BLUE COAT®

# 5 STEPS FOR STRONGER ADVANCED THREAT PROTECTION

## HOW TO DEEPEN YOUR DEFENSES AGAINST ADVANCED THREATS BY LEVERAGING YOUR EXISTING SECURITY SOLUTIONS AND EXPLORING OPPORTUNITIES TO CLOSE GAPS

BLUE COAT®

Security Empowers Business

# INTRODUCTION

Security technology is increasingly sophisticated and continues to evolve quickly – so why do attacks still succeed with such alarming frequency? The Heartbleed vulnerability and the Target data breach are just two of the latest incidents that underscore a harsh reality: The threat landscape too is evolving quickly. Today's network-based advanced threats are more diverse, more numerous, more refined, more targeted, and more persistent than ever before. At the same time, businesses are embracing new technology advances to enhance product offerings, improve customer experience and increase productivity. IT teams must transform their approach to empower the business.

Businesses that strive to strengthen their defenses against advanced attacks must address two key questions: **How to maximize the value** of the security systems and solutions they already have in place; and **which other technologies and approaches** could deliver more comprehensive and effective protection moving forward.

This paper outlines positive steps your organization can take to defend against advanced threats.

### Five Steps

**#1: Understand the scale of today's advanced threats**

**#2: Measure and monitor the effectiveness of your current security**

**#3 Leverage your vendor's expertise to optimize your current installation**

**#4: Take a network-based approach for 20/20 visibility into all threats**

**#5: Implement a lifecycle defense, not piecemeal solutions**

## #1: Understand the Scale of Today's Advanced Threats

When considering how to address today's advanced threats, a natural first question is "How serious is the problem?" It is easy for organizations to make one of two mistakes in sizing up the threat landscape: underestimating the scale of the risks and under-preparing for real issues that arise; or overestimating the scale and over-investing in security solutions and resources. In both cases, the real issue is that **organizations often don't actually trust the security solutions they have put in place**.

A common symptom is under-reacting when alerts are issued. In the words of Gartner analyst Avivah Litan, "I have heard several times and from several sources that in the case of each large breach over the past few years, the alarms and alerts went off but no one paid attention to them."[1] This was largely the case with the Target data breach in 2014, according to a report issued by the U.S. Senate Committee on Commerce, Science, and Transportation in March, 2014. Too many alarms and alerts caused complacency, and in the end 40 million credit card numbers were compromised.

Other organizations over-react to incidents because they don't understand the full context. For example, in 2011 the U.S. Department of Homeland Security notified the Economic Development Administration (EDA) that there was a possible malware infection within the agency's systems, and in response the EDA destroyed not only uninfected desktop computers but also printers, cameras, and keyboards. Millions of dollars of equipment was unnecessarily destroyed.[2]

Therefore it is incumbent on every organization to understand not only the big picture of the threat landscape, but also their specific threat profile given the size, scope, and nature of their operations. Here are a few facts to provide context in understanding the actual depth and breadth of today's advanced threats:

[1] "Major companies, like Target, often fail to act on malware alerts", Computerworld, 3/14/14
[2] Source: www.arstechnica.com, July 8, 2013.

