Addressing the Full Attack Continuum: A Security Model for Before, During, and After an Attack

What You Will Learn

Recent changes in hacking combined with the emergence of the Internet of Everything have profoundly changed how we protect our systems, driving us to think about a new approach to cybersecurity. In this paper, learn about the challenges that created the need for a new threat-centric security model spanning the full attack continuum: before, during and after an attack.

At Cisco, our threat-centric approach to security spans the attack continuum to deliver:

- Superior visibility
- Continuous control
- Advanced threat protection

It's Time for a New Security Model

Today's threat landscape is nothing like that of 10 years ago. Simple attacks that caused containable damage have given way to modern, sophisticated, and well-funded cybercrime operations capable of disrupting and causing major loss to organizations and national infrastructure. These are difficult to detect, can remain in networks for long periods of time, and amass resources to launch attacks elsewhere.

Legacy protection methods that exclusively rely on detection and blocking 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 this was just the beginning of what would evolve into the industrialization of hacking. For nearly 10 years, viruses endured as the primary method of attack but were largely matched by defenders' talents to protect against them over time. Motivated by the notoriety and knowledge gained in discovering and publicizing a new vulnerability, attackers continued to innovate. Distinct threat cycles emerged, an "arms race" so to speak. Attackers launch new types of threats approximately every five years, and defenders quickly innovate to protect against them.

It's no surprise that threat cycles map to major technology shifts. Technology changes present new attack vectors. Historically, each new attack vector presented a new kind of threat:

- **Early viruses:** Target the operating system and spread by a "sneaker" network
- **Macro viruses:** Take advantage of users sharing files
- **Worm-type threats:** Use enterprise networks and increase Internet usage to move from machine to machine
- **Spyware and rootkits:** Emerged with new applications, devices, and online communities

Today we face advanced malware, targeted attacks, and advanced persistent threats (APTs). Motivations and attack tools separate this era from the past, making attacks particularly challenging to detect, understand, and stop.

The industrialization of hacking created a faster, more effective, and more efficient criminal economy that profits from IT infrastructure attacks. An organized exchange of exploits emerged as the open market fueled a shift from exploitation to theft, disruption, and destruction. As cybercriminals realized the money to be made, their work was standardized and mechanized, and became more process driven. Attackers understand the fundamentally static nature of classic security technologies and their disparate deployment, exploiting the gaps and vulnerabilities within. Today, many hacker groups even follow software development processes, QA or bench testing their products against security technologies before releasing them in the “wild” to continue evading common protections.

Financial incentives for secrecy have become paramount, and “hactivist” groups motivated to launch attacks for economic or political gain face little chance of retribution or prosecution. New methods to circumvent protection (port and protocol hopping, encrypted tunneling, droppers, blended threats, social engineering and zero-day attacks) have made it easier, faster, and cheaper for hackers to get in.

Defenders find it increasingly difficult to even detect threats, much less keep them out. Compounding their elusiveness, the attacks themselves can change rapidly as they progress through the enterprise, seeking a persistent foothold and extracting critical data.

The Any-to-Any Challenge

Modern extended networks and network components constantly evolve, spawning new attack vectors: mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, embedded computers, as well as a proliferation of endpoints and services we’re only beginning to imagine with the emergence of the Internet of Everything. People work inside and outside the network on any device, accessing any application and in multiple clouds. This is the any-to-any challenge. While these dynamics enhance our communications and productivity, they also increase the points and ways in which hackers access networks. Unfortunately, most organizations’ approach to security hasn’t evolved in lockstep with increased vulnerabilities.

Most organizations secure extended networks with disparate technologies that don’t, and can’t, work together. Often, they rely on service providers for security in the cloud and hosting companies to protect Internet infrastructure. In this emergent reality, security administrators have little visibility or control over the devices and applications accessing the corporate network, limiting their ability to keep pace with new threats.

New Security Dynamics

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

1. **How do we keep up with attacks that are different, constant, and more and more sophisticated?** Organizations transitioning to the cloud, virtualization, or mobile devices must align their security infrastructure accordingly.
2. **How do we allow our business to change rapidly and still maintain security?** Attackers don’t discriminate. They 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 indicators of compromise.

3. **We have so many fragmented security elements. How can we manage it all?** Organizations can't afford to leave gaps in protection that can be easily exploited by today's sophisticated attackers. At the same time, adding complexity with incompatible security solutions won't deliver the level of protection required against advanced threats.

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.

A New Model for a New Dynamic: Before, During, and After

Most security tools today focus on visibility and blocking at the point of entry in order to protect systems. However, the proliferation of threats far outpaces these network defense tactics, and the subsequent gap can never fully be closed. No new technology will adequately address this security dynamic. Instead, a new criteria is required: a defense model that detects, mitigates and remediates before, during, and after an attack.

You need more than point-in-time detection technologies because attackers design threats specifically to elude initial detection. If a file goes undiscovered or if it evolves and becomes malicious after entering the environment, you need to trace its steps to quickly identify the behavior and follow-on activities of the attacker.

Security methods must focus on both detection and the ability to mitigate the impact after an attacker gets in. You need to look at their security model holistically and gain visibility and control not just at the endpoints but across the extended network and the entire attack continuum before an attack happens, during the time it's in progress, and after it has damaged systems or stolen information.

