proofpoint™

Predictive Defense and Real-Time Insight

The Next Step in Advanced Threat Protection for the Enterprise.

"Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities."

-- Neil MacDonald and Peter Firstbrook, Gartner

As clearly evidenced by the daily headlines about security breaches, traditional defense tools are failing to protect enterprises from advanced targeted attacks and new sophisticated forms of malware.

Researchers cited phish as the origin of 95% of targeted and APT-driven threats in the last year[i], and over 76% of IT security and operations staff have stated they'd been impacted by exploits or malware that had evaded their existing Intrusion Detection and Antivirus solutions[ii].

Gartner's conclusion: Organizations can't rely solely on traditional blocking gateways, but must invest in prevention, detection, response and predictive capabilities for complete protection.

In this report:

[i]2013 Verizon Data Breach Investigations Report

[ii]Ponemon Institute study, "The State of Advanced Persistent Threats", Dec 2013

Featuring research from Gartner

Gartner®

Such protection can't stop at the firewall; given a modern, mobile workforce, Enterprise-owned and employee-owned devices must all also be protected. One in every five clicks on malicious URLs in phish (20%) happens while the user is off the corporate network[iii].

At the same time, information flow is vital to business, and cannot be interrupted – so any successful solution must also be effectively transparent to the end user, and trigger only when a threat is conclusive.

But triggering only reactively – when a user has already clicked on a link and started to view a web page or file – is also ineffective. The multi-vector execution engines and dynamic malware analysis systems ("sandboxes") that do so must catch every inbound malware binary – a risky game, given traffic volume and the likelihood of polymorphic malware (malware that generates a different signature on every download). Many such reactive solutions also can't intercept https connections, meaning malware is free to download and communicate data back out without fear of detection.

Effective protection demands predictive defense capability. Proofpoint's Predictive Defense technology uses big-data analysis and advanced statistical modeling to proactively perform advanced dynamic malware analysis on potentially suspicious URLs and e-mail attachments to confirm threats before users click links or open attachments.

Effective protection demands predictive defense capability.

But some attacks will always penetrate the defensive perimeter. Which is why effective defenses acknowledge and plan for that inevitability, providing a responsive capability – ideally one with real-time, actionable intelligence, so that IT may act in a timely and effective way. Proofpoint's Targeted Attack Protection solution's real-time dashboard and "follow-me" protection provide an ongoing view into and defense against these attacks, identifying by name exactly which users clicked, what they clicked on, the forensics of the exploit, and more.

This combination of reduced time-to-detection and end-to-end insight and protection enables proactive protection of an organization's users, minimizing computer compromises within the enterprise, and reducing incident response time, effort, and costs.

Evaluating Proofpoint's Targeted Attack Protection solution against Gartner's reccomendations clearly shows why Proofpoint is considered a leading solution in the marketplace.

[iii]proofpoint.com/humanfactor

Gartner Research Criteria	Proofpoint Solution Functionality
Predictive; ability to anticipate new attack types	***Predictive Defense;*** Proofpoint's Big Data driven prediction and real-time scoring engine utilizing a cloud-based statistical model to predict URL destinations likely to be malicious as part of an emerging attack.
Detective; capabilities to find attacks	***Next-generation Detection;*** Proofpoint's Dynamic Malware Analysis Service enables detection of sophisticated targeted attacks, including those using polymorphic and zero-day malware, malicious attachments, and other advanced exploits
Preventive; policies, products and processes to prevent an attack	***Follow-me Protection:*** Proofpoint provides the URL re-writing of links within all suspicious emails to enable click-time protection via the URL Defense Service that is agnostic to browser, user device, and user location – on or off the network, local, mobile or global – to ensure continuous productive operations.
Retrospective; ability to investigate and remediate/ root cause analysis	***Threat Insight Service:*** Proofpoint provides real-time visibility into threat activity to monitor threat volumes, vectors of attack, identification of specific users that were attacked, and real-time notifications for potential incidents that require investigation, and other critical security metrics

For more information on Proofpoint's Targeted Attack Protection products, please visit proofpoint.com/tap – and read Gartner's research on ***Designing an Adaptive Security Architecture for Protection From Advanced Attacks***, available in the following pages.

