BLUE COAT®

REVOLUTIONIZING ADVANCED THREAT PROTECTION

HOW TO BEAT ADVANCED THREATS WITH AN INTEGRATED APPROACH TO SECURITY VISIBILITY, ANALYTICS, THREAT INTELLIGENCE, AND ENFORCEMENT

BLUE COAT®

Security Empowers Business

INTRODUCTION

Today's threat protection paradigm is broken. Most organizations rely on signature-based tools to block attacks at the network perimeter, and security information and event management (SIEM) products to provide incident resolution. But today's attackers have found too many ways to evade signature-based products, and SIEM products cannot pin-point successful attacks until after they have inflicted considerable damage. As a result, it seems that every week another major company sees its reputation destroyed by a major data breach.

This paper presents a new framework for defeating advanced cyberthreats. It discusses:

- The problems with relying on signature-based security tools and conventional security information and event management products.
- A framework that integrates security visibility, security analytics, detection of zero-day threats, and blocking and enforcement solutions for combatting advanced threats.
- A three-stage model of an advanced threat protection lifecycle defense, implemented with products and services from Blue Coat.

Weaknesses of Today's Information Security Defenses

News outlets are filled with stories about massive thefts of personally identifiable information, stealth attacks on intellectual property, and disabled web sites. The costs for victimized enterprises range from damaged brand reputation, to loss of competitive position, to millions of dollars in regulatory fines and data breach notification expenses.

Often it appears that the bad guys are winning an arms race by continuously introducing new ways to overcome traditional information security defenses. These defenses are vulnerable because they rely on a signature-based, prevention-only "picket fence" security model.

Attacks evade signature-based tools

Most enterprises employ a variety of signature-based security tools like next-generation firewalls (NGFWs), intrusion prevention systems (IPSs), data loss prevention (DLP) tools, and host antivirus packages to identify known threats in network traffic.

But attackers have developed many techniques to evade signature-based tools, including:

- Blasting out unknown and next-generation malware in zero-day attacks that penetrate networks before signatures can be created and distributed.
- Targeting individual organizations with customized malware for which no signatures exist.
- Using social engineering and spear phishing techniques that fool employees into helping the attacker circumvent defenses.
- Concealing attacks in SSL-encrypted traffic (which now makes up 30%-40% of all Internet traffic) that can't be deciphered by IPS and web gateway defenses.
- Using encryption, compression and morphing tools to hide malware from antivirus programs.
- Embedding malware in otherwise useful apps and games.
- Broadening the attack surface; that is, finding vulnerabilities in additional types of endpoints such as mobile devices and industrial control systems.

The vast majority of information security experts now agree that signature-based defenses alone are unable to stop today's most serious advanced threats.

> "[Signature-based detection is] still an integral part [of malware defense], but it's not going to be the only thing. We need to move away from trying to build Maginot lines that look bulletproof but are actually easy to get around."
>
> *Nicolas Cristin, Carnegie Mellon University*, quoted in The Antivirus Era is Over

SIEM Products Don't Provide Enough Context

Most enterprises have recognized that some attackers will break through the network perimeter, and have implemented security information and event management products to identify breaches and their causes. Unfortunately, SIEM products have severe limitations.

Many SIEM products cannot process the massive volume of security events created by today's networking and security systems and end user devices. To compensate, they work with only samples or summaries of log data. This means that security analysts and incident responders have incomplete visibility into the sequence of actions that make up advanced attacks, making them much harder to identify.

In addition, SIEM products also have a limited ability to reconstruct the complete context of attacks. They can evaluate event and log data from security and network devices, but they cannot correlate it with emails, malicious files and web sites that are involved in advanced attacks, or help analysts connect events that are spread out over long periods of time.