- **Traditional, mass-market cyber attacks still need to be dealt with.** Familiar exploits such as worms, Trojan-horse attacks, viruses, spyware, botnets, phishing, baiting, buffer overflows, and SQL injections are still out there. Traditional security solutions such as anti-virus software, firewalls, intrusion prevention systems (IPS), and secure web/email gateways typically provide an excellent front line of defense, but many of these attacks are evolving and still succeed.
- **New advanced threats are emerging.** Attackers are using a full spectrum of intrusion technologies and techniques, often exploiting unreported vulnerabilities in operating systems and applications. For example, *VM-evasive* threats are designed to evade virtualized resources such as traditional sandbox appliances; *zero-day threats* attack an OS or application vulnerability that is unknown to the general public; *polymorphic threats* continuously change, making it impossible for traditional signature-based security defenses to detect; and *blended threats* employ multiple attack vectors (paths and targets) and multiple types of malware to disguise the attack, confuse security analysts, and increase the likelihood of a successful data breach.
- **Malware is dramatically on the rise.** More than 200,000 new malware samples are discovered every day, according to Kaspersky Lab, and Blue Coat estimates that nearly two-thirds of cyber attacks originate from malware delivery networks (malnets). And new malware attacks are often successful: 90% of companies reported a security breach in the last 24 months, according to the 2013 Ponemon Report.
- **Encryption technologies such as SSL/TLS hide security threats.** Many threats today are encrypted via SSL (also known as HTTPS or TLS), thus hiding malware from many solutions. Encrypted SSL traffic now represents 15-25% of all outbound web traffic and up to 40% of production web traffic, but 80 percent of defense-in-depth systems do not inspect encrypted traffic, according to Gartner.[3] Even if you've decided to implement a solution, such as an SSL visibility appliance, there is still a question of where to deploy it for maximum effectiveness, while adhering to corporate and legal privacy policies.
- **Mobility adds a new dimension to advanced threats.** Mobile threats represent a growing percentage of overall traffic[4]. CIO Magazine reports that there are over 1 million malicious and high-risk Android apps. And most people unknowingly do things on their mobile devices that make them susceptible to fraud, identity theft, and data loss.
- **The window of opportunity for advanced threats is wider.** According to the 2013 Verizon Data Breach Report, 84% of advanced persistent threats (APTs) took only seconds, minutes, or hours to compromise their targets, while 78% of breaches took weeks, months, or years to discover.
- **There are more types of attackers.** Today's cyber attackers aren't just kids on a lark. They fall into three broad categories: cybercriminals who hack for profit (a multi-billion-dollar business today); state-sponsored hackers who hack with the objective of compromising data or sabotaging systems; and hacktivists, or computer hackers driven by political ideology.

## #2: Measure and Monitor the Effectiveness of Your Current Security

Once you understand the scope of the advanced threats your company must defend against, you need to determine whether additional threat detection and protection is required. The key is measurement and tracking. You need to establish meaningful metrics for evaluating the effectiveness of your security solutions, and measure them constantly and consistently.

A good starting point is to quantify your success in defending against malware, and this begins with understanding how your workforce is interacting with the Internet each day. Consider a day in the life of just one large financial services enterprise, with 250,000 employees worldwide. The company began measuring and discovered that every single day, on aggregate, its workforce makes **660 million attempts** to access websites. Of those, 2.2 million attempts are blocked by its global intelligence system as known malicious sites. In addition, **244 malicious files** are blocked by network perimeter anti-malware.

Also, make sure you know when systems are infected, and which ones. A "Potentially Infected Clients" report, which is typically available through malware protection systems, will tell you how many devices have needed remediation over a period of time (and alert you to the systems that are attempting to send out confidential or proprietary information). Monitor this to see if your rate is increasing or decreasing

[3] Gartner Report: Security Leaders Must Address Threats from Rising SSL Traffic, December 2013.
[4] Blue Coat report: Blue Coat Systems 2013 Mobile Malware Report, February, 2013

over time, so you can make better decisions about when to invest in additional malware protection solutions.

Similarly, make sure you're taking advantage of bandwidth usage monitors in your existing security solutions. If bandwidth usage increases dramatically, it may be a sign that users and/or malware are getting around your policies and controls.

The number and urgency of alerts should also be closely monitored and reported. If you have too many alerts, staff may become complacent – or they may not know how to triage to filter out false positives and ensure that the most important alerts are investigated.

In addition, it's important to know exactly how many applications are running on your network – and whether or not they're approved for use on the network. The more applications you have running the higher the likelihood that you'll be victimized by an advanced threat – because many applications contain vulnerabilities that attackers can exploit remotely. By closely monitoring your applications you'll be better equipped to defend against corresponding vulnerabilities. And when you see an application that has no business being there, you may be identifying an attack that's already in progress.

Equally important, it pays to quantify the true costs of a breach for your organization. Include both hard-dollar and soft-dollar costs such as:

- Investigation and forensics costs
- Customer and partner communication costs
- Public relations costs
- Lost revenue due to damaged reputation
- Regulatory fines and civil claims
- Opportunity costs and missed sales due to outages

## #3 Leverage Your Vendor's Expertise to Optimize Your Current Installation

Your internal security and IT teams may have experience and expertise installing advanced threat protection solutions. Your vendor's consultants have more. Harness their knowledge to make sure that your solution is installed and configured properly so that you can optimize your investment from day one.