Source: Proofpoint

From the Gartner Files:

Designing an Adaptive Security Architecture for Protection From Advanced Attacks

Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.

Key Challenges

- Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers.
- Most organizations continue to overly invest in prevention-only strategies.
- Detective, preventive, response and predictive capabilities from vendors have been delivered in nonintegrated silos, increasing costs and decreasing their effectiveness.
- Information security doesn't have the continuous visibility it needs to detect advanced attacks.
- Because enterprise systems are under continuous attack and are continuously compromised, an ad hoc approach to "incident response" is the wrong mindset.

Recommendations

Information security architects:

- Shift your security mindset from "incident response" to "continuous response," wherein systems are assumed to be compromised and require continuous monitoring and remediation.
- Adopt an adaptive security architecture for protection from advanced threats using Gartner's 12 critical capabilities as the framework.
- Spend less on prevention; invest in detection, response and predictive capabilities.
- Favor context-aware network, endpoint and application security protection platforms from vendors that provide and integrate prediction, prevention, detection and response capabilities.
- Develop a security operations center that supports continuous monitoring and is responsible for the continuous threat protection process.
- Architect for comprehensive, continuous monitoring at all layers of the IT stack: network packets, flows, OS activities, content, user behaviors and application transactions.

Strategic Planning Assumptions

By 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches — up from less than 10% in 2014.

By 2020, 40% of enterprises will have established a security data warehouse — up from less than 5% in 2014.

By 2018, 80% of endpoint protection platforms will include user activity monitoring and forensic capabilities — up from less than 5% in 2013.

Introduction

This document was revised on 18 February 2014. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Most enterprise security protection efforts and products have focused primarily on blocking and prevention techniques (such as antivirus) as well as on policy-based controls (such as firewalls), to block threats (the upper-right quadrant of Figure 1). However, perfect prevention is impossible (see "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence"). Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are

in a state of continuous compromise. However, organizations have deluded themselves into believing that 100% prevention is possible, and they have become overly reliant on blocking-based and signature-based mechanisms for protection. As a result, most enterprises have limited capabilities to detect and respond to breaches[1] (the bottom half of Figure 1) when they inevitably occur, resulting in longer "dwell times" and increased damage.

In reality, going forward, improved prevention, detection, response and prediction capabilities are all needed to deal with all types of attacks, "advanced" or not (see Note 1). Furthermore, these should not be viewed as siloed capabilities; rather, they should work intelligently together as an integrated, adaptive system to constitute a complete protection process for advanced threats.

Analysis

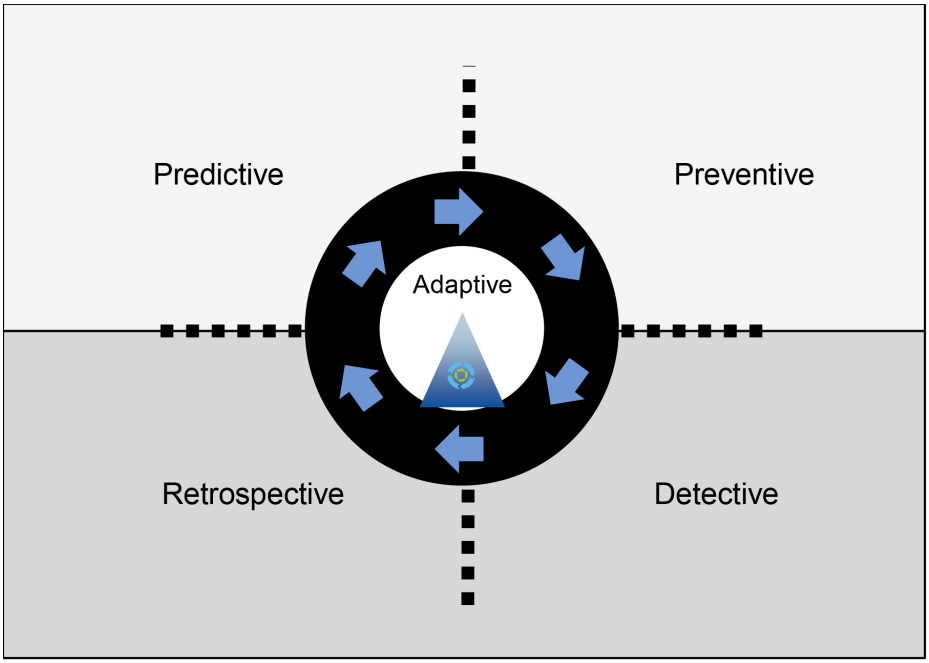
To help enterprises design an architecture and select from among competing solutions for adaptive protection from advanced threats, we have developed an architecture composed of four high-level categories of competencies, with three drill-down capabilities in each category, for a total of 12 capabilities (described in more detail later in this research). It is necessary to focus on capabilities within each category to deliver comprehensive, adaptive protection from attacks.

