White Paper

Addressing the Full Attack Continuum: Before, During, and After an Attack

It's Time for a New Security Model

Today's threat landscape is nothing like that of just 10 years ago. Simple attacks that caused containable damage have given way to modern cybercrime operations that are sophisticated, well-funded, and capable of causing major disruptions to organizations and the national infrastructure. Not only are these advanced attacks difficult to detect, but they also remain in networks for long periods of time and amass network resources to launch attacks elsewhere.

Traditional defenses that rely exclusively on detection and blocking for protection are no longer adequate. It's time for a new security model that addresses the full attack continuum—before, during, and after an attack.

The Industrialization of Hacking

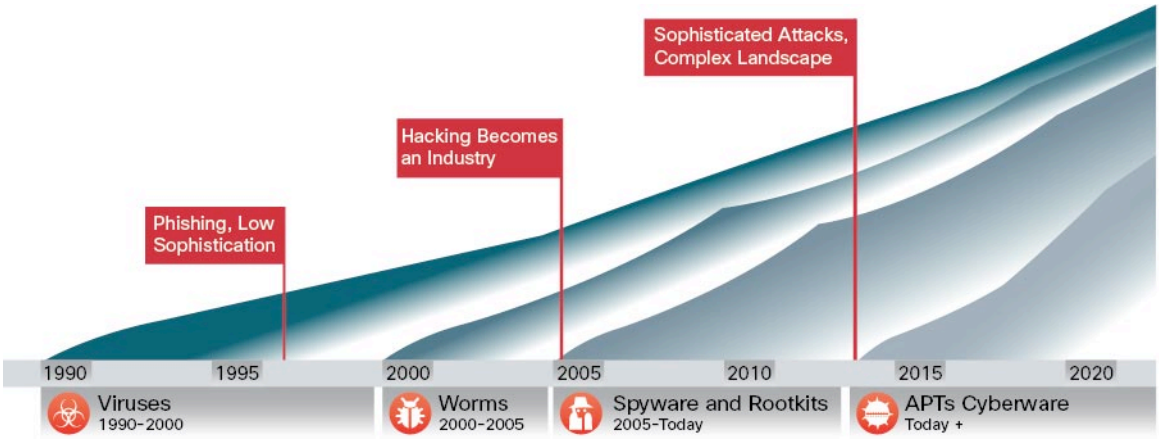
The first PC viruses appeared more than 25 years ago. Little did we realize that they were just the beginning of what would evolve into the industrialization of hacking.

For nearly 10 years, viruses endured as the primary method of attack, and over time they were largely matched by defenders' ability to block and protect against them. Motivated by the notoriety and the knowledge gained by the discovery and publicizing of new vulnerabilities, attackers continued to innovate. What ensued were distinct threat cycles, an "arms race," so to speak. Approximately every five years attackers would launch new types of threats—from macroviruses to worms to spyware and rootkits—and defenders would quickly innovate to protect networks from them.

It's no surprise that we can map these cycles to major technology shifts that presented new attack vectors (see Figure 1). Early viruses primarily targeted the operating system and were spread by 'sneaker net.' Macro viruses took advantage of users sharing files. Worm-type threats that moved from machine to machine made use of enterprise networks and the increasing use of the Internet activity. And spyware and rootkits emerged with new applications, devices, and online communities. Today we're faced with advanced malware, targeted attacks, and advanced persistent threats (APTs). What separates this era from the past are the motivations and the tools behind the attacks, making them particularly challenging to detect, understand, and stop.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Figure 1. The Industrialization of Hacking



The industrialization of hacking is creating a faster, more effective, and more efficient criminal economy profiting from attacks to our IT infrastructure. The organized exchange of exploits is flourishing and lucrative, with the open market helping to fuel the shift from exploitation to theft, disruption, and destruction. And as cybercriminals have realized there is significant money to be made, their work has become more standardized, mechanized, and process driven. Attackers understand the static nature of classic security technologies and their disparate deployments, so they can exploit the gaps between, and vulnerabilities within them. It's even commonplace for hacker groups to follow software development processes, like quality-assurance testing or bench-testing products against security technologies before releasing them into the wild, to help ensure they'll continue to evade common protections.

There are now significant financial incentives for secrecy, and many "hactivist" groups are motivated to launch attacks that result in economic or political gain with little chance of retribution or prosecution. New methods like port and protocol hopping, encrypted tunneling, droppers, and blended threats and techniques that use social engineering and zero-day attacks have made it easier, faster, and cheaper for hackers to get in and increasingly difficult for defenders to see them and keep them out. Compounding the elusiveness, the attacks themselves can change rapidly as they progress through the enterprise seeking a persistent foothold and exfiltrating critical data.