Point Security Tools are Not Integrated

In many enterprises, a lack of integration between point tools prevents security organizations from detecting and analyzing ongoing attacks. New malware types uncovered by an analysis product may not be visible to blocking tools without time-consuming manual steps. Clues to multi-stage attacks collected by various security systems are not shared, so security analysts have no place to make correlations and detect patterns that would reveal the actions of attackers. Threat intelligence is not shared efficiently among enterprises, leaving them exposed to zero-day malware and new threat types.

Slow Responses Increase Risks and Breach Costs

Fast detection and response can stop advanced attacks before they cause damage, or minimize the amount of intellectual property and protected personal information attackers are able to extricate from the organization. Unfortunately, according to the Verizon 2014 Data Breach Investigation Report, 68% of web app attacks take weeks, months or years to discover, even though in 69% of the cases stolen data was extricated in minutes, hours or days. Of financially motivated web app attacks, 88% were discovered by outside parties (such as customers, fraud agencies and law enforcement) rather than the organization that was attacked.

This is strong evidence that today's methods are failing to detect and contain attacks in an acceptable timeframe.

> "We cannot assume we can stop the attackers, so we have to plan for compromise. The difference between success and failure breaks down to how quickly you can isolate the attack, contain the damage, and then remediate the issue."
>
> *Mike Rothman, President of Securosis*, in Applied Network Security Analysis: Moving from Data to Information

A Framework for Advanced Threat Protection

But the arms race is not lost. Several advances in security technology give enterprises and government agencies hope for staying ahead of attackers. These include:

- Tools that give enterprises complete real-time visibility into ongoing attacks and extensive contextual data for incident response and post-breach analysis.
- New security analytics products that allow enterprises to expedite the discovery of security breaches and remediate even the most sophisticated attacks.
- Security technologies that use behavioral analysis and dynamic analysis ("next-generation sandboxing") to detect advanced malware for which no signatures exist.
- Cloud-based threat intelligence networks and knowledgebases that speed up the dissemination of real-time threat data so enterprises can "inoculate" themselves as soon as new attacks appear.

BLUE COAT®

Security Empowers Business

- Integration of these components with existing blocking and analysis tools to create a security ecosystem that offers comprehensive security against advanced threats.

These advanced capabilities can be integrated into an advanced threat protection framework (Figure 1). This framework allows organizations to detect and block more attacks and respond more quickly to breaches.

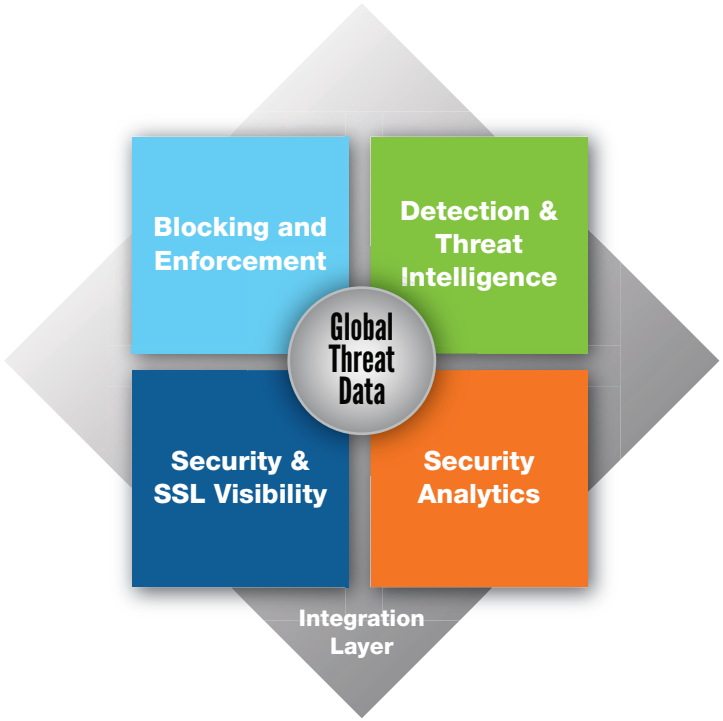
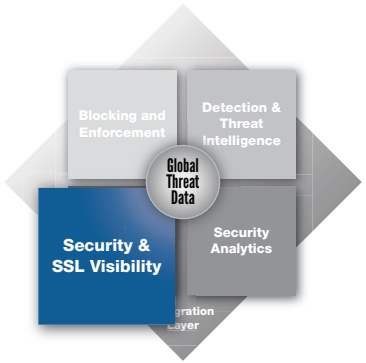