Critical Competencies of an Adaptive Protection Architecture

1 **"Preventive"** describes the set of policies, products and processes that is put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by reducing their surface area for attack, and by blocking them and their attack methods before they impact the enterprise.

2 **"Detective"** capabilities are designed to find attacks that have evaded the preventive category. The key goal of this category is to reduce the dwell time of threats and, thus, the potential damage they can cause. Detection capabilities are critical because the enterprise must assume that it is already compromised.

Figure 1. The Four Stages of an Adaptive Protection Architecture



Source: Gartner (February 2014)

3 **"Retrospective"** proficiencies are required to investigate and remediate issues discovered by detective activities (or by outside services), to provide forensic analysis and root cause analysis, and to recommend new preventive measure to avoid future incidents.

4 **"Predictive"** capabilities enable the security organization to learn from external events via external monitoring of the hacker underground to proactively anticipate new attack types against the current state of systems and information that it is protecting, and to proactively prioritize and address exposures. This intelligence is then used to feed back into the preventive and detective capabilities, thus closing the loop on the entire process.

The adaptive protection architecture is a useful framework to help enterprises classify existing and potential security investments to ensure that there is a balanced approach to security investments. Rather than allowing the "hot" security startup of the day to define security investments, security organizations should evaluate their existing investments and competencies to determine where they are deficient. The adaptive protection architecture is also useful in classifying and evaluating vendors. Those that provide capabilities in multiple categories are more strategic than vendors that only fit in one category.

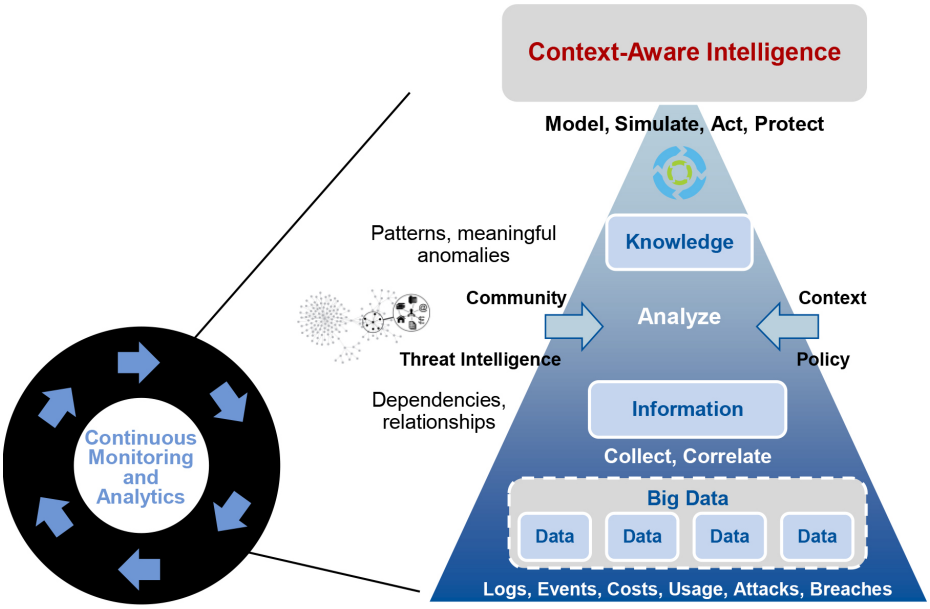
Security Protection as a Continuous Process

