicious bots • Crowd-sourced from Imperva Incapsula network – Remote file inclusion (RFI) attack syntax • Distributes intelligence feed to improve the accuracy of attack detection. Accuracy is further improved when a malicious IP address is also classified as a bot by the WAF.

With the right WAF solution, your organization gains a multilayer defense that uses both direct and indirect methods for preventing and mitigating bot damage:

- **Direct:** The direct method works by actually detecting and responding to bad bots using threat intelligence and bot classification for newly discovered bots.
- **Indirect:** Indirect protection mitigates or thwarts the actions of bots (e.g. account takeovers), without having to actually detect the bot itself. A combination of both delivers comprehensive protection of your enterprise's critical web assets.

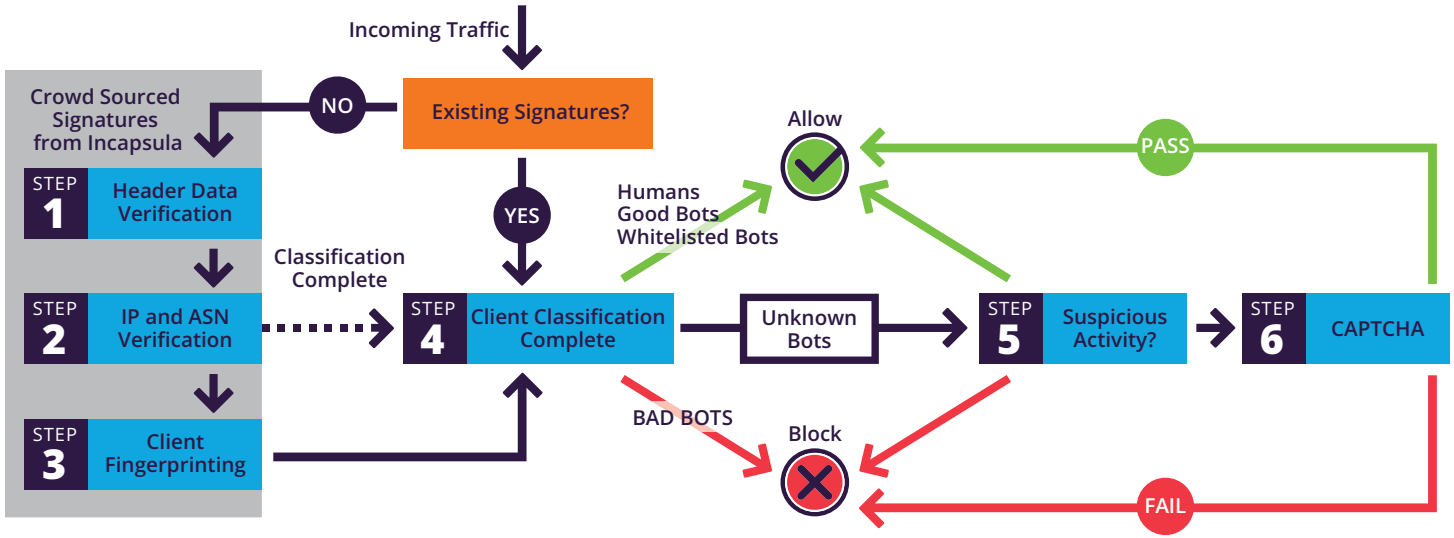
Bot Detection and Classification with Imperva

More organizations rely on Imperva to protect their critical web applications than any other vendor. Imperva web application security solutions fit seamlessly into physical, virtual, and cloud-based data centers. Imperva delivers the market's most advanced web application security, constantly updated with threat intelligence curated by the renowned Imperva Defense Center research team.

- Imperva SecureSphere Web Application Firewall: SecureSphere Web Application Firewall analyzes all user access to your business-critical web applications and protects your applications and data from cyberattacks including botnets, DDoS attacks, and account takeover attempts.
- Imperva ThreatRadar: ThreatRadar is the premier threat intelligence feed that arms the industry-leading SecureSphere Web Application Firewall. ThreatRadar is available with Bot Protection, which enables SecureSphere Web Application Firewall to accurately distinguish between human and bot traffic, identify good and bad bots, classify traffic by browser type, and more.

