Breaking the Cyber Attack Lifecycle

Palo Alto Networks: Reinventing Enterprise Operations and Defense

March 2015

Palo Alto Networks
4301 Great America Parkway
Santa Clara, CA 95054

www.paloaltonetworks.com

paloalto NETWORKS®

the enterprise security company™

Executive Summary

Cybercrime is big business. By many estimates, cybercrime is now a US$1 trillion dollar industry. Every organization with digital assets is vulnerable to attack and the growing sophistication of cyber criminals and their evolving tactics only increases the chance of a security breach involving the theft of sensitive data. Effective cyber defense must withstand changes to adversaries' tactics and tools that traditional, non-integrated "best of breed" approaches cannot address. It must also protect against advanced known threats, as well as unknown threats, which can be challenging to address with legacy solutions. The Enterprise Security Platform from Palo Alto Networks® is a modern approach to providing new defense and resilience in detecting and preventing attacks at every stage of the Cyber Attack Lifecycle.

Cyber Attacks on the Rise

From the highly-publicized data breach at Sony to the theft of personal financial data at JP Morgan Chase, these attacks expose a complete failure of cyber defense and prevention to companies of all sizes. In 2014, nearly half (43 percent) of U.S. companies surveyed in a study by the Ponemon Institute experienced a data breach involving the loss or theft of more than 1,000 records — up more than 10 percent from 2013 [1].

Criminals are executing sophisticated attacks on global organizations with alarming regularity to obtain confidential information, steal trade secrets or disrupt business operations. It's clear that businesses must do more to protect against these advanced cyber threats.

For the past decade, technology approaches to securing organizations have stood still, while adversaries continue to find clever new ways to bypass traditional defenses. Despite substantial investments made in securing their networks, many organizations find themselves vulnerable and unable to defend their organizations against cyber attacks.

U.S. COMPANIES VULNERABLE TO ATTACK

"There are two kinds of big companies in the United States. There are those who've been hacked and those who don't know they've been hacked."

— FBI Director James Comey
in the Washington Times,
Nov. 3, 2014

Legacy techniques are proving inadequate because they generally provide alerts on threats only and take a "detection-focused" approach, which requires manual intervention or costly Incident Response (IR) services once a breach occurs. But more importantly, these legacy solutions are made up of a "patchwork" of point products that not only lack the ability to protect against all threat vectors, but also make it very difficult to coordinate and share intelligence among the various devices. For example, if sandboxing hardware detects an unknown threat, it will not automatically share protections with Intrusion Prevention Systems (IPS) and endpoint agents, leaving the organization defenseless against multi-dimensional attacks. The "detection-focused" approach fails to enable IT and cybersecurity professionals to defend their enterprise.

Many experts believe the problem will only get worse. For example, widely-used older software such as Windows XP, which recently stopped receiving patches and security updates, leave a large proportion of users vulnerable to newly discovered exploits. In addition, Windows Server 2003 End of Support (EOS) in July 2015 may also leave businesses vulnerable to major security and compliance risks. And finally, businesses are increasingly adopting new technologies such as cloud, Bring Your Own Device (BYOD) and the Internet of Things (IoT), but these technologies also create new opportunities for attackers to breach connected devices and infiltrate enterprise organizations.

Businesses cannot afford to keep investing in fragmented, detection-focused devices in their efforts to keep pace with the rapidly evolving threat landscape.

[1] Ponemon Institute, "Is Your Company Ready for a Big Data Breach?" September 2014 http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

The Cyber Attack Lifecycle – How Cyber Criminals Operate

The Cyber Attack Lifecycle is a sequence of events that an attacker goes through to successfully infiltrate a network and exfiltrate data from it. The good news is that blocking just one stage in this lifecycle is all that is needed to protect a company's network and data from attack.

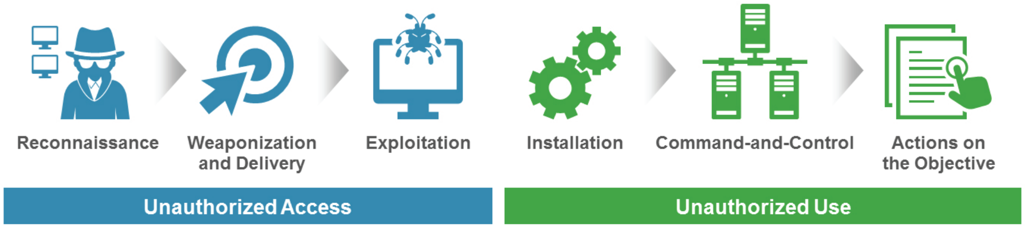


Figure 1: The Lockheed Martin Cyber Kill Chain® Model.