In an era of continuous compromise, enterprises need to shift from a mindset of "incident response" — wherein incidents are thought of as occasional, one-off events — to a mindset of continuous response — wherein attacks are relentless, hackers' ability to penetrate systems and information is never fully blocked, and systems must be assumed to be continuously compromised, and, thus, they must be continuously monitored (see Figure 2).

Continuous Monitoring and Analytics Is at the Core of the Adaptive Protection Architecture

As shown in Figure 2, to enable a truly adaptive and risk-based response to advanced threats, the core of a next-generation security protection

Figure 2. Continuous Monitoring Required for an Adaptive Protection Architecture



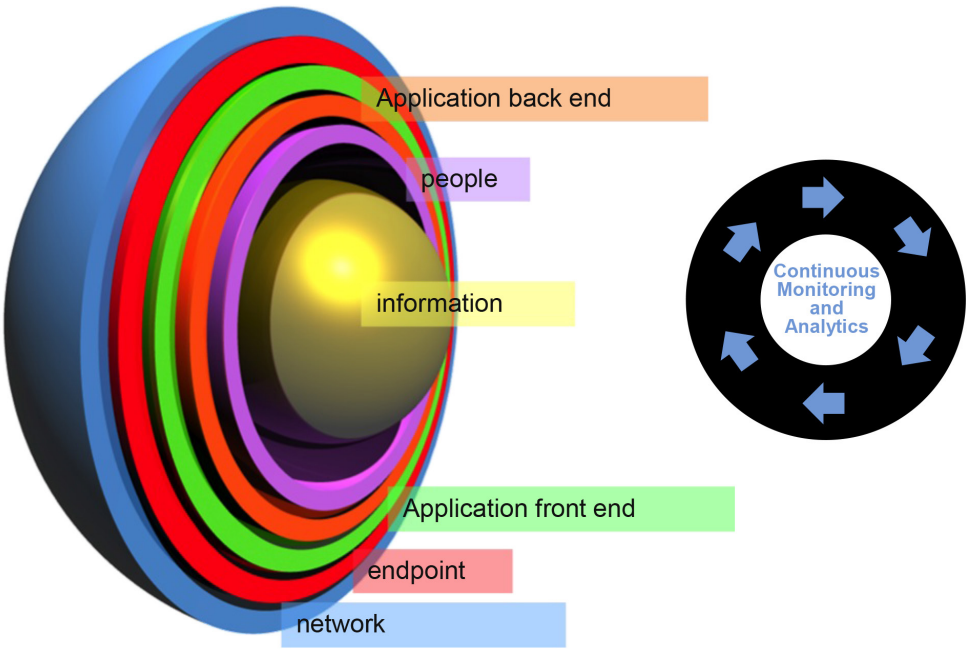
Source: Gartner (February 2014)

process will be continuous, pervasive monitoring and visibility that are constantly analyzed for indications of compromise. This will generate significant amounts of data. However, big data is only big noise unless appropriate analytics (supplemented with external sources of context, community and threat intelligence to improve accuracy) are used to distill it into actionable insight for the enterprise. The data can be analyzed using a variety of techniques, including heuristics, statistical analysis, inference modeling, machine learning, clustering analysis, entity link analysis and Bayesian modeling.

We believe that, going forward, all effective security protection platforms will include domain-specific embedded analytics as a core capability, in addition to traditional security information and event management (SIEM) systems. Enterprise monitoring should be pervasive and encompass as many layers of the IT stack as possible, including network activity, endpoints, system interactions, application transactions and user activity monitoring. This visibility must include enterprise-owned and employee-owned devices, and it must span enterprise data centers as well as the consumption of services from cloud-based providers.[2] The future of defense in-depth lies not only in layers of controls, but also in layers of monitoring and visibility (see Figure 3).