Here's how Imperva protects your web presence against bad bots:

Imperva Bot Classification Process



IMPERVA®

STEP 1

Header data verification

By inspecting hypertext transfer protocol (HTTP) headers, Imperva gains valuable insight into visitors, including various clues into whether each client is human or automated, and whether or not it is malicious. For every client connecting to the web application, Imperva checks the HTTP header data and order. The HTTP header is matched against a known set of bad signatures in the crowd-sourced threat intelligence feed from Imperva to determine if the client is malicious.

STEP 2

Internet protocol and autonomous system number verification

Imperva looks for the identity of the Internet protocol (IP) and autonomous system number (ASN) owners and whether they match the visitor's identity. This can be used to identify malicious bots posing as legitimate ones. For example, if a bot claims to be from a search engine such as Google, but neither the IP nor the ASN match that company, it's a sign that it's likely a dangerous impostor.

STEP 3

Client finger printing

To thwart attacks where bots use legitimate user agents and correct header data, if the client's identity is not matched in Steps 1 and 2, Imperva introduces a non-intrusive JavaScript and cookie challenge in the HTTP response that checks for client behavior. This step confirms that the client claiming to be a browser is in fact one and not a malicious bot masquerading as a browser.

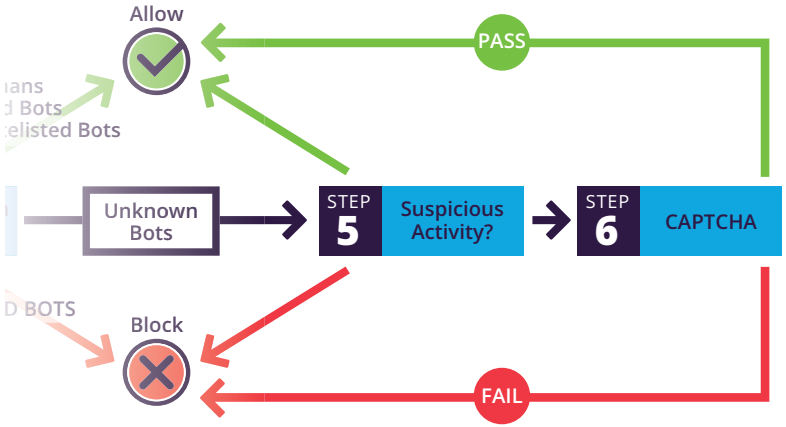
STEP 4

Classification completed

At this point, Imperva knows the client type—human or bot. If it's a bot, it also knows whether it's a good, bad, or unknown bot. If it's unknown, then Imperva proceeds to the next step: correlation.

Bot Classification and Response with Imperva

Once Imperva knows that the incoming traffic is a bot and whether it's good or bad, it can either allow it or block it. But what if the bot is unknown? Imperva then employs correlation and CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technologies to determine whether the traffic should be allowed or blocked.



STEP 5 Checking for Suspicious Bot Activity

Unknown bots without any known reputation are tracked within SecureSphere Web Application Firewall for abnormal or suspicious activity. SecureSphere Web Application Firewall uses intelligence and real-time monitoring data such as geo-location, IP reputation, anonymous proxies/TOR nodes, velocity checks, and others to determine legitimacy of an unknown bot.

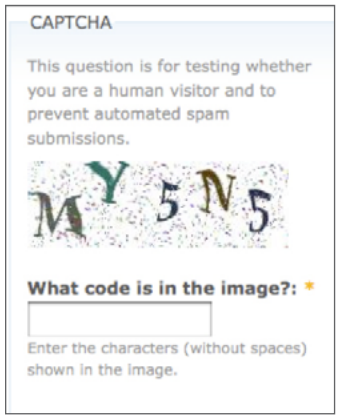
Imperva further boosts both the efficacy and accuracy by enabling detailed correlation between all available sources of information to establish a clearer picture. In addition to activating numerous pre-defined correlation policies, SecureSphere administrators can further minimize false positives by crafting their own custom policies to account for additional pieces of data–such as irregularities in how HTTP or extensible markup language (XML) services are being used. For example, if a bot is detected and it is attempting to perform an SQL-injection attack from behind an anonymous proxy, then a policy could be created that tells SecureSphere to alert administrators and block the traffic.