Figure 1: A framework for advanced threat protection

Security and SSL Visibility

Security visibility is a critical requirement for Advanced Threat Protection. Threat-blocking tools such as NGFWs, IPSs and host antivirus solutions are only effective when they can inspect all of the network traffic entering and exiting the enterprise. Also, security analytics, impact analysis and incident resolution require a complete record of network traffic and all related security data so they can perform comprehensive real-time and back-in-time analysis.



To prevent blind spots, a successful advanced threat protection solution must be able to:

- Decrypt encrypted network traffic, particularly SSL.
- Capture all network traffic, across all major protocols, without any loss of data through sampling or summarization.
- Recognize everything that crosses the network, both as network packets and as higher-level elements such as files, email and instant messages, application traffic and security events.
- Capture and store weeks, months or more of historical data.
- Extract, index and classify metadata efficiently so that historical analysis can be performed quickly on massive volumes of data.

Unless all of these capabilities are available, downstream threat protection technologies and incident response professionals will not have the data they need to do an effective job of blocking known threats, analyzing unknown ones, and fully investigating breaches.

Big Data Security Analytics

Security analytics helps organizations derive actionable intelligence from massive volumes of security and network data.

Heuristic detection and correlation can identify files and events that resemble known malware and attack patterns. This helps defend against polymorphic malware that can't be detected by straight signature matching. Statistical analysis can detect suspicious variations in behavior, particularly network flows.

BLUE COAT®

Security Empowers Business

Security analytics also plays a major role in incident response, helping analysts identify indicators of compromise (IOCs) and understand the tactics, techniques and procedures of attackers. A security analytics solution can reconstruct attack activity in chronological order, including emails, chat, web, VoIP and other user sessions, with related text, images and associated files.

Reconstructing timelines this way gives security analysts invaluable tools to detect attacks as they are occurring and answer specific questions such as:

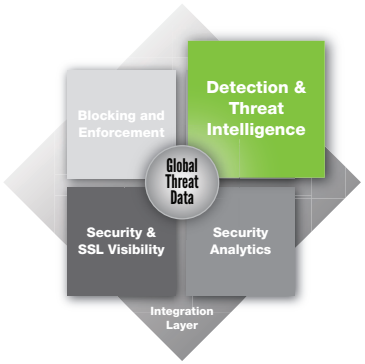
- Who is responsible and how did they do it?
- What systems were affected and what data was compromised?
- Is the attack continuing, and if so, how can we stop it immediately?
- Is the attack over, and if so, how can we prevent a recurrence?

A security analytics solution can also help analysts answer broad questions like:

- What attacks are most common, and which have been most successful?
- What systems are most vulnerable?
- Where are our security processes strong, and where are they weak?

Detection and Threat Intelligence

Many zero-day and advanced attacks use targeted or polymorphic malware that won't be detected by signature-based security tools.



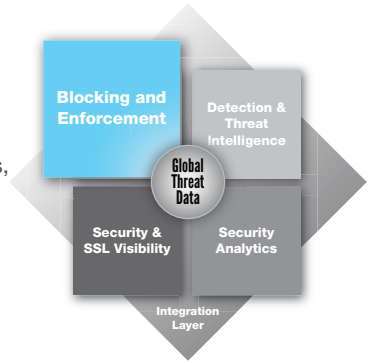
To detect malware in files for which no signature exists, many enterprises are deploying dynamic analysis technology that employs next-generation sandboxing. With sandboxing, files that have not been previously identified as good or bad are sent to execute in a protected environment. The solution records and analyzes malicious and potentially malicious behaviors, for example attempts to change registry keys, access security-related files, disable anti-virus packages, or "phone home" to a command-and-control (CnC) server on the Internet.

