Solution Brief

Building Resilience in a Digital Enterprise

Top five steps to help reduce the risk of advanced targeted attacks

TM

To be successful in business today, an enterprise must operate securely in the cyberdomain. We're in a period of unprecedented change, where transformative technology is creating new opportunities for business innovation and new ways for cybercriminals or state actors to threaten the business. Building resilient digital services and safeguarding sensitive data are essential to establishing trust with customers and maintaining business continuity. As such, improving business resilience against targeted and persistent cyberattacks should be an executive priority. The goal of this paper is to help business and security executives prioritize their security control investments in key areas to maximize protection against advanced targeted attacks. However, these steps represent only a starting point. Building cyber resilience against advanced targeted attacks takes a long-term approach that involves security architecture, insights, and cultural change in the organization.

Understanding Advanced Targeted Threats

According to the SANS Critical Security Controls, one of the key tenets of an effective cyberdefense program is "Offense informs defense." Targeted threats designed to steal or destroy sensitive business data follow a common pattern. By understanding an adversary's methods, an enterprise CISO can prioritize investments in the right security architecture layers to have the most impact on business risk reduction. The external attack model paints a more complete picture of adversary's methods by identifying pre- and post-exploit actions, rather than narrowly focusing on one aspect of the attack itself. With better alignment to real-world threat operations, the external attack model provides an excellent guide for security executives to focus defense in depth controls and increase the value of security to the business.

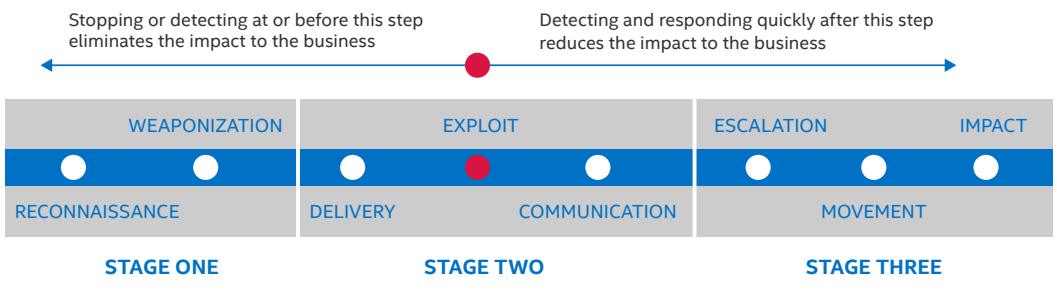


Figure 1. External attack model.

intel Security

Awareness of adversary tactics and techniques offers the key insights necessary to prevent, detect, or respond faster and more effectively. Using this model, an enterprise should prioritize building security capability to prevent and detect adversary actions in stage two, commonly called the "infection stage" of the attack model.

The infection stage has three main components: delivery, exploit, and communication.

The major adversary actions at each stage are listed in the table below:

Infection Stage	Adversary Actions
Delivery	Socially engineered email with malicious link or attachment.
	Download of malicious file or content from the web.
Exploit	Vulnerability exploit in Adobe, Flash, MSOffice, Java, browsers.
	Installation of advanced or zero-day malware.
	Installation of a remote access Trojan.
	SQL Injection against web applications.
Communication	Command and control over DNS, HTTP, HTTP protocols.
	Remote access Trojan.

Table 1. The infection stage of an attack.

"Delivery" is defined as the initial attack vector and is typically accomplished via email or removable media. According to industry statistics from the *Verizon Data Breach Report* and the SANS Institute, spear phishing is still the most effective way for an attacker to deliver advanced malware and gain a foothold in an enterprise network. The malware is usually packaged inside a PDF or other document created with a common user application. The malware has a high success rate due to application vulnerabilities and the likelihood that it will bypass antivirus controls. "Exploit" is the actual vulnerability exploitation that results in the installation of a backdoor, such as a remote access Trojan. Finally, the "communication" stage is where the attacker interacts with the exploited machine through the backdoor Trojan and attempts to escalate or steal administrative credentials. If an attacker completes each of these stages, he has gained a foothold and can move around the enterprise network in stealth mode. It becomes very difficult at this point to prevent or detect the movement and the potential theft of data. So it is important to maximize prevention, detection, and response capability as early as possible in the attack model.