- **Before:** Identify what's on the extended network to implement policies and controls to defend it
- **During:** Detect and block malware continuously
- **After:** Reduce the impact of an attack by identifying point of entry, determining the scope, containing the threat, eliminating the risk of reinfection, and remediating

Before an Attack

Combatting context-aware attackers requires context-aware security. Organizations face attackers with more information about the infrastructure than defenders often have themselves.

To defend your network before an attack occurs, you need to win the information battle. Gain total visibility of your environment. This includes, but is not limited to, physical and virtual hosts, operating systems, applications, services, protocols, users and content, and network behavior. Understand the risks to your infrastructure based on target value, legitimacy of an attack, and history. Without understanding what you're trying to protect, you will be unprepared to configure security technologies to defend. Make informed decisions with visibly actionable alerts. Visibility needs to span the entirety of the network: endpoints, email and web gateways, virtual environments, mobile devices, and your data center.

During an Attack

Defense during an attack requires acting on awareness. Implement a strategy that can aggregate and correlate data from across the extended network with historical patterns and global attack intelligence. Provide context and discriminate between active attacks, exfiltration, and reconnaissance versus just background activity. Evolve point-in-time security to continual analysis and decision making. Take action when a file, initially deemed safe, demonstrates malicious behavior. Employ intelligent automation to enforce security policies with real-time insight and without manual intervention.

Relentless attacks and blended threats do not occur at a single point in time. They strike constantly and demand continuous security. Traditional security technologies evaluate an attack only at a point in time, based on a single data point of the attack. This approach is no match against advanced attacks.

After an Attack

Retrospective security demands big-data analysis. Develop comprehensive security intelligence with an infrastructure that continuously gathers and analyzes data. Automate a process that identifies indicators of compromise. Detect sophisticated malware that alters its behavior. Remediate the issue. Compromises that can go undetected for weeks or months can be rapidly identified, scoped, contained and fixed.

With this threat-centric model of security, you can address the entire attack continuum, across all attack vectors and respond in real time, at any time, all the time.

Enabling the New Security Model

To erect the new security model, focus on three strategic imperatives:

- **Visibility driven:** See everything accurately. This requires a combination of breadth and depth. Breadth sees and gathers 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 correlates this information, applies intelligence to understand context, makes better decisions, and takes action either manually or automatically.
- **Threat focused:** Think like an attacker. Being threat focused means applying visibility and context to understand and adapt to changes in the environment and then evolving protections to take action and stop threats. Today's networks extend to wherever employees work and where data exists and can be accessed from. Despite best efforts, keeping pace with constantly evolving attack vectors is a challenge and an opportunity for attackers. Policies and controls reduce the surface area of attacks, but threats still get through. As a result, technologies must focus on detecting, understanding, and stopping threats. As ongoing processes, advanced malware, and zero-day attacks require continuous analysis and real-time security intelligence delivered from the cloud and shared across all products for improved efficacy.
- **Platform-based:** Integrate a true platform of scalable, easy-to-deploy services and applications. More than a network issue, security now 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. They need to be as pervasive as the attacks they combat. This constitutes a shift from only deploying point security appliances to integrating a scalable and easy-to-deploy platform. Not only does a platform-based approach increase security effectiveness, eliminating silos and the security gaps they create, but it also accelerates time to detection and streamlines enforcement.

Covering the Entire Attack Continuum

To overcome today's security challenges and gain better protection, you need visibility-driven, threat-focused, and platform-based solutions that span the entire attack continuum. Across-the-board protection (spanning the attack continuum) requires the integration of technologies with different areas of focus. The Cisco® security portfolio, which now includes Sourcefire products, offers a comprehensive range of threat-centric cybersecurity solutions that fight advanced malware, targeted attacks, and APTs. These specific, platform-based solutions offer the industry’s broadest set of enforcement and remediation options at attack vectors where threats manifest.

Cisco solutions work together to provide protection throughout the attack continuum and also that can be integrated with complementary solutions for an overall security system:

- **Before an attack:** Discover threats, and enforce and harden policies with Cisco Firewall, ASA 5500-X Series Next-Generation Firewalls, Identity Services Engine, and Network Access Control (NAC) products.
- **During an attack:** Detect, block, and defend against attacks that have already penetrated the network and are in progress with next-generation intrusion prevention systems, and email and web security.
- **After an attack:** Scope, contain, and remediate an attack to minimize damage with advanced malware protection and network behavior analysis.

Scalable to support even the largest global organizations, deploy these solutions when and how they’re needed, as physical and virtual appliances or as cloud-based services, providing continuous visibility and control across the extended network and all attack vectors.

Conclusion

The industrialization of hacking combined with the any-to-any challenge have profoundly changed how we protect our systems, driving us to think about a new approach to cybersecurity. Security strategies that focus on perimeter-based defenses and preventative techniques will only leave attackers free to act as they please after they’re inside networks.

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 extended networks and the full attack continuum.

Deliver a threat-centric approach to security that reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum. Act smarter and quicker before, during, and after an attack.

To learn more about Cisco security solutions, visit http://www.cisco.com/go/security.

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.**

Printed in USA C11-733368-00 11/14