The Any-to-Any Challenge

Modern extended networks and their components constantly evolve and spawn new attack vectors. These include mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, and embedded computers, as well as a proliferation of devices and services we're only beginning to imagine, brought on by the Internet of Everything. People are inside and outside the network, on any device, accessing any application, and in many different clouds. This ubiquity is the "any-to-any" challenge, and while these dynamics have enhanced our communications, they have also increased the entry points and methods that hackers use to get in. Unfortunately, the way most organizations approach security hasn't evolved in lockstep.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

The majority of organizations secure extended networks using disparate technologies that don't, and can't, work together. They may also overly rely on service providers for security in the cloud and on hosting companies to protect the Internet infrastructure. In this new reality, security administrators all too often have little visibility or control over the devices and applications accessing the corporate network and limited ability to keep pace with new threats.

New Security Dynamics

Faced with the combination of advanced attacks and the any-to-any infrastructure, security professionals are asking themselves three big questions:

1. *With new business models and attack vectors, how do we maintain security and compliance as our IT landscape continues to change?* Organizations transitioning to the cloud, virtualization, or mobile devices for the productivity, agility, and efficiency these technologies provide must align their security infrastructure accordingly.
2. *In an evolving threat landscape, how do we improve our ability to continuously protect against new attack vectors and increasingly sophisticated threats?* Attackers don't discriminate; they'll seize on any weak link in the chain. They relentlessly drive their attacks home, frequently using tools that have been developed specifically to circumvent the target's chosen security infrastructure. They go to great lengths to remain undetected, using technologies and methods that result in nearly imperceptible indications of compromise.
3. *How are we going to address the first two questions and reduce the complexity and fragmentation of security solutions at the same time?* Organizations can't afford to leave gaps in protection that today's sophisticated attackers exploit. At the same time, adding complexity with disparate security solutions that aren't integrated won't deliver the level of protection required against advanced threats.

> *"100 percent of companies have connections to domains that are known malware threat sites."*
>
> –Cisco Annual Security Report 2014

The combination of these dynamics—changing business models, an evolving threat landscape, and security complexity and fragmentation—has created security gaps, broken the security lifecycle, reduced visibility, and introduced security management challenges. To truly protect organizations in the face of these dynamics, we need to change our approach to security. It's time for a new threat-centric security model.

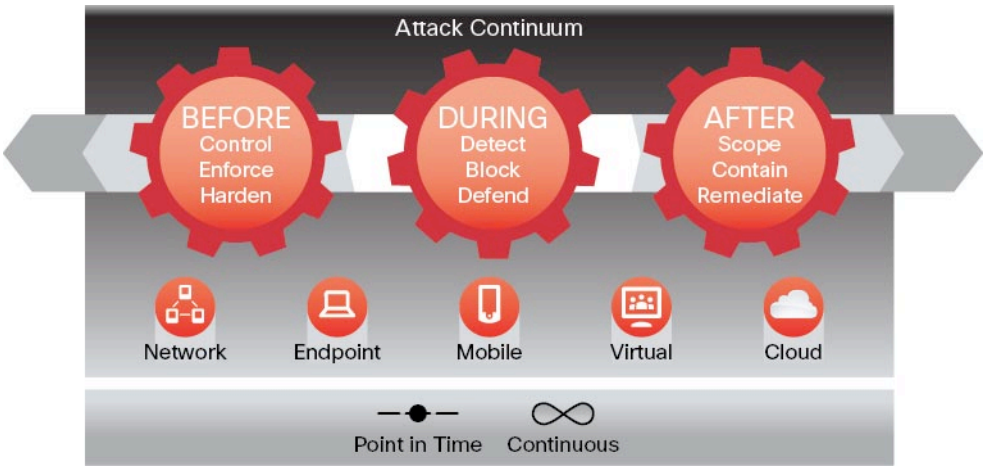
Addressing the Full Attack Continuum: Before, During, and After an Attack

Most security tools today focus on providing visibility into the network and blocking malware at the point of entry. They scan files once at an initial point in time to determine whether they are malicious. But advanced attacks do not occur at a single point in time; they are ongoing and require continuous scrutiny. Adversaries now employ tactics such as port hopping, encapsulation, zero-day attacks, command and control (C&C) detection evasion, sleep techniques, lateral movement, encrypted traffic, blended threats, and sandbox evasion to elude initial detection. If the file isn't caught or if it evolves and becomes malicious after entering the environment, point-in-time detection technologies cease to be useful in identifying the unfolding follow-on activities of the attacker.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Security methods can't just focus on detection but must also include the ability to mitigate the impact once an attacker gets in. Organizations need to look at their security model holistically and gain visibility and control across the extended network and the full attack continuum: before an attack happens, during the time it is in progress, and even after it begins to damage systems or steal information (see Figure 2).

