

# Protecting Against Advanced Malware and Targeted APT Attacks

## Overview

Defending against next-generation threats requires a strategy that moves beyond signatures and behavioral heuristics. Over 95% of businesses unknowingly host compromised endpoints, despite their use of traditional and next-generation firewalls, intrusion prevention systems (IPS), antivirus and Web gateways. This situation—the new status quo—results from criminals leveraging multiple zero-day vulnerabilities, commercial-quality toolkits and social media to perpetrate next-generation attacks.

Over 90% of today's attacks morph within hours to look new and unknown to signature-based tools. These attacks also do not trigger heuristics because of techniques like camouflage, multi-stage packaging, targeting and other advanced persistent threat (APT) tactics. While signatures and heuristics remain valuable against known threats, criminals are adding new capabilities and concocting new evasion tactics to bypass traditional and next-generation firewalls, IPS, antivirus and Web gateways, leaving a wide-open hole for cybercriminals.



To regain the upper hand against next-generation attacks, enterprises must turn to “lean forward” techniques for protection: signature-less, proactive and real time. Through constant testing of any suspicious code and blocking of communications with malicious hosts, next-generation protections are able to detect and combat advanced malware, zero-day and targeted APT attacks.

Source: FireEye

Featuring research from

**Gartner**

---

## How does advanced malware get past traditional barriers?

---

Advanced targeted attacks use custom-created code that goes undetected by signature-based techniques. While traditional security mechanisms offer policy controls and compliance value, they no longer stop advanced targeted threats.

- **Traditional and Next-Generation Firewalls:** Firewalls allow generic http Web traffic. Next-generation firewalls (NGFW) add layers of policy rules based on users and applications. While NGFW's consolidate traditional protections such as antivirus and IPS, they do not add dynamic protection that can stop advanced, targeted threats, content or behavior.
- **Intrusion Prevention Systems (IPS):** Signatures, packet inspection, DNS analysis and heuristics will not detect anything unusual in a zero-day exploit, especially if the code is heavily disguised or delivered in stages.
- **Antivirus & Web malware filtering:** Since the malware and the vulnerability it exploits are unknown (zero-day), and the Website has a clean reputation, traditional antivirus and Web filters will let exploit attack traffic to pass.
- **Email spam filtering:** Spoofed phishing sites use dynamic domains and URLs, so blacklisting lags behind criminal activities. It takes more than two days to shut down the average phishing site.
- **Web Filtering:** Less than a quarter of enterprises restrict social networking sites. In addition, dynamic URLs, hacks of legitimate Websites and addresses that are active for brief periods make static URL blacklisting as a malware protection strategy obsolete.

### Addressing Advanced Targeted Threats

In the following sections, Gartner offers "Strategies for Dealing with Advanced Targeted Threats." It is clear that cyber attackers are extremely motivated to penetrate network defenses while also remaining under the radar for as long as possible to maximize their earning potential.

FireEye is the leader in a new category of threat prevention adapted to the resilient, evasive and complex nature of advanced targeted threats. One key to preventing advanced targeted attacks is to understand and stop the attack lifecycle. This includes disrupting the initial exploit phase, the callback phase, subsequent download phase(s), and data exfiltration phase. FireEye protects against all these phases of an attack to disrupt it as early in the cycle as possible and mitigate the impact of a network breach.

FireEye's Malware Protection Systems complement traditional defenses by detecting and blocking the advanced malware, zero-day and targeted APT attacks that firewalls, IPS, antivirus and Web gateways cannot stop. By using FireEye's signature-less, dynamic code execution to detect the unknown, organizations gain real-time inbound and outbound protections to plug the network hole left wide open by traditional, signature-based technologies. Leading companies in every industry have already deployed FireEye to eliminate advanced targeted attacks that pose such a high risk to the bottom line.

---

Source: FireEye

## Strategies for Dealing With Advanced Targeted Threats

There has been a lot of hype regarding the term “advanced persistent threat,” and this research provides Gartner’s guidance for choosing the best approach to address growing forms of targeted attacks. Security managers should use this as a decision framework for upgrading enterprise security controls to deal with advanced targeted attacks.