This Cyber Attack Lifecycle model illustrates how we view each stage in the lifecycle:

1. **Reconnaissance:** Just like burglars and thieves, attackers carefully plan their attacks. They research, identify, and select targets, oftentimes using phishing tactics or extracting public information from an employee's LinkedIn profile or corporate websites. These criminals also scan for network vulnerabilities and services or applications they can exploit.

2. **Weaponization & Delivery:** Next, the attackers determine which methods to use. They may choose to embed intruder code within seemingly innocuous files like a PDF or Word document or email message. Or, for highly-targeted attacks, attackers may craft deliverables to catch specific interests of an individual.

3. **Exploitation:** Once attackers gain access "inside" an organization, they can activate attack code on the victim's host and ultimately take control of the target machine.

4. **Installation:** Attackers will seek to establish privileged operations, root kit, escalate privileges, and establish persistence.

5. **Command-and-Control:** Attackers establish a command channel back through the Internet to a specific server so they can communicate and pass data back and forth between infected devices and their server.

6. **Actions on the Objective:** Attackers may have many different motivations for attack, and it's not always for profit. Their reasons could be data exfiltration, destruction of critical infrastructure, or to deface web property or create fear/extortion.

Innovative solutions like Palo Alto Networks Enterprise Security Platform work together in a coordinated manner to protect businesses at every stage of the Cyber Attack Lifecycle through detective and preventive controls.

Palo Alto Networks Enterprise Security Platform

To protect organizations from threats at every point in the Cyber Attack Lifecycle, the Palo Alto Networks Enterprise Security Platform offers a unique, preventive approach to secure computing environments, prevent known and unknown threats, and safely enable an increasingly complex and rapidly growing number of applications. The platform does this by proactively reducing the attack surface of the enterprise, and then fully inspecting all allowed traffic for threats. Reducing the attack surface allows businesses to prevent attackers from successfully exploiting vulnerabilities on endpoints.

Unlike legacy port-based security practices that provide limited protection across a handful of threat vectors, the Enterprise Security Platform protects every part of the global enterprise network, addressing vulnerabilities and malware arriving at the endpoint, mobile device, network perimeter and within the data center.

This powerful, multi-layered defense platform integrates next-generation firewalls, cloud-based threat intelligence and Traps advanced endpoint protection. The integration forms a closed-loop approach that is able to automate threat intelligence sharing across all security platform devices and endpoint agents, actively preventing new threats from gaining access into a controlled enterprise. For example, when the platform flags potentially suspicious payloads, the threat intelligence cloud creates signatures, which are sent back to all points of enforcement (firewall and endpoint agent) for immediate protection and prevention. This reduces complexity, false positives and risk, allowing IT operations and cyber defense professionals to protect enterprise users, applications, data and infrastructure.

Next-Generation Firewalls

The Palo Alto Networks family of next-generation firewalls is the core of the Enterprise Security Platform. It is designed to provide better native visibility, control and protection of all network traffic than any other vendor — including native ability to inspect all network traffic — no matter the port or protocol an application uses, including SSL encrypted traffic.

The next-generation firewalls offer many built-in security features, ranging from IPS and URL filtering, to anti-malware and App-ID™ (identify any application on any port) and User-ID™ (tie users and groups to security policies). These next-generation security appliances are able to stop the majority of attacks by proactively limiting the ways into an organization, reducing the attack surface to a small set of known, and controlled, applications.