STEP 6

CAPTCHA

When suspicious or abnormal activity is detected, Imperva customers can also turn on CAPTCHA, instead of blocking the session/IP address outright and further improve the accuracy of Imperva Bot Protection.

SecureSphere Web Application Firewall is integrated with Google's free reCAPTCHA service.



Source: Gartner (July 2015)[5]

The Web Application Firewall Leader

Imperva is the only vendor ranked in the Leaders Quadrant for two years running for the Gartner Magic Quadrant for Web Application Firewalls.

[5] *Gartner "Magic Quadrant for Web Application Firewalls" by Jeremy D'Hoinne, Adam Hils, Greg Young, Nicole Papadopoulos, 15 June 2015.*

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Imperva. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

IMPERVA®

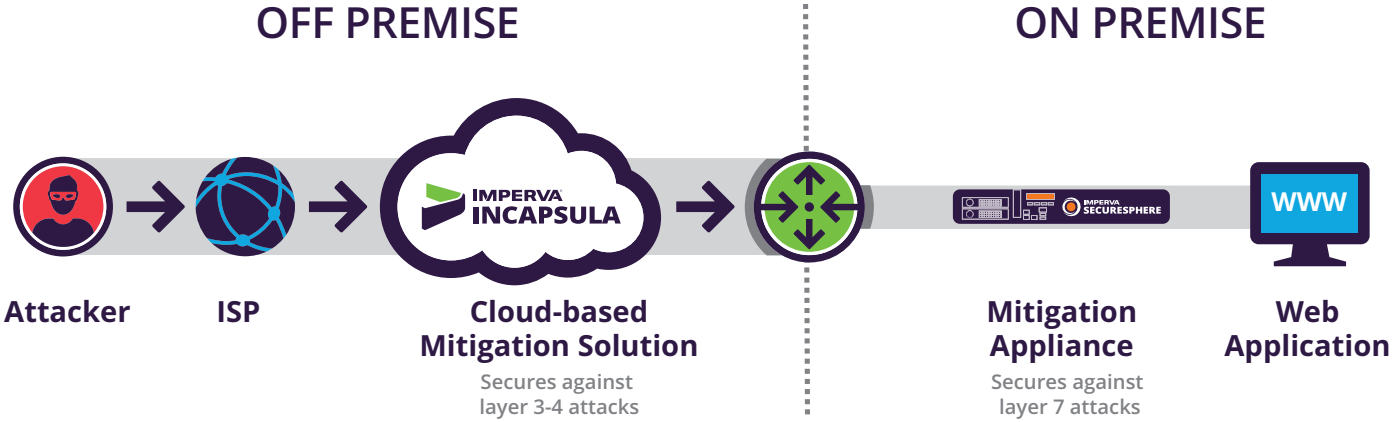
Bot Mitigation: Stopping DDos Attacks with Imperva

While Imperva provides direct protection against bad bots, it also delivers indirect protection to thwart the activities of bad bots, even when they remain undetected. This gives you a multilayered defense and the greatest protection against attacks on your enterprise's web presence–including DDoS and application DDoS threats.

Using a combination of on-premises SecureSphere Web Application Firewall and the cloud-based Imperva Incapsula DDoS protection service gives you a spectrum of coverage for both network and application layer-DDoS attacks.

Imperva Incapsula

Incapsula secures websites against the largest and smartest types of DDoS attacks–including network, protocol, and application-level (Layers 3, 4, and 7) attacks–with minimal business disruption. This cloud-based service keeps online businesses up and running at high performance levels even under attack, avoiding financial losses and serious reputation damage.