### Key Findings

- Advanced threats are using targeted attacks to get due diligence levels of security controls.
- The source of the targeted threat is less important than the vulnerability it exploits.
- Simply adding more layers of defense does not necessarily increase security against targeted threats — security controls need to evolve.

### Recommendations

- Assess your current level of defense to ensure a solid due diligence baseline.
- Focus on upgrading critical security processes regarding configuration control, application control, Web security and intrusion prevention.
- Evaluate your ability to deploy “lean forward” techniques to detect and rapidly react to advanced threats until your security controls reach parity.

### STRATEGIC PLANNING ASSUMPTION

Through year-end 2015, financially motivated attacks will continue to be the source of more than 70% of the most damaging cyberthreats.

### ANALYSIS

The term “advanced persistent threat” (APT) has been overhyped in the press and is distracting organizations from a very real problem. Targeted attacks are penetrating standard levels of security controls and causing significant business damage to enterprises that do not evolve their security controls. Gartner estimates that, for the average enterprise, 4% to 8% of executables that pass through antivirus and other defenses

are malicious. Enterprises need to focus on reducing vulnerabilities and increasing monitoring capabilities to deter or more quickly react to evolving threats, and not focus on what country the attacks are coming from.

### Advanced Targeted Threats and Advanced Persistent Threats

As business use of the Internet evolves, the threats also continue to evolve. It wasn’t that long ago that simple website defacement attacks and denial-of-service incidents were the most damaging forms of attack. However, starting in 2008 or so, we began to see the growth of financially motivated, targeted attacks. Targeted attacks are a much higher risk to the bottom line, and are generally launched by more-sophisticated attackers who are motivated to penetrate defenses quietly to get inside and steal information — for as long as possible, because that maximizes their revenue opportunities. These same techniques were later used by politically motivated techniques. Gartner believes that, through year-end 2015, financially motivated attacks will continue to be the source of more than 70% of the most damaging cyberthreats.

There have been very specific attacks against U.S. national interests that are believed to have come from other countries. The term “advanced persistent threat” was coined by the military to refer to a specific threat actor (China). It was expanded to include other aggressive nation states, but has been co-opted by the media and by security vendors to hype the source of an attack, which distracts from the real issue — focusing on the vulnerabilities that the attackers are exploiting.

Gartner uses a simple definition of APT. “Advanced” means it gets through your existing defenses. “Persistent” means it succeeds in hiding from your existing level of detection. “Threat” means it causes you harm. We think the targeted aspect is more important to focus on and, for the purposes of this research, will use the term “advanced targeted threat.” The reality is that the most important issues are the vulnerabilities

and the techniques used to exploit them, not the country that appears to be the source of the attack. The major advance in new threats has been the level of tailoring and targeting — these are not noisy, mass attacks that are easily handled by simple, signature-dependent security approaches. Targeted attacks aim to achieve a specific impact against specific enterprises, and have three major goals:

- **Denial of service:** Disrupting business operations
- **Theft of service:** Obtaining use of the business product or service without paying for it
- **Information compromise:** Stealing, destroying or modifying business-critical information

The motivation for advanced targeted threats is usually financial gain, such as through extortion during a denial-of-service attack, trying to obtain “ransom” for stolen information, or selling stolen identity information to criminal groups. This is not to say that state-sponsored attacks do not occur, because they do. Many state-sponsored attacks have been very clever. However, in the majority of cases, they are using attack techniques that were first seen in financially motivated attacks. Some of the state-sponsored attacks exploited “zero day” vulnerabilities that weren’t seen before, but financially motivated targeted attacks have done that for years.

Targeted attacks often use custom-created executables that are rarely detected by signature-based techniques. To be successful, such attacks generally require some means of communication back to an outside party, whether out of band (as when an insider puts information onto removable media and physically carries it outside of enterprise control) or in band (as when Internet mechanisms are used in modern botnet-style threats). All the innovative techniques used in these attacks are detectable. One key to preventing their success is to focus on avoiding, minimizing or shielding the vulnerabilities they are exploiting.