An enterprise's continuous monitoring of all entities and layers will generate a greater volume, velocity and variety of data than traditional SIEM systems can effectively monitor. This is one reason why Gartner research has established that big data analytics will be brought to next-generation security protection solutions (see "Information Security Is Becoming a Big Data Analytics Problem"), and also one of the reasons why, by 2020, 40% of enterprises will have established a "security data warehouse" for the storage of this monitoring data to support retrospective analysis. By storing and analyzing the data over time, as well as by incorporating context and including outside threat and community intelligence, patterns of "normal" can be established and data analytics can be used to identify when meaningful deviations from normal have occurred. As technologies supporting these

Figure 3. Continuous Monitoring of All Technology Layers



Source: Gartner (February 2014)

capabilities become more mainstream, we believe that the adaptive protection architecture will also move into the mainstream as platform vendors that have numerous component pieces integrate the capabilities and provide an embedded analytics engine that is pretuned and ready to use out of the box.

Six Key Inputs Into the Adaptive Protection Architecture

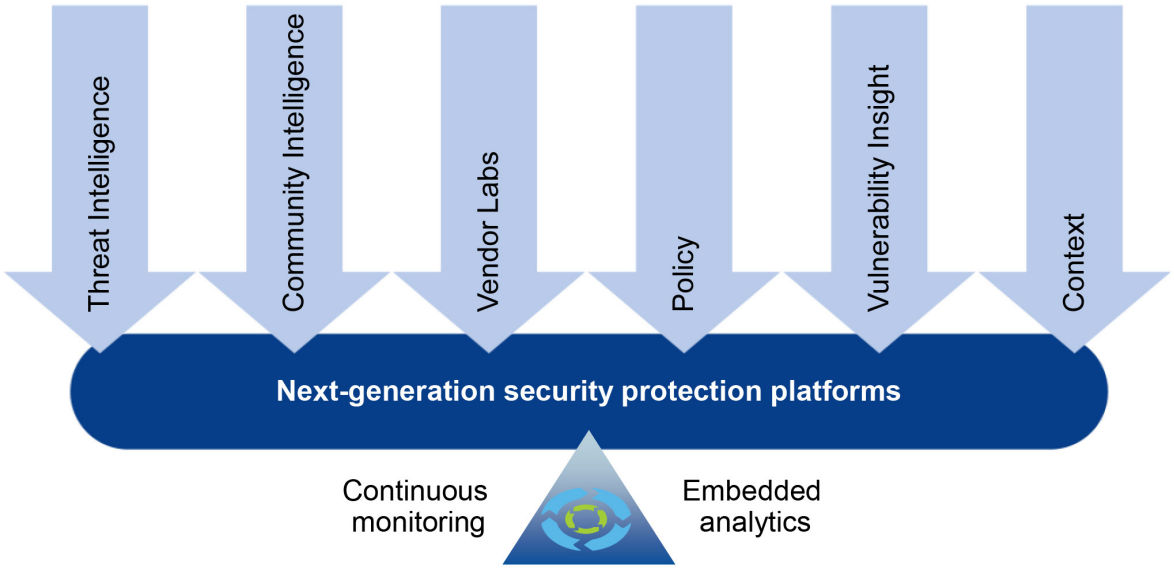
Before we explore the 12 capabilities of the adaptive protection architecture, there are six key inputs that should be an integral part of the architecture and used throughout the process for security decision making (see Figure 4).

Policy: Policies define and express the organization's requirements for system configuration, patching requirements, network connectivity, applications that are allowed to be executed, applications that are banned, anti-malware scanning frequency, sensitive data protection, what to do in the event of an outbreak and so on. These are typically derived from internal guidelines and external influences, such as regulatory requirements. Policies drive how enterprise security platforms will proactively prevent and reactively respond to advanced threats.