For example, if you've purchased a solution that takes advantage of a global intelligence network, such as Blue Coat's, your vendor can help you fully tap into the depth and breadth of the "network effect." With assistance from the vendor you can harness the shared intelligence to discover new malware, malnets, threats or malicious files, and share that intelligence throughout your local infrastructure and global community. The result will be faster protection against advanced targeted attacks and zero-day malware.

In the process, your vendor can help you maximize the benefits of innovations in sandboxing; a solution that tricks malware into thinking it's in your production environment, automates risk scoring using behavior-based pattern matching to rank threats, and adds your own custom malware pattern detection. Vendors can make sure your solution takes maximum advantage of capabilities, such as the ability to direct files to one or more malware sandbox appliances and pre-filter "good" and "bad" files to improve performance. These capabilities keep you a step ahead of malware exploits – always just a little smarter.

Your vendor can also help you with specific installation and configuration tasks such as:

- Selecting the optimal number and type of physical and/or virtual appliances.
- Determining where to install your appliances to capture the most important traffic.
- Using network Taps and network packet brokers (NPBs) to aggregate traffic from multiple network segments and direct it to your security analytics appliances.
- Configuring reports that satisfy IT management and the demands of external security auditors.
- Discovering and establishing baseline reports, to help alert when anomalies occur later.
- Leveraging reputation-based blacklists to alert upon identification of traffic associated with known-bad IP addresses, known-bad URLs, or malware-infected files.
- Configuring an advanced threat protection system to automatically ship suspicious files off to internal and/or external advanced malware analysis (sandboxing) systems.

- Establishing whitelists so that files known to be free from malware are cleared from analysis.
- Constructing policies that help IT monitor and enforce your organization's acceptable-use policies.
- Ensuring that your security analytics appliances don't miss hidden threats embedded within Secure Sockets Layer (SSL)-encrypted communications.
- Showing you how to identify network anomalies that may lead to advanced threats.
- Showing you how to investigate the causes and effects of a reported cyber attack, discover the extent of damage, and determine whether the attack is still underway.
- Preserving digital evidence that law enforcement can use to prosecute cybercriminals.
- Integrating your security analytics solution into your existing security ecosystem for comprehensive advanced threat protection – from enforcement, to assurance, and to remediation.

In short, the relatively small expense of leveraging the vendor's expertise is usually an excellent investment. After all, you've made a significant investment in hardware and software; make sure you're getting the most out of it.

## #4: Take a Network-based Approach for 20/20 Visibility into All Threats.

Visibility is vital for an effective defense against advanced threats – particularly **network** visibility. The more visibility you have into your network traffic at all phases of the lifecycle, the more you can analyze, understand, control, and remediate issues and incidents.

That is why it is so important to take a network-based approach to advanced threat protection. With network-based anti-malware tools you get full visibility into all inbound traffic; you can analyze it and filter out malicious content before it arrives at the endpoint; and you can increase coverage and catch more malware (by using multiple anti-malware engines at the network level). The key elements of a network-centric approach include:

**1. Blocking all known threats at the network gateway to minimize alert overload.**
This is what secure web gateway products do, and your secure web gateway solution should provide broad and sophisticated capabilities such as:

- **Visibility into SSL traffic.** SSL encryption protects the privacy of network-based communications. But it is also used by hackers to mask advanced threats. To identify hidden threats, you need complete visibility into the SSL traffic. The big question for many companies is where to deploy decryption to maximize efficiency. Companies are starting to deploy SSL visibility appliances for ALL traffic across the WAN, enabling their network gateway firewall, IPS, and IDS solutions. Many are already utilizing solutions such as Blue Coat ProxySG to selectively decrypt web traffic. To comply with local privacy regulations that protect certain classes of data – such as financial or health-related – you need to be able to selectively decrypt network traffic according to your policy needs.
- **True Termination of all network requests (proxy).** Proxying all network requests guarantees that threats will be unable to tunnel their way into your network. From the U.S. Senate "Target Kill Chain Analysis" Report[5]; "Another protective step at this phase would have been strong firewalls between Target's internal systems and the outside Internet (e.g., routing traffic through a proxy) to help disrupt the attacker's command and control. Target could also have filtered or blocked certain Internet connections commonly used for command and control."
- **Whitelisting, or allowing the "known good."** Whitelisting is simply maintaining a registry of approved files that have been granted permission by an administrator. Whitelisting can be provided by a content analysis system. This type of solution works in conjunction with secure web gateway products, such as the ProxySG appliance, to provide extra layers of protection. A good content analysis system can also increase the performance of anti-malware scanning and sandboxing by eliminating the need to analyze known "good" files as well as known "bad" files. If a file is on the whitelist, it will be delivered to the requester and no further processing is needed. The whitelisting can also improve security even further by preventing users from