Top Five Steps to Reduce the Risk of Advanced Targeted Attacks

Designing the enterprise security architecture with operational knowledge of targeted threat methods will help organizations prioritize investments at each security layer for the most effectiveness and value. The SANs Critical Security Controls guide states that one of the key tenets of a good cyberdefense program is as follows: "Prioritize controls that will provide the greatest risk reduction." When looking at the attack model, preventing, detecting, and containing an attack in stage two will provide the greatest risk reduction capability. In stage two, it is to prevent an attacker from going any further, as he is most exposed to detection because of all the attack indicators he leaves in his wake during an exploit attempt. Many organizations are at risk and need to quickly improve capability to prevent, detect, or respond to a breach. The following represent the top five steps an organization can take to reduce risk immediately.

1. **User awareness:** Train all users on anti-malware procedures and how to recognize, respond, and report phishing emails. Proper user education will greatly reduce the chance of exploitation and will speed up response actions.
2. **Endpoint client anti-malware:** Deploy and implement application whitelisting on user workstations and laptops. Application whitelisting will prevent advanced and zero-day malware from exploiting your system. This is also recommended as a "Quick Win" from the SANS Critical Security Controls.

3. **Network anti-malware:** Maximize email and web protocol anti-malware capability with integrated intelligence and malware sandboxing on the Internet boundary. Email and web are the primary delivery vectors for advanced malware. Using intelligence and malware sandboxing are also recommended by SANS Critical Security Controls (CSC- 5).
4. **Incident response program and trusted cyberintelligence sources for incident detection:** Trusted cyberintelligence sources could come from vendor subscriptions, open source, or your industry ISAC. Developing incident response is recommended by SANS Critical Security Controls (CSC- 5).
5. **Centralized collection of essential data sources (proxy, DNS, IP flow, Microsoft Active Directory, and DHCP) and correlation against trusted intelligence sources:** Use incident response to validate and contain any compromised systems. Collecting proxy logs and DNS data is recommended by SANS Critical Security Controls (CSC- 5).

Using Standards as a Measurement

The SANS Critical Security Controls and recommended Quick Wins provide an excellent guide to maximize anti-malware prevention and detection capability. The SANS Critical Security Control 5 are practical steps that will significantly reduce exposure to advanced malware and provide a measurable way to improve security. Below is a chart that demonstrates how Intel Security solutions can simplify implementation of the all the recommended anti-malware controls.

NIST Control	SANS CSC	Control Description	Attack Chain Stage	Intel Security Solution
Prevention	CSC 2-1	Deploy application whitelisting.	Exploit	McAfee® ePO™/McAfee Application Control
Prevention	CSC 5-1	Deploy antivirus/antispam, host intrusion prevention, and firewall to end-user devices and servers; centrally collect logs.	Exploit	McAfee ePO/McAfee VirusScan®/ McAfee Host Intrusion Prevention
Prevention	CSC 5-2	Use anti-malware with cloud-based reputation intelligence and performs central updates.	Exploit	McAfee Global Threat Intelligence is integrated to all endpoint and network products
Prevention	CSC 5-3	Disable auto-run.	Delivery, Exploit	OS function
Prevention	CSC 5-4	Auto virus scan of removable media.	Delivery, Exploit	McAfee ePO/VirusScan Enterprise/McAfee Application Control
Prevention	CSC 5-5	Scan and block all email attachments with malicious code or unauthorized file content.	Delivery	McAfee Web Gateway, McAfee Email Gateway and McAfee Advanced Threat Defense with integrated McAfee Data Loss Prevention
Prevention	CSC 5-6	Enable anti-exploitation features in the OS.	Exploit	OS function
Prevention	CSC 5-7	Limit the use of external devices and monitor for violations.	Delivery	McAfee ePO/Data Loss Prevention Endpoint
Prevention	CSC 5-8	Use behavior and signature-based protection tools.	Delivery, Exploit, C2	All Intel Security products use a combination of behavior and signature-based capability
Prevention	CSC 5-9	Use network based anti-malware to identify executables and malicious content.	Delivery	McAfee Web Gateway and McAfee Email Gateway with McAfee Advanced Threat Defense