### **Own the Vulnerability; Don’t Blame the Threat**

Cyberattacks are very different from physical attacks. There are no unstoppable forces in cyberattacks. If you close the vulnerability, then you stop the curious teenager, the experimental

hacker, the cybercriminal and the information warrior. For example, for Stuxnet to succeed, it exploited a well-known, hard-coded password, and the fact that USB drivers were regularly used to transfer data to and from nuclear power plant control networks. Many attacks that include zero-day exploits often use well-known vulnerabilities as part of the overall attacks. Closing or shielding some well-known vulnerabilities would have made Stuxnet much less likely to succeed.

Because software and people will always be vulnerable (see Note 1), we will always need defenses to mitigate those vulnerabilities. However, in 2011, we are in one of those periods that occurs every five years or so (see Note 2), where the attackers find new levels of vulnerabilities to exploit, and the threats get ahead of the due diligence level of protection. When that happens, Type A organizations need to react quickly to upgrade defenses in a lean-forward manner, because they often have the most to lose, while Type B and C organizations will often only be able to take less stringent measures or wait for standard product offerings to offer more-effective capabilities (see Figure 1).

Starting at the bottom of Figure 1, the first step for all enterprises is to take measures to advance their due diligence level of security. Gartner recommends focusing on high-priority security controls (for example, the SANS Institute’s Consensus Audit Guidelines or the PCI Security Standards Council’s Prioritized Approach) and emphasizing improving the effectiveness of change control/configuration management, vulnerability management, intrusion prevention and privilege management processes. The high visibility and economic impact of the incidents at other companies can often be used to convince management to support more stringent policies and controls in these areas, with little need to increase budget. One important upgrade to these processes is moving toward more continuous monitoring versus yearly or quarterly auditing.

However, most Type A and many Type B enterprises will find that the risks to the business are too high to ignore, and they should take steps to “harden” their environments beyond the due diligence level. At this level, security information and event management (SIEM) products or other approaches that correlate information across defense “silos” should be used to gain better exception monitoring capabilities,

and new techniques — such as whitelisting and proactive application vulnerability testing prior to deployment — should be employed to deny advanced targeted threats the ability to install executables on servers and PCs.

Businesses and government agencies involved in critical infrastructure, high-tech or financial operations that are constant targets of cybercrime and other advanced threats need to add lean-forward capabilities to have continual visibility into potential attacks and compromises. The use of specialized threat detection, network forensics and situational awareness technologies can be very effective in quickly detecting and reacting to the first stages of an advanced targeted threat, but require high levels of skilled resources to be effective. The real key is avoiding as many attacks as possible, and more rapidly reacting to those that just can't be avoided.

### Evolve Defenses; Don't Just Add Layers

The best approach to reducing the risk of compromise is always "security in depth" — if you can afford it. Affording it means not just the money to buy increasing numbers of security products, but also the staff and operations support to use and integrate everything together. Having more security layers does not automatically mean more security. In the real world, many security

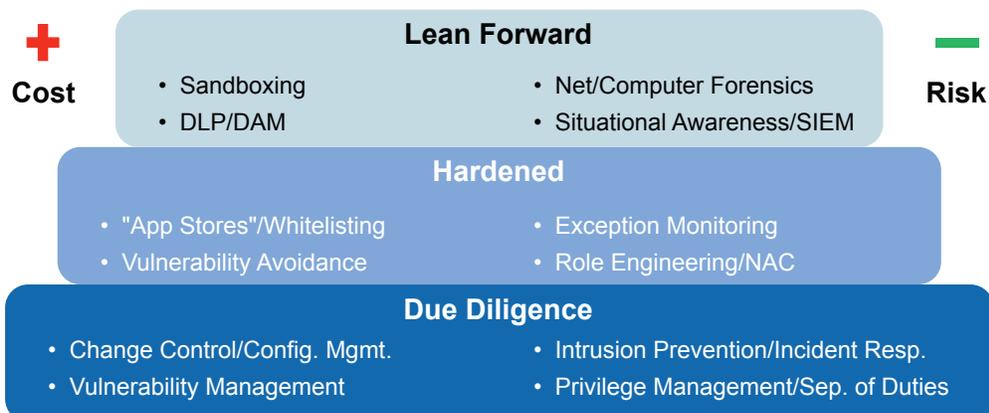
budgets do not support what translates into, "Keep spending on what you were spending on, and spend on more new stuff, too."