Signatures can be developed for files identified as malicious or suspicious. These signatures can be used to block any additional instances attempting to enter the network, and can also be shared with other enterprises through a global threat intelligence service.

In addition, the behavior of malicious files offers many clues about the methods, intentions and targets of the attacker. This information can be used by a security analytics solution to help reconstruct and reverse engineer advanced, multi-stage attacks.

Blocking and Enforcement

Most organizations have invested heavily in blocking and enforcement products, including firewalls, secure web gateways, NGFWs, IPSs, unified threat management (UTM) appliances, DLP systems, and network antivirus packages.



These products become more effective as part of an advanced threat protection environment, because:

- The security and SSL visibility products ensure that the blocking tools have no blind spots in network traffic.
- The security analytics tools help identify polymorphic malware and new attack patterns, so these can be blocked in the future.
- Detection and threat intelligence technology detects previously unknown types of malware, so signatures can be developed to block that malware.

Integration Layer and Global Threat Data

In an advanced threat protection framework an integration layer provides an extensive set of connectors and integration tools so security information can be shared quickly and reliably among security

BLUE COAT®

Security Empowers Business

products. This ensures that once new malware and attack patterns have been recognized, signatures are immediately available to blocking and enforcement products, including, secure web gateways, NGFWs, and DLP systems. It also means that alerts from those systems can be sent to a security analytics solution, so analysts can pivot on an alert and reconstruct the sequence of events occurring during and after the attack, to determine its source and full scope.

Information sharing becomes even more powerful when the enterprise can access a cloud-based global threat database. This allows organizations to share threat signatures and URL reputation data so they can block malware and traffic to and from web sites used by cybercriminals, botnets, spammers, and state-controlled attackers.

Tapping security data from thousands of organizations and millions of users creates a network effect that is critical for allowing enterprises to inoculate themselves against zero-day attacks and targeted attacks as soon as these are identified “in the wild.”

An Advanced Threat Protection Lifecycle Defense

The advanced threat protection framework discussed so far gives enterprises the tools to implement a complete, smooth-flowing advanced threat protection lifecycle defense.

The next four sections of this white paper discuss the stages of a lifecycle defense and how each of them can be implemented with products and services from Blue Coat.

The stages of the lifecycle defense, together with selected Blue Coat products, are shown in Figure 2.