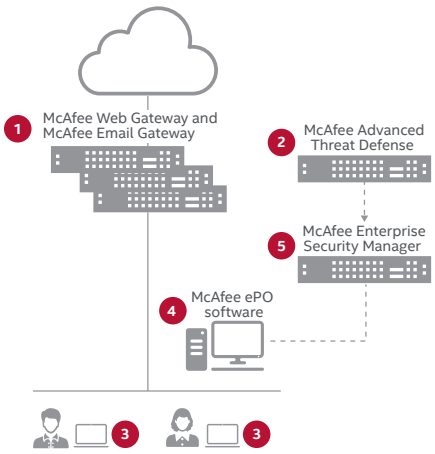
Implementing the Top Five with Intel Security Solutions

User awareness

The user is the first line of defense against advanced targeted attacks. Spear phishing is still the most common and most successful technique for the delivery of malware. Developing a repeatable user awareness and training program will help turn the user into part of the security solution. Intel Security Professional Services can help design and implement this program, as well as measure its success through testing.

Anti-malware

As the web is the most prevalent vector for malware delivery, it is important to maximize anti-malware inspection on HTTP and HTTPS protocols. McAfee Web Gateway is continuously rated as the top solution for gateway anti-malware, with more than 95% effectiveness against known and unknown malware.[1] McAfee Advanced Threat Defense, an integrated malware analytics platform, will extend the prevention and detection capability of McAfee Web Gateway even higher. In addition, McAfee Advanced Threat Defense produces critical indicators of compromise in the form of STIX or Open IOC, enabling faster detection capability. For client protection, McAfee Application Control is a whitelisting solution that will immediately reduce the attack surface for targeted threats and provide improved protection against unknown malware.



1. McAfee Web Gateway and McAfee Email Gateway are deployed on the Internet boundary to provide initial anti-malware protection. Both products are Gartner top-rated solutions for protecting against advanced malware using signature and behavior techniques with integrated intelligence.
2. The anti-malware capability of McAfee Web Gateway and McAfee Email Gateway can be extended with the integration of McAfee Advanced Threat Defense, a malware analysis sandbox interoperable with both products. McAfee Advanced Threat Defense provides advanced analysis and intelligence capability.
3. McAfee Application Control is a whitelisting solution that is centrally managed through McAfee ePO software. It can be deployed on client endpoints or servers. McAfee Application Control stops advanced malware installation and sends alerts to McAfee ePO software for reporting and management.
4. McAfee ePO software provides a central logging and policy configuration point for endpoints and servers. Events and alerts from McAfee ePO software can be sent to McAfee Enterprise Security Manager.
5. McAfee Enterprise Security Manager is an SIEM that acts as a central repository for all security and system logs. McAfee Enterprise Security Manager can be used by security operations security analysts to detect compromised assets and for management reporting.

Figure 2. Web anti-malware, analytics, SIEM, and whitelisting in action.

Security operations

Effective incident detection and response is essential to protect the enterprise against advanced targeted attacks. The first step is developing an incident response process with analysts trained in malware and attack techniques. Intel Security Professional Services can help design and implement an incident response program, train analysts on malware analysis techniques, and test process effectiveness through penetration testing or table-top drills. Identifying attacks early requires having the right operational data and the right trusted intelligence sources. In the infection stage, we recommended that organizations focus detection use cases on command and control initially. McAfee Enterprise Security Manager simplifies the intelligence integration and analysis process with Cyber Threat Manager and BackTrace, an automated program to search through historical data.