Moving up the layers in Figure 1 will reduce risk, but requires new or changed processes and controls. In addition to the monitoring capabilities of security controls, such as firewalls and intrusion prevention systems, we have listed the products loosely in order of increasing cost and complexity. Gartner considers the product categories listed at the top to be the main components of an active lean-forward, continuous monitoring program that, while increasing effectiveness against advanced threats, will also require increased resources and skill levels. Tools further down the list generally will require higher investments in acquisition and staffing, but will also provide a higher payoff in the effectiveness of detecting advanced threats, and support more rapid tuning or enhancement of network-based security controls.

A lean-forward, continuous monitoring process includes the following steps:

1. Establish a baseline.
2. Update threat information.
3. Monitor and inspect network traffic and host logs.

**FIGURE 1** Realistic Approach to Neutralizing Advanced Targeted Threat Impact



**Minimize vulnerabilities and attack apertures, make sure the business can still operate — and then focus on the threat.**

4. Investigate possible threat activity.
5. Activate an incident response process, or update defenses or work-arounds.
6. Go to Step 1.

All the lean-forward tools discussed will be available as point products, but subsets of their functionality will be absorbed into other network security platforms and will be “good enough” for many. For example, most SIEM and next-generation firewall products have added some of the flow analysis features of network behavior analysis. Leading Web security gateway and next-generation firewall vendors are adding reputation services, application awareness and other features of specialized threat-detection products. Many advanced vulnerability testing products are adding “seek, refine, repeat” functions that provide some aspects of penetration testing. The digital forensics area (computer plus network forensics) will likely stay in its own market, but many features will be available from SIEM products.

### Focus on Security, Not Compliance

There is a big difference between compliance and security. We’re using the term “due diligence” from the viewpoint of your customer: Did you protect your customer’s data well enough to look him in the eye and honestly say, “We did the best we could”? Due diligence from a compliance point of view is simply limiting your company’s liability from legal action — it is never the answer to dealing with advanced threats.

#### Note 1. Key Issues in Addressing Advanced Threats

Because enterprises can never completely avoid vulnerabilities, the Recommended Reading section points to a number of Gartner documents that detail other key security capabilities. Future Gartner research will expand on this area.

Conversely, security through stasis is never the answer. We could avoid the next major terrorist attack by never allowing planes to fly, but that wouldn’t help the economy. Security must support the business need, and businesses invariably need flexibility and change. A lean-forward approach to security is going beyond the due diligence level of the standard network security and vulnerability assessment controls, and using tools and processes to continuously look for active threats on your internal networks. However, you must be prepared to invest in and staff lean-forward processes — and you must be prepared to take action if you find something. Although ignorance is no excuse, being found to have explicit knowledge of security deficiencies and allowing an incident to occur can result in being found liable for more than just the direct damage.

### Starting Points

To ensure that your business is protected from advanced targeted threats, you must first start from a solid baseline: What is your current level of security program maturity in dealing with standard levels of attacks? Where gaps are identified that require an upgrade or a change to security processes and controls, incorporate some of the lean-forward capabilities (through products or services) detailed here to evolve your security defenses to get ahead of (or at least stay even with) evolving advanced targeted threats.

#### Note 2. Periods of Vulnerability

From 2001 through 2003, worms that exploited vulnerabilities in Microsoft Windows got ahead of protection, driving advances in intrusion prevention systems, just as in 1995, advances in macroviruses drove advances in antivirus protection, and phishing attacks in 2006 drove advances in email security. The same thing is happening today with advanced targeted threats, leading to advances in anti-malware, intrusion prevention and network forensics.

---

## About FireEye

---

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as traditional and next-generation firewalls, IPS, antivirus and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.



For more information, visit [www.fireeye.com](http://www.fireeye.com)