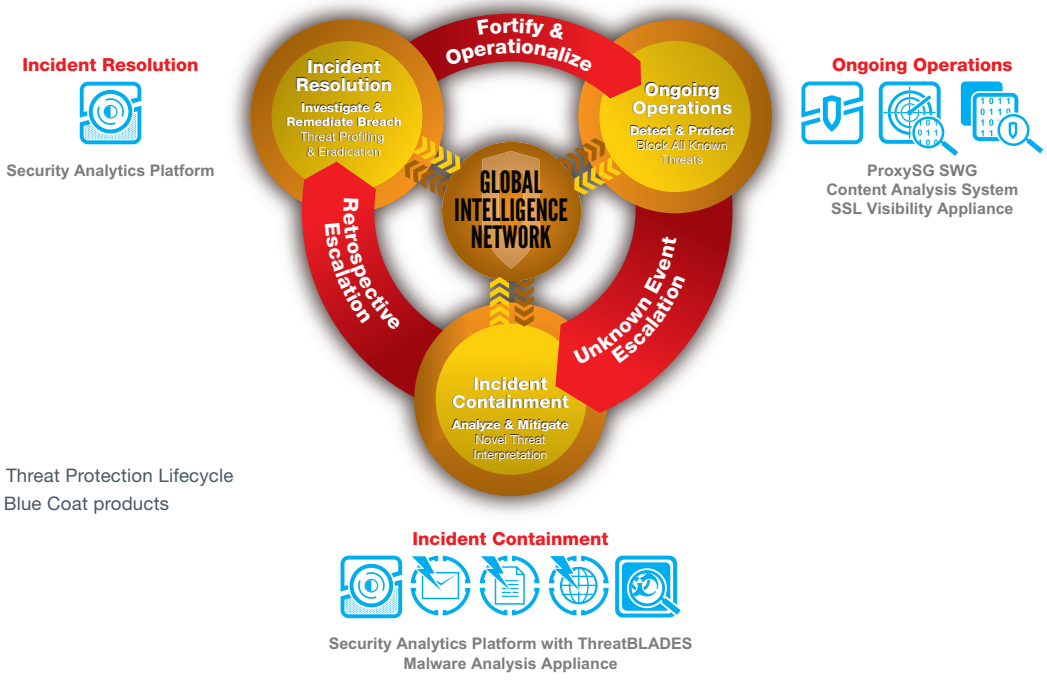


Figure 2: An Advanced Threat Protection Lifecycle defense, with selected Blue Coat products

BLUE COAT®

Security Empowers Business

Ongoing Operations

Ongoing Operations, the first stage of the advanced threat protection lifecycle defense, focuses on the detection and blocking of known threats. Most of the activities in this phase are carried out by technologies that belong in the Security and SSL Visibility, and Blocking and Enforcement sections of the advanced threat protection framework discussed earlier.

One key activity in this stage is decrypting and managing encrypted network traffic so all of it can be inspected.

This is followed by inspecting traffic for known malicious networks, malware and other known threats, and then blocking unwanted traffic and files.

A further set of actions can involve escalating unknown files for dynamic analysis and alerting security operations center (SOC) and incident response staffs of suspicious activities.

The Blue Coat products and services that are most important in the Ongoing Operations stage of the lifecycle defense include;

Blue Coat SSL Visibility Appliance: This is a highly efficient device for decrypting and managing SSL traffic so its contents can be scanned by multiple security tools, including NGFWs, secure web gateways, IPSs and security analytics tools. It can perform policy-based decryption on inbound and outbound SSL traffic arriving and leaving via any port and any protocol, not just HTTPS on port 443, and can be deployed inline or out of band. It also allows administrators to specify what traffic should not be decrypted, so they can comply with data privacy regulations.

Blue Coat ProxySG appliance and Secure Web Gateway Virtual Appliance: These are recognized as the world's leading secure web gateways. Besides providing critical web security features, such as user authentication, web filtering, data loss prevention and bandwidth management, they can be used to detect known malware networks (malnets) and enforce web acceptable use policies.

Blue Coat Content Analysis System: This appliance integrates with the ProxySG appliance to orchestrate malware scanning and application whitelisting. It uses single or dual anti-malware engines to block known threats, based on a database of over 1 billion records. It includes a broker feature to send unknown suspicious content to analysis and sandbox tools for deeper study, including the Blue Coat Malware Analysis Appliance and third party sandbox products. It can reduce files sent to the sandbox by 37% by filtering out known good and bad files, decreasing the number of sandbox appliances needed.

Incident Containment

Incident Containment, the second stage of the advanced threat protection lifecycle defense, focuses on the automated analysis of zero-day threats and prevention of additional damage. Most of the activities in this phase are carried out by technologies that fit in the Security Analytics, and Detection and Threat Intelligence sections of the advanced threat protection framework.

One key activity in this stage is "detonating" unknown files in an isolated environment (a sandbox) and monitoring their actions. This stage not only identifies previously unknown malware, it also produces a detailed record of malicious actions, so analysts can understand the behavior of the attack and the intensions of the attacker.

Sources of potentially unknown files can include web, email and file transport protocols, so it's important that all sources are scanned for advanced, zero-day malware.