Bot Mitigation: Preventing Account Takeover with Imperva

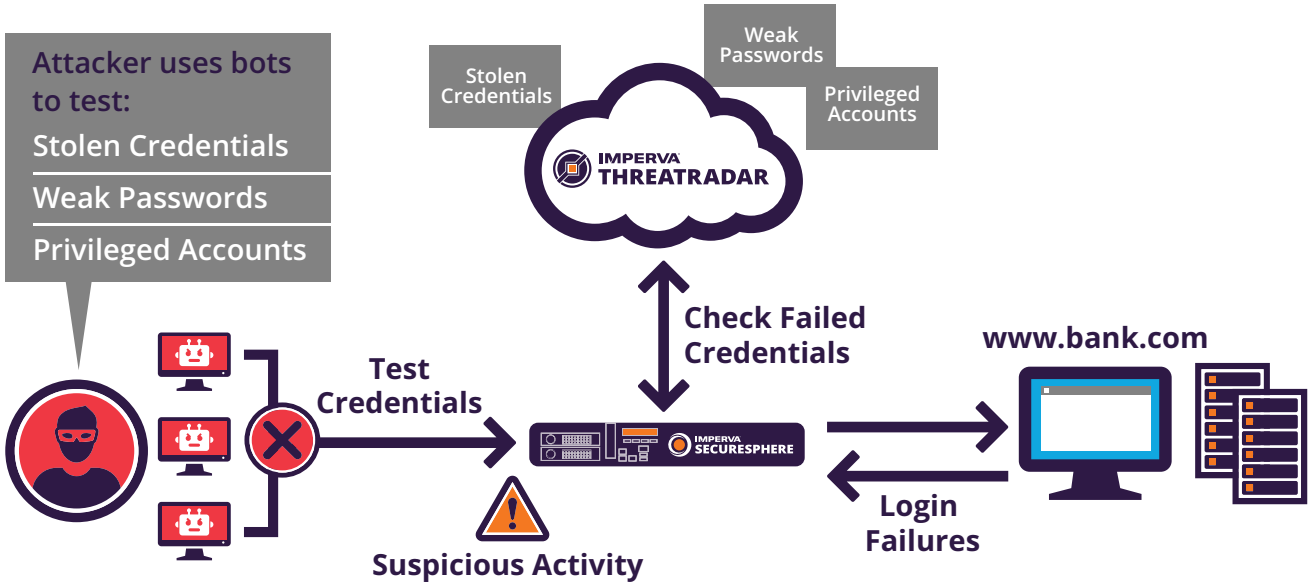
Further protecting your enterprise from the actions of undetected malicious bots, Imperva ThreatRadar can outsmart account takeover exploits with:

- Credential intelligence: Detects credential stuffing using stolen credentials and weak passwords
- Device intelligence: Detects risky devices based on device finger-printing and suspicious behavior

Here's how Imperva credential intelligence works:

- Repeated login failures trigger checks against Imperva's repositories of stolen credentials, weak passwords, and privileged account passwords.
- A successful match against one of these repositories confirms a credential stuffing attack.
- Configurable mitigation rules within SecureSphere can alert and automatically block such clients.