Context: Context-aware security (see Note 2) is the use of supplemental information to improve information security decision making at the time a decision is made, based on current conditions (for example, location, time of day, vulnerability state and so on). The use of context will be critical to identifying attacks that have bypassed traditional security protection mechanisms, and in helping to identify meaningful deviations from normal behavior without increasing the amount of false positives (see "The Future of Information Security Is Context Aware and Adaptive").

Community intelligence: To better protect against advanced threats, information should be aggregated, analyzed and shared across cloud-based communities that, ideally, have the ability to aggregate and analyze data for organizations in similar industries and geographic regions. This "crowdsourced" intelligence can then be shared to improve the overall protection capabilities of all participants. For example, community intelligence

Figure 4. Policy, Context, Vulnerability Insight, Community Intelligence and Threat Intelligence Are Critical for Comprehensive Protection



Source: Gartner (February 2014)

will help answer questions such as, "What are other enterprises like mine seeing? Have other people encountered this application/URL/IP address before? Has one of my peers developed a new way to detect an advanced threat and made this information available to others?" Thus, better communities will enable enterprises to share best practices, knowledge and techniques in a peering fashion. Larger communities will benefit from a network effect. Some communities will be self-forming, like FS-ISAC;[3] some will be government-sponsored, such as the United States Computer Emergency Readiness Team (US-CERT); and others will be created by the security vendor, its partner ecosystem and users of its platform.[4]

Threat intelligence: The core of threat intelligence will be reputation feeds that provide insight into the trustworthiness of objects — for example, IP addresses, domains, URLs, files, applications and so on. However, advanced threat intelligence services (see "Technology Overview for Security Threat Intelligence Service Providers") will also provide enterprises with insight into how attackers and campaigns are organized and what specific targets they are attacking. In addition, these services will provide specific guidance on how enterprises can protect their systems and information from these attackers. Increasingly, threat intelligence is being delivered in machine-readable formats that are more easily and directly integratable into network, Web, email and endpoint security platforms that are designed to consume them (see "Technology Overview for Machine-Readable Threat Intelligence").

Vulnerability insight: This information provides insight on vulnerabilities to devices, systems, applications and interfaces that the enterprise may have in use. In addition to known vulnerabilities, this insight should include visibility into unknown vulnerabilities that are present in an enterprise's custom and third-party applications. This can be accomplished by proactively testing these applications, libraries and interfaces for unknown vulnerabilities.

Vendor labs: Most security protection platform vendors provide information feeds that directly support their protection solutions — for example, signature updates as well as rule and pattern updates to provide protection from newly discovered threats.

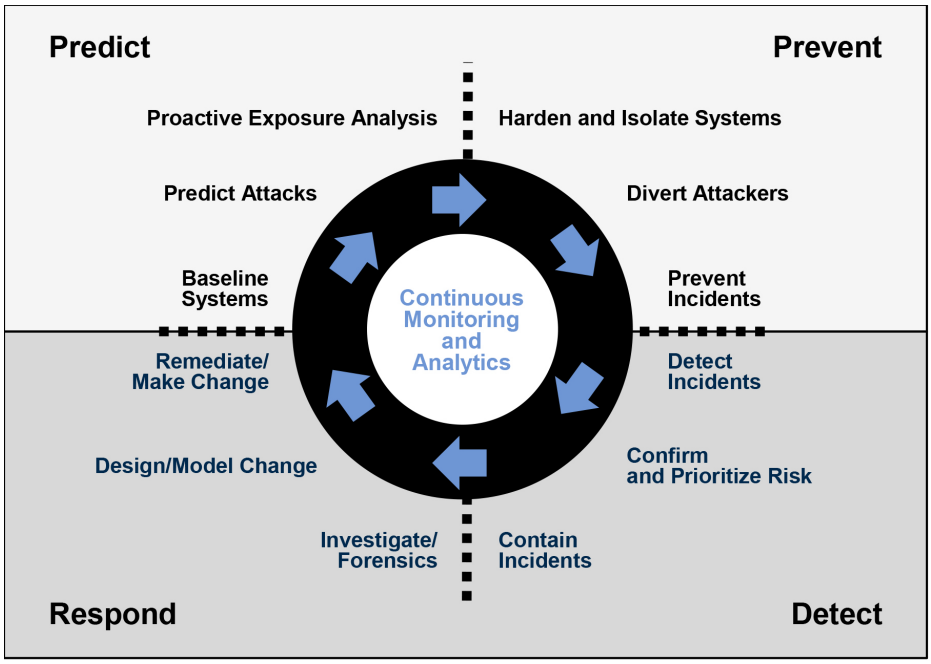
12 Critical Capabilities of an Adaptive Protection Process