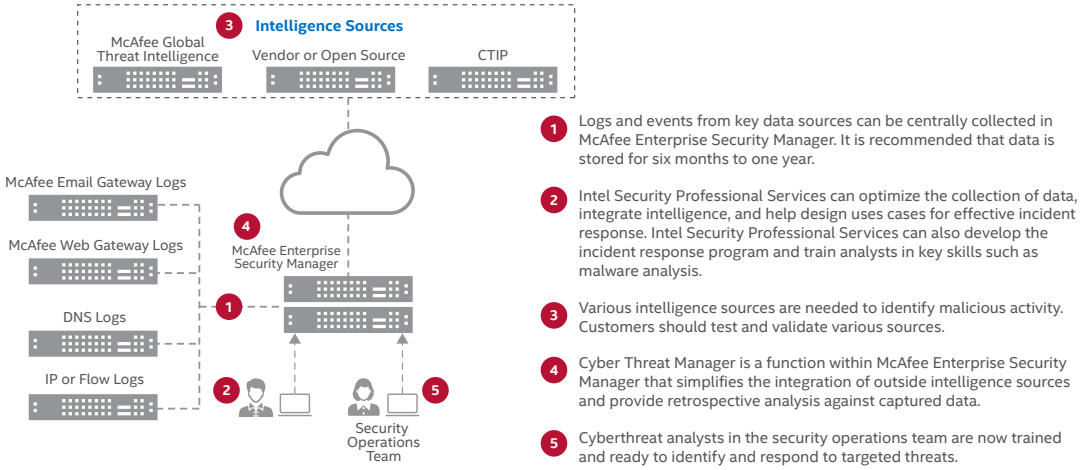


Figure 3. Effective incident detection and response rely on SIEM and automated tools that sift through historical data.

Improved security with Intel Security Solutions

The recommendations in this solution guide are designed to improve security capability for the customer. By using a threat-focused approach, we are able to place security investments into areas that will reduce risk to the business. By aligning security capability building blocks with the attack model, the value is clearly recognizable.

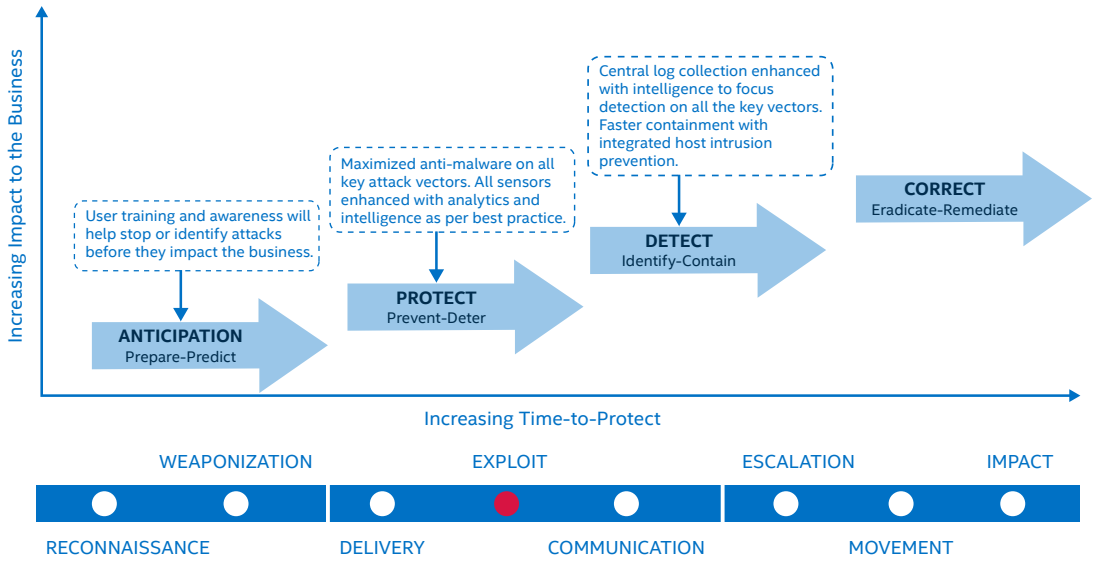


Figure 4. A threat-focused approach to increasing time-to-protection and decreasing impact to the business.

By focusing on balanced controls across user training, anti-malware backed by intelligence and security operations, the solutions enable an enterprise to:

- **Prevent more attacks earlier:** The anti-malware steps are focused on key vectors, are enhanced by intelligence, and are aligned to best practice recommendations.
- **Detect and contain more attacks faster:** Focused data collection combined with simplified intelligence management and trained analysts' increases the efficiency, effectiveness, and capacity of security operations.

Summary

Intel Security solutions can enable business resilience in the cyberdomain through an integrated enterprise security architecture with balanced controls and integrated security multipliers. By leveraging Intel Security solutions and a connected architecture, an organization can improve cyber resilience and confidently move in new business directions.

1. McAfee Web Gateway Security Appliance Test, January 24, 2013
   http://www.mcafee.com/us/resources/reports/rp-avtest-comparative-web-gateway.pdf

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com