A second activity involves reconstructing the attack in order to identify the systems that have been compromised and the data that has been accessed.

Analysts and administrators are then able to patch vulnerable systems, update configurations, and take other actions to prevent reinfection and block new instances of the same and similar attacks.

The Blue Coat products and services that are most important in the Incident Containment stage of the lifecycle defense are:

Blue Coat Malware Analysis Appliance: This next-generation sandboxing device can rapidly assess large numbers of unknown files and URLs for indications of malicious activity. It "detonates" files in a secure, virtualized environment and records malicious and suspicious activities. Unlike other sandboxing tools, it uses multiple techniques to detect VM evasive malware, including kernel-level event detection and the ability to emulate user actions like mouse clicks. It provides the unique ability to replicate actual customer desktop "golden images," including custom applications, to detect application-specific attacks.

The Malware Analysis Appliance also provides risk scoring to separate high risk from low risk files, and alerting to warn security administrators and end users. Information from the malware analysis is automatically shared with ProxySG appliances so future instances of the identified malware can be blocked at the gateway, allowing all ProxySG customers to benefit from this intelligence.

Blue Coat ThreatBLADES: These software blades run directly on the Blue Coat Security Analytics Platform (which is discussed in depth below). Each ThreatBLADE is optimized to scan specific protocols, detect and extract files, URLs and IP addresses, inspect and categorize those files, URLs and IP addresses as known good, known bad (malicious), or unknown.

The ThreatBLADES alert analysts and administrators to the presence of known threats, and can send unknown files and URLs to the Malware Analysis Appliance for detonation and behavioral analysis.

- **The WebThreat BLADE** provides comprehensive protection against web-based threats. It detects and reports suspicious web sites in more than 100 different categories, and uses reputation data on URLs and IP addresses to identify network traffic originating from known bots, spammers, phishing sites, malware sources and compromised websites.
- **The MailThreat BLADE** provides in-depth protection against email-based threats. It extracts attached files delivered over all standard email protocols, and uses hashes to identify known good and known bad files.
- **The FileThreat BLADE** extracts and analyzes key file types, including Microsoft Office documents, Adobe Flash and PDFs, Java, EXE files, email attachments, Android APK files and web objects. It uses real-time analysis to detect malicious files, and reputation intelligence to identify recent file-based attacks and threats delivered over standard file transport protocols like FTP and SMB.

Incident Resolution

Incident Resolution, the third stage of the advanced threat protection lifecycle defense, involves the in-depth investigation of attacks and remediation of damage caused. The key tools in this phase fit in the Big Data Security Analytics section of the advanced threat protection framework.

Key activities in this phase include attack reconstruction and root cause analysis. These allow analysts and incident responders to determine the full source and scope of attacks and to identity the compromised systems and the exact intentions of the attackers.

To combat complex, long-lasting attacks, analysts must be provided with a complete set of data – not just packets, but also session flows, files, emails, and other artifacts and the results of sandboxing analysis. This data needs to be available for extended time periods, weeks or months. Also, the analysts need security analytics tools that can identify and extract information related to a specific indicator of compromise, for example, all emails, attachments and prior and subsequent traffic related to a piece of malicious malware.

The results are used to assess and quantify the damage caused by attacks, to clean up compromised systems, to update signatures and threat intelligence, to validate compliance to information security regulations, and to improve IT processes in order to prevent future attacks.

The Blue Coat product that is critical to the Incident Resolution stage of the lifecycle defense is:

Security Analytics Platform: This system records and classifies every packet that enters the network, even on today's fastest networks.

Deep Packet Inspection (DPI) provides visibility into all information in the captured packets from Layer 2 through Layer 7, and classifies over 1,800 applications and thousands of metadata details.

Session and application reconstruction convert traffic from raw packets to meaningful artifacts like files, emails, instant messages, VoIP conversations and application traffic. These artifacts can be scanned and analyzed by IPSs, anti-virus products and malware analysis tools, and can provide context to security analytics tools. The Security Analytics Platform can even identify and reconstruct complex PHP, Ajax and JavaScript files.