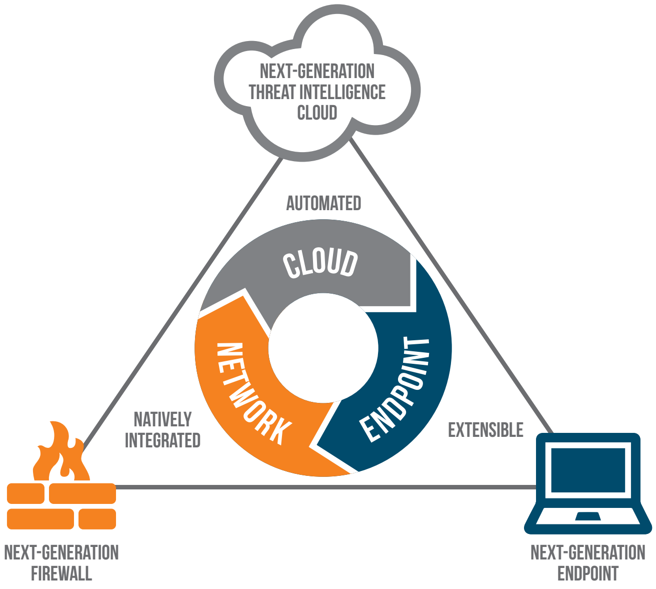


Figure 2: Enterprise Security Platform Integrates Network, Cloud and Endpoint Security

Global Threat Intelligence Cloud

With more than 6,100 WildFire™ global customers contributing threat intelligence, the threat intelligence cloud uses this research and quickly converts it into signatures so the entire global community can make decisions in real-time and stay one step ahead of cyber criminals. The cloud-based WildFire service detects and creates protections against advanced malware, including threats that have never been seen before, exploits, and outbound Command and Control (C2) activity, by observing their actual behavior rather than relying on pre-existing signatures.

Threat Prevention and PAN-DB/URL-Filtering features receive and implement these protections to prevent advanced threats. WildFire produces an average of 300 new anti-malware rules every 15 minutes and automatically shares this with its customers to ensure organizations are protected against the diverse and growing number of new global threats. In addition, protections for DNS/CnC and malicious URLs are automatically sent to customers in timely increments ranging from every 15 or 30 minutes eliminating the need for expensive, manual processes to stay on top of new threats.

Integrating WildFire with the Threat Prevention and URL Filtering services within Palo Alto Networks entire firewall family and endpoint agents provides a novel approach for reducing the attack surface and protecting enterprises.

Advanced Endpoint Protection

Instead of focusing on the millions of individual attacks themselves or reacting once an endpoint has been compromised, Palo Alto Networks Traps™ is designed to actively defeat attacks targeting endpoints, including unknown malware and zero-day exploits. Traps automatically detects and blocks all known malware techniques that every attacker must link together in order to execute any type of attack, regardless of its complexity. Throughout each event, Traps collects detailed forensics and reports this information to the Endpoint Security Manager (ESM), resulting in better visibility and confirmation of attacks that were prevented. With Traps, endpoints are always protected, regardless of patch, signature or software update levels, plus it doesn't require prior knowledge of an attack in order to prevent it.

REDUCE THREAT LANDSCAPE

"When [WildFire] finds something corrupted or a potential threat, it's quickly identified and all our systems are instantly protected. Our past security system inspected email attachments that passed through our centralized email exchange server. In many cases, threats were invisible to it and entered our networks.

WildFire solves this problem and gives us the same level of real-time inspection of traffic passing from the public to private network. Once we saw WildFire's effectiveness we expanded it to all devices and branches."

— Massimiliano Tesser, Group CIO, CAME Group

The Palo Alto Networks platform is aligned with Forrester's Zero Trust model of information security that advocates a "never trust, always verify" philosophy in protecting information resources. Palo Alto Networks provides visibility and control across all network traffic and ports, regardless of where an attacker uses them — at the network edge, in the data center or at the endpoint.

Detecting and Preventing Attacks at Every Stage of the Cyber Attack Lifecycle

Palo Alto Networks delivers a novel way to address the common types of attack at every stage of the Cyber Attack Lifecycle, regardless of where the initial attack occurs. The Enterprise Security Platform provides prevention capabilities at each stage to block the attackers' ability to access and move laterally within the enterprise. Below are some examples showing the use of Palo Alto Networks Enterprise Security Platform to detect and prevent threats at every stage of the Cyber Attack Lifecycle.

Reconnaissance

Just like burglars and thieves, cyber criminals carefully plan their attacks. They research, identify, and select targets, oftentimes using phishing tactics or extracting public information from an employee's LinkedIn profile, for example, or corporate websites. These attackers also scan networks for vulnerabilities, services, and applications they can exploit.