Figure 2. The New Security Model



- **Before:** Defenders need comprehensive awareness and visibility of what's on the extended network in order to implement policies and controls to defend it.
- **During:** The ability to continuously detect malware and block it is critical.
- **After:** Defenders need retrospective security in order to marginalize the impact of an attack. They must identify the point of entry, determine the scope, contain the threat, eliminate the risk of re-infection, and remediate the disruption.

Before an Attack

Context-aware attackers require context-aware security. Organizations are fighting against attackers that have more information about the infrastructure that defenders are trying to protect, than the defenders often have themselves. To defend before an attack occurs, organizations need total visibility of their environment—including, but not limited to, physical and virtual hosts, operating systems, applications, services, protocols, users, content, and network behavior—in hopes to achieve information superiority over attackers. Defenders need to understand the risks to their infrastructure, based on its target value, the legitimacy of an attack, and history. If they don't understand what they're trying to protect, they will be unprepared to configure security technologies to defend. Visibility needs to span the entirety of the network—from, endpoints, email and web gateways, virtual environments and mobile devices, as well as to the data center. And from this visibility, actionable alerts must be generated so that defenders can make informed decisions.

During an Attack

Relentless attacks do not occur in a single point of time; they are an ongoing activity and demand continuous security. Traditional security technologies can only detect an attack at a point in time, based on a single data point of the attack itself. This approach is no match against advanced attacks. Instead, what's needed is a security infrastructure based on the concept of awareness; one that can aggregate and correlate data from across the

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

extended network with historical patterns and global attack intelligence to provide context and discriminate between active attacks, exfiltration, and reconnaissance versus simply background noise. This evolves security from an exercise at a point in time to one of continual analysis and decision-making. Should a file pass through that was thought to be safe but that later demonstrates malicious behavior, organizations can take action. With this real-time insight security professionals can employ intelligent automation to enforce security policies without manual intervention.

After an Attack

To address the full attack continuum, organizations need retrospective security. Retrospective security is a big data challenge and a capability that few are able to deliver. With an infrastructure that can continuously gather and analyze data to create security intelligence, security teams can, through automation, identify indications of compromise, detect malware that is sophisticated enough to alter its behavior to avoid detection, and then remediate the problem. Compromises that would have gone undetected for weeks or months can be identified, scoped, contained, and remediated.

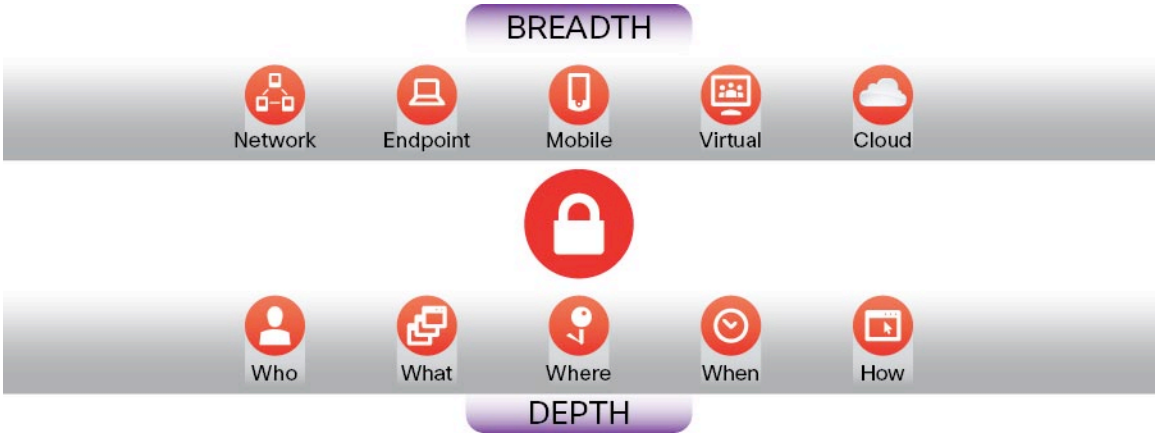
This threat-centric model of security lets organizations address the full attack continuum, across all attack vectors and respond at any time, all the time, and in real time.

Enabling the New Security Model

To enable the New Security Model, Cisco believes that modern security technologies need to focus on three strategic imperatives: they must be visibility-driven, threat-focused, and platform-based.

Visibility-driven: Security administrators must be able to accurately see everything that is happening. This capability requires a combination of breadth and depth (see Figure 3). Breadth is having the capability to see and gather data from all potential attack vectors across the network fabric, endpoints, email and web gateways, mobile devices, virtual environments, and the cloud to gain knowledge about environments and threats. Depth provides the capability to correlate this information, apply intelligence to understand the context, make better decisions, and take action either manually or automatically.