[5] The United States Senate, Committee On Commerce Science & Transportation, Majority Staff Report for Chairman Rockefeller, March 26, 2014, http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf.

downloading specific file/data types that are not on the whitelist. A good example would be blocking any .exe files that are not known good files.

- **Malware scanning to block the "known bad."** The combination of a good secure web gateway appliance and a content analysis system with malware scanning and whitelisting can block all known threats, sources and signatures and direct truly unknown content for malware analysis. Ideally, content analysis systems should harness – and contribute to – intelligence gathered worldwide from a wide variety of sources, such as WebPulse, a part of the Blue Coat Global Intelligence Network. This creates a network effect or multiplier for the discovery of new malware, threats or malicious files, and the shared intelligence translates to faster and better protection against advanced targeted attacks and zero-day malware.

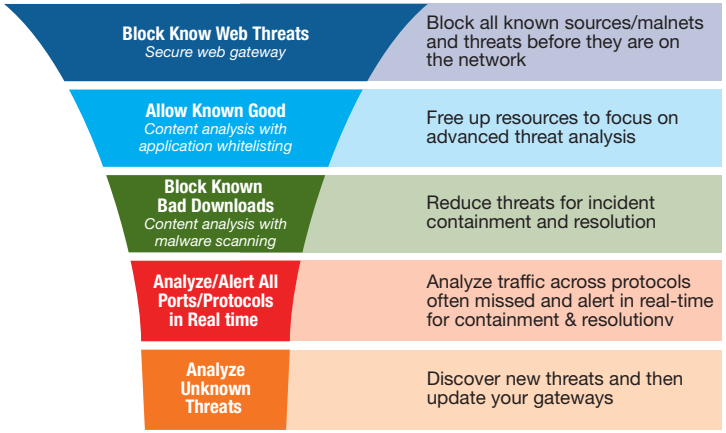


Figure 1: A network-based approach provides a funnel for dealing with known and unknown advanced threats.

### 2. Continuous monitoring of network traffic

- Analyze real-time network traffic across all ports and protocols with predictive alerts and prioritized risk scoring on zero-day threats, APTs, encrypted threats, spear phishing, malicious behavior, botnets and targeted attacks on process.
- Monitor suspicious outbound traffic through the web gateway to identify potential leakage of sensitive information and 'phone home' activity.

### 3. Using Sandboxing to Protect against *Unknown* Threats and Contain Incidents

Defending against unknown threats requires malware analysis sandboxing to understand the threat and contain incidents. Sandboxing limits the environments in which code can execute. It isolates an application to prevent malware, intruders, system resources, or other applications from interacting with it. Effective advanced threat protection solutions use sandboxing tools to discern malicious behavior patterns in unknown and suspicious files, and they share results among multiple security entities so that once malware is identified, further downloads can be blocked at the web gateway.

Keep in mind that not all malware may be equally malicious given your specific environment. You should look for behavior-based malware classification patterns – not code-based signatures – to flag events based on potential malicious activity which provide risk scoring, either out of the box or customizable based on criteria you set yourself. And take a close look at the quality of information generated by the sandbox. Look for rich forensic intelligence, risk scores for threat prioritization, and a range of post-analysis resources so you can respond faster and more effectively to attacks.

### 4. Resolving Incidents through Threat Profiling and Eradication

Breaches that do occur must be quickly investigated, analyzed, and remediated, and the resulting intelligence should be shared via a global intelligence network. Some of the specific product attributes and capabilities to look for in this area include:

- **Retrospective analysis:** To resolve incidents quickly and effectively, you need the ability to see exactly what happened: when, where, how, and to whom. Think of it as having a DVR for network traffic. You can stop, rewind, watch in slow motion, and understand precisely what took place. With retrospective analysis capabilities you can identify the advanced and targeted attacks that slip past traditional security tools and take action to resolve issues and prevent future occurrences.
- **Detailed reporting:** This includes views of user activity, web usage patterns, application access, video usage, blocked sites, sites accessed by category, time of day, length of time, and so on – so you can troubleshoot threats, track dangerous user activities, conserve bandwidth by identifying abuse patterns, and report on web usage by

user, group, location, URL, and more. You also need detailed reporting to help you verify the performance of business-critical applications (by site and across your enterprise), discover unauthorized applications, and identify the causes of performance problems.