Stage 1: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Prevent use of social engineering and block known malicious URLs through URL filtering
- Continuous inspection of network traffic flows to detect and prevent port scans and host sweeps using Intrusion Prevention network security/threat prevention technology.

Weaponization and Delivery

Next, the attacker determines which methods to use. They may choose to embed intruder code within seemingly innocuous files like a PDF or Word document or email message. Or, for highly-targeted attacks, attackers may craft deliverables to catch specific interests of an individual.

Stage 2: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Full visibility into all traffic, including SSL, and block high-risk applications using next-generation firewall and GlobalProtect™ to extend those protections to remote and mobile devices.
- Protect against perimeter breaches by blocking malicious or risky websites such as hacking, phishing, malware, and more, using PAN-DB for URL filtering.
- Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.
- Detect unknown threats and automatically deliver protections globally to thwart new attacks via WildFire.

Exploitation

Once attackers gain access "inside" an organization, they can activate attack code on the victim's host and ultimately take control of the target machine.

Stage 3: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Block known and unknown vulnerability exploits using Traps Advanced Endpoint Protection, which also provides detailed forensics on breaches so WildFire can automatically deliver protections globally to thwart additional follow-on attacks.
- Block unwanted applications through App-ID and detect unknown malware pervasively throughout the network with WildFire.

Installation

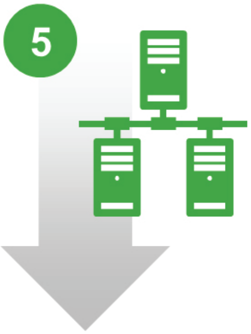
Attackers will seek to establish privileged operations, root kit, escalate privileges, and establish persistence.

Stage 4: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Prevent local exploitation leading to privilege escalation/password theft with Traps, which also prevents malware from accessing OS functions. Traps sends samples of unknown malware it encounters to WildFire to create additional protections.
- Establish secure zones with strictly enforced user access control with next-generation firewall/GlobalProtect, and provide ongoing monitoring and inspection of all traffic between zones (Zero Trust model).
- Granular control of applications to allow only authorized applications on the enterprise, limiting the attackers' ability to move laterally with unknown tools and scripts.

Command and Control

Attackers establish a command channel back through the Internet to a specific server so they can communicate and pass data back and forth between infected devices and their server.



Stage 5: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Block outbound command-and-control communications (through anti-CnC signatures), as well as file and data pattern uploads.
- Block outbound communication to known malicious URLs through PAN-DB for URL filtering.
- Block novel attack techniques with App-ID, which is able to identify applications on any port.
- Re-direct malicious outbound communication to internal honeypots to identify and block compromised hosts.
- Create a database of malicious domains to ensure global awareness/ prevention through DNS monitoring.

Actions on the Objective

Attackers may have many different motivations for attack, and it's not always for profit. Their reasons could be data exfiltration, destruction of critical infrastructure, or to deface web property or create fear/extortion.

Stage 6: How Palo Alto Networks Breaks the Cyber Attack Lifecycle

- Block outbound command-and-control communications (through anti-CnC signatures), as well as file and data pattern uploads.
- Block outbound communication to known malicious URLs through PAN-DB for URL filtering.
- Granular application and user control to enforce file transfer application policies on the enterprise, eliminating known archiving and transfer tactics.

Conclusion

The Enterprise Security Platform from Palo Alto Networks allows companies to remain agile in the face of advanced attacks and provides a unique ability to defend enterprises against cyber criminals. The platform protects every part of the global enterprise network, addressing vulnerabilities and malware arriving at the endpoint, mobile device, network perimeter and within the data center. This provides new defense and resilience to prevent attackers at every stage of the Cyber Attack Lifecycle. In addition to the resilience and prevention against today's most sophisticated attacks, Palo Alto Networks provides:

- Automated prevention tools that minimize reliance on manual operations
- Easy transition from legacy point-appliances and tools
- Extensibility to extend prevention and resilience to every location a Palo Alto Networks device and agent exists within the enterprise: promoting Zero Trust segments into physical and cloud-based data centers

In all, the Enterprise Security Platform reduces costs and risk while introducing an entirely new approach for operating and defending enterprises wherever they operate.

For more information regarding the Palo Alto Networks Enterprise Security Platform and its component technologies, please visit www.paloaltonetworks.com.

paloalto NETWORKS®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com