Figure 3. Breadth and Depth



© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

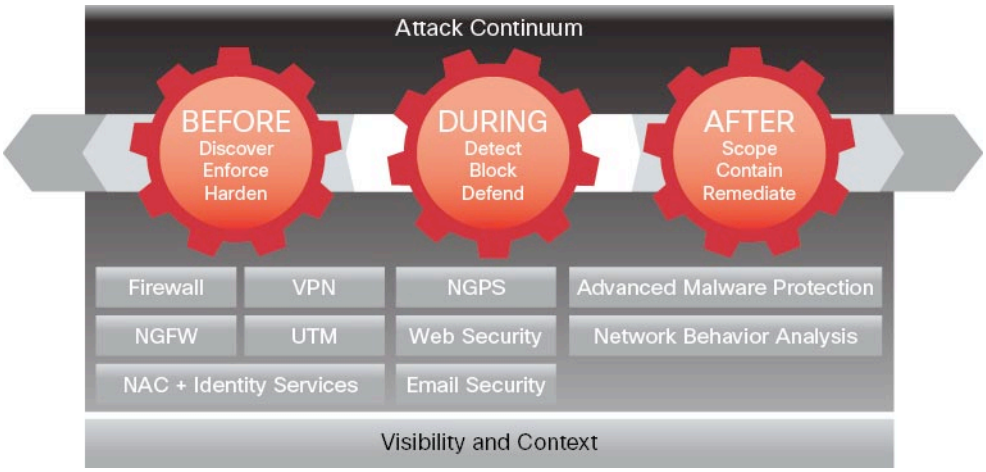
Threat-focused: Today's networks extend to wherever employees are, wherever data is, and wherever data can be accessed from. Despite best efforts, keeping pace with constantly evolving attack vectors is a challenge for security professionals and an opportunity for attackers. Policies and controls are essential to reduce the surface area of attack, but threats still get through. As a result, technologies must also focus on detecting, understanding, and stopping threats. Being threat-focused means thinking like an attacker, applying visibility and context in order to understand and adapt to changes in the environment and then evolving protections to take action and stop threats. With advanced malware and zero-day attacks, this is an on-going process that requires continuous analysis and real-time security intelligence delivered from the cloud and shared across all products for improved efficacy.

Platform-based: Security is now more than a network issue; it requires an integrated system of agile and open platforms that cover the network, devices, and the cloud. These platforms need to be extensible, built for scale, and centrally managed for unified policy and consistent controls. Simply put, they need to be as pervasive as the attacks we are combating. This constitutes a shift from deploying simple point security appliances to integrating a true platform of scalable, easy-to-deploy services and applications. Not only does a platform-based approach increase security effectiveness, eliminating silos and the security gaps they create, but it also accelerates the time to detection and streamlines enforcement.

Covering the Full Attack Continuum

To overcome today's security challenges and gain better protection, organizations need solutions that span the entire attack continuum and are designed based on the tenets of being visibility-driven, threat-focused and platform-based. Cisco offers a comprehensive portfolio of threat-centric cybersecurity solutions that span the entire attack continuum.

Figure 4. Covering the Entire Attack Continuum



These specific, platform-based solutions offer the industry's broadest set of enforcement and remediation options at attack vectors where threats manifest. These solutions work together to provide protection throughout the attack continuum and also integrate into complementary solutions for an overall security system.

- Before an attack, solutions that include firewalls, Next-Generation Firewalls, Network Access Control, and identity services, to name a few, give security professionals the tools they need to discover threats and enforce and harden policies.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

- During an attack, Next-Generation Intrusion Prevention Systems and email and web security solutions provide the ability to detect, block, and defend against attacks that have penetrated the network and are in progress.
- After an attack, organizations can leverage Cisco Advanced Malware Protection and network behavior analysis to quickly and effectively scope, contain, and remediate an attack to minimize damage.

Scalable to support even the largest global organizations, these solutions are available when and how organizations need them, as physical and virtual appliances, or as cloud-based services. They are also integrated to provide continuous visibility and control across the extended network and all attack vectors.

Conclusion

The industrialization of hacking, combined with the any-to-any challenge, is profoundly changing how we must protect our systems, driving us to think about a new approach to cybersecurity. Security strategies that focus on perimeter-based defenses and preventive techniques will only leave attackers free to act as they please once inside the network.

Changing business models, an evolving threat landscape, and security complexity and fragmentation have created security gaps, broken the security lifecycle, reduced visibility, and introduced security management challenges. It's time for a new threat-centric security model that delivers the visibility and control organizations need across the extended network and the full attack continuum.

Cisco is uniquely capable of delivering a threat-centric approach to security that reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum. With this new security model, organizations can act smarter and more quickly before, during, and after an attack.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-731741-00 05/14

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.