- **Security analytics:** This provides a way to bridge the gap between prevention and preparedness. Security analytics can analyze network traffic to help prevent basic, known attacks from occurring; equally important, they can help organizations prepare for advanced and unknown attacks that occur – so that companies can resolve issues quickly, learn from incidents, and apply new intelligence so that future attacks do not succeed.

## #5: Implement a Lifecycle Defense, Not Piecemeal Solutions.

Among forward-looking enterprises, there is a shift underway from the traditional attack prevention mode to a **lifecycle defense** that *integrates* security solutions to provide more effective attack detection, preparedness, and response – including prevention.

This shift requires a new closed-loop process to security technology – a more integrated approach that not only blocks known exploits but also tells you the *how, what, where, when* and *why* of advanced targeted attacks and security breaches – all while delivering end-to-end visibility of data exfiltration and malware infiltration on the network.

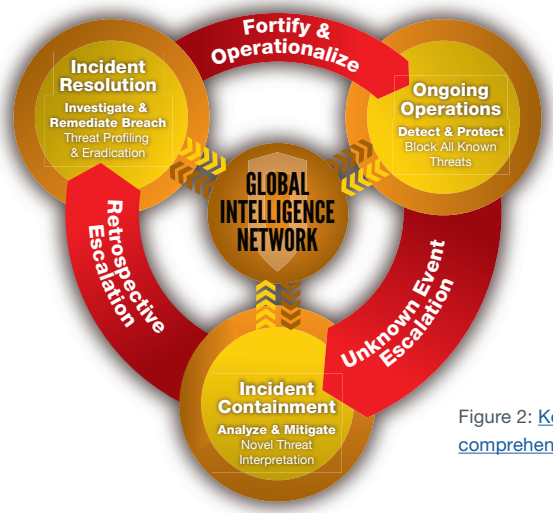


Figure 2: Key elements of a comprehensive defense.

The lifecycle defense encompasses detecting and blocking known threats in ongoing operations; analyzing unknown threats and containing incidents that do occur; and investigating, remediating and resolving breaches retrospectively.

For example, many companies are finding that they need multiple web access logs – using multiple protocols (HTTP, HTTPS, streaming media, SOCKS, etc.) so they can institute a continuous process for operations and security. With a lifecycle defense, they can implement a variety of standard web access context logs, provide full capture data, and tune additional security logs to vector in on what might try to hide in the ocean of data.

In addition, the lifecycle defense leverages the network effect by sharing threat intelligence from enterprises and users worldwide. For example, WebPulse harnesses the data of more than 75 million users, recognizes and understands more than 50 languages, and utilizes a combination of traffic, content and reputation analysis of real-time requests to build a comprehensive view of the web-based malware ecosystem. This results in WebPulse blocking over 3.3 million threats from over 1 billion web rating requests per day.

Blue Coat provides an online interactive checklist tool, where you can consider the top 10 questions to ask when designing an adaptive, lifecycle defense against advanced threats, along with the key areas to address at each phase of the lifecycle.

## Don't Just Focus on the Dangers. Consider the Possibilities.

Security risks have multiplied over the past few years, but we've also entered an era of unprecedented opportunity and innovation. Advanced threat protection solutions can defend us against the dangers of sophisticated attacks, but they can also be a catalyst for achieving new levels of productivity, efficiency, creativity, and collaboration.

We urge you to think about advanced threat protection – and security in general – in a whole new way: in terms of empowerment. This new approach will help you see business value you may have missed. It will allow you to recognize opportunities to liberate rather than constrain employees. And it will help you attain something you never expected from security technology: peace of mind.

For additional information about Blue Coat solutions for advanced threat protection, please visit us at http://www.bluecoat.com/atplifecycle.

BLUE COAT®

Security Empowers Business



v.WP-5STEPS-FOR-STRONGER-ADVANCED-THREAT-PROTECTION-EN-v2b-1014

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000