Detecting Account Takeover—Using Credential Intelligence

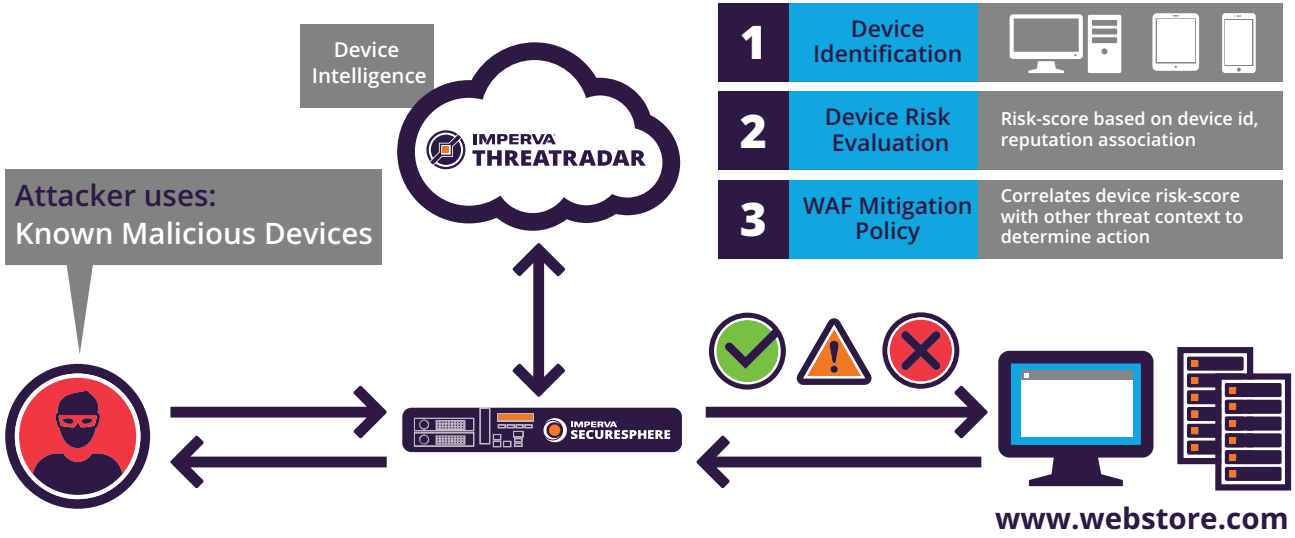


IMPERVA

Similarly, Imperva device intelligence helps detect and thwart account takeovers. Here's how:

- Device profiling: SecureSphere Web Application Firewall injects JavaScript into every device that attempts to log into the web application to identify whether it is a new or returning device.
- Device risk evaluation: During the login process, SecureSphere Web Application Firewall invokes ThreatRadar APIs to evaluate the risk score of the device. This score is based on the device reputation (e.g., whether it's jail-broken), use of evasion techniques, and known associations with multiple accounts.
- Mitigation rules: The device risk score is correlated with other feeds in SecureSphere Web Application Firewall to determine the mitigation action–audit, alert, or block–for a specific login attempt.

Detecting Account Takeover—Using Device Intelligence



Security for the Real World

One of the largest banks in Europe–with 2,000 branches and 30 million customers, 12 million of which are online customers–needed to reduce the risk of online banking for its customers and address online transaction fraud. The retail bank turned to Imperva for help.

Challenge:

The bank was seeing a significant increase in automated attacks such as bots, man-in-the-browser (MITB), DDoS, and phishing. Two areas of threat were particularly damaging:

- **Credential reconnaissance:** Bots were used to launch brute-force attacks targeted at customer accounts, with the goal of locking users out after several failed login attempts. Customers impacted by the attacks could lose faith in the bank's ability to protect their money and identity.
- **Credential stuffing:** The bank also experienced bot-driven attacks that used brute-force mechanisms to log into user accounts using stolen credentials and perform fraudulent transactions.

Both the security operations and fraud teams were overwhelmed with responding to alerts and manually reviewing and analyzing log records to investigate the attacks.

Solution:

With SecureSphere Web Application Firewall, ThreatRadar Bot Protection, and ThreatRadar Account Takeover Protection from Imperva, the bank can now block:

- Malicious bots launching brute-force attacks that target login pages using failed login thresholds and velocity techniques
- Account takeover attempts using stolen credentials

Results:

With the right defense in place, the bank:

- Reduced DDoS-caused downtime/outages
- Protected Internet-based revenue streams
- Maintained customer trust in the brand, website, and applications
- Protected confidential company and customer information

Additional Resources

Learn more about how to protect your organization against bad bots, DDoS threats, application-layer DDoS attacks, and account takeover attacks. Check out the following resources:

Five Ways Imperva Surpasses the Competition for Web Application Security

Top 5 Solution Requirements for Account Takeover Protection

DDoS Response Playbook

About Imperva

Imperva® (NYSE:IMPV) is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere, CounterBreach, Incapsula and Skyfence product lines enable organizations to discover assets and risks, protect information wherever it lives—in the cloud and on-premises—and comply with regulations. The Imperva Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the-minute threat intelligence, and publishes reports that provide insight and guidance on the latest threats and how to mitigate them. Imperva is headquartered in Redwood Shores, California.