The Security Analytics Platform not only collects and stores complete security data, it also provides critical big data security analytics tools to correlate and process massive volumes of data in order to detect ongoing attacks and answer critical post-breach questions. Using data and tools provided by the Security Analytics Platform, analysts can apply what Blue Coat calls the "CRIME" Methodology and determine:

BLUE COAT®

Security Empowers Business

- The **Context** of a threat or breach – What happened before, during and after the attack?
- The **Root Cause** – Where did the attack originate and who was responsible?
- The **Impact** – What systems were affected, what data was compromised, what networks and users were affected, and what dangerous artifacts might still be on the network?
- **Mitigation** – What steps need to be taken to fix problems caused by the attack and prevent it from resuming?
- **Eradication** – What needs to be done to clean up remaining effects of the breach and prevent similar attacks in the future?

The Security Analytics Platform delivers enterprise performance and scalability, with full packet capture at up to 10Gbps. It can provide context to alerts received from NGFW, IPS, SIEM, DLP and malware analysis products. Deployment options include software, dedicated appliances and virtual appliances.

The Blue Coat Global Intelligence Network

At the center of the advanced threat protection lifecycle defense is the Global Intelligence Network, which shares threat data from thousands of enterprises.

By rapidly disseminating information on newly discovered malware, suspicious URLs and IP addresses, attack patterns and other threat data, a Global Intelligence Network can:

- Help block zero-day and targeted attacks at the gateway as soon as they appear in the wild.
- Provide analysts and incident responders with intelligence to analyze new threats faster and more accurately.
- Build up real-time white lists and black lists so there are fewer unknown files that need to be analyzed by anti-malware and sandboxing systems.

The Global Intelligence Network, powered by Blue Coat WebPulse collaborative defense, creates an ecosystem for collecting and sharing data from 75 million users at over 15,000 companies, together with leading technology providers and independent threat intelligence sources. It features threat labs staffed by seasoned security professionals, who detect advanced threats using multiple best-of-breed threat engines, sandboxing and behavioral analysis, correlation rules, machine learning, and other sophisticated techniques.

Summary and Business Implications

To stop cybercriminals, hacktivists and state-supported hackers, enterprises must go beyond traditional signature-based security defenses and SIEM products. These technologies are still critical in a modern defense-in-depth strategy, but attackers have found too many ways to evade the former, and the latter provides too limited a set of data and tools to reliably detect ongoing attacks and to find patterns in historical information.

The solution is to move toward a more complete approach to advanced threat protection.

In this approach, a Security and SSL Visibility component provides data for more effective blocking and better analysis of the unknown.

A Big Data Security Analytics component identifies unknown threats and provides data and tools so security analysts can perform comprehensive historical analysis and get at the root causes of vulnerabilities and attacks.

A Detection and Threat Intelligence component provides additional tools like sandboxing to identify unknown malware, and helps acquire real-time security information from thousands of outside sources.

Blocking and Enforcement become more effective, because blocking tools are provided with up-do-date information on known and unknown threats.

When these technologies are deployed to create an Advanced Threat Protection Lifecycle Defense, enterprises maximize their ability to detect and block known attacks, analyze and contain zero-day threats, and reconstruct and remediate even the most sophisticated assaults. The results will include better defense against known threats, shortening the duration attacks that are successful, as well as dramatic reductions in lost revenue, lost productivity, lost customer loyalty, breach notification fees, and clean-up costs.

For more information on the concepts and products discussed in this white paper, and to determine how these solutions can help in your environment, please visit Blue Coat at www.bluecoat.com/advanced-threat-protection.

BLUE COAT®

Security Empowers Business

v.WP-REVOLUTIONIZING-ADVANCED-THREAT-PROTECTION-EN-v1b-0714

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