To enable a comprehensive adaptive security protection architecture, we believe that 12 specific capabilities are necessary to augment our ability to block and prevent attacks, as well as detect and respond to attacks (see Figure 5).

Below is a brief description of the 12 categories of capabilities, starting in the upper-right quadrant and moving clockwise. Note that the ordering does not imply importance; rather, all 12 capabilities should be considered equally important for comprehensive protection.

Harden and isolate systems: We believe the foundation of any information security protection architecture should start by reducing the surface area of attack by using a combination of techniques. These techniques limit a hacker's ability to reach systems, find vulnerabilities to target and get malware to execute. Traditional "default deny" (also referred to as "whitelisting") is a powerful capability and approach that falls into this category, whether at the network firewall (only communicate on this port/protocol) or the system application control level (only allow these applications to execute; see "How to Successfully Deploy Application Control"). Data encryption can be thought of as a form of whitelisting and hardening at the information level. Vulnerability and patch management approaches to identify and close vulnerabilities also map to this category. Emerging endpoint isolation and "sandboxing" techniques, which proactively limit the ability of a network/system/process/application to

Figure 5. 12 Critical Capabilities of Gartner's Adaptive Security Architecture



Source: Gartner (February 2014)

interact with others, are another example from this category[5] (see "Technology Overview for Virtualization and Containment Solutions for Advanced Targeted Attacks").

Divert attackers: Simply stated, techniques applied in this evolving category try to address the asymmetric advantages that hackers have in time. These techniques waste hackers' time by making it more difficult for them to locate legitimate systems and vulnerabilities to attack, hiding or obfuscating system interfaces and information through a variety of techniques (such as the creation of fake systems, vulnerabilities and information). For example, the Mykonos technology acquired by Juniper Networks creates the illusion of application layer vulnerabilities where none exist,[6] thereby providing an active form of honeypots.[7] Unisys Stealth hides networked systems,[8] and CSG's Invotas solution implements a variety of diversion techniques.[9] While security through obscurity is insufficient, it is appropriate to consider these capabilities in a layered, defense-in-depth protection strategy.

In addition to wasting hackers' time, these techniques can, with high assurance, quickly identify anyone trying to access fake systems, vulnerabilities and information as a hacker (since legitimate users would not be accessing these), and prevent them from causing damage. At the user interface layer, newer vendors, such as Shape Security,[10] harden applications at the user interface layer to protect against automated attacks.

Prevent incidents: This category maps to well-established approaches to prevent hackers from gaining unauthorized access to systems; it includes traditional "signature based" anti-malware scanning as well as network and host-based intrusion prevention systems. "Behavioral signatures" may also be used at different layers here — for example, to prevent systems from communicating with known command-and-control centers by using threat intelligence from third-party reputation service feeds and integrating it into network, gateway or host-based controls (or within a host, thereby preventing one process from injecting itself into the memory space of another).

Detect incidents: Some attacks will inevitably bypass traditional blocking and prevention mechanisms, in which case it is key to detect the intrusion in as short a time as possible to minimize the hacker's ability to inflict damage or exfiltrate sensitive information. A variety of techniques may be used here (see Note 3), but most rely on the analysis of data gathered by continuous monitoring at the core of the adaptive protection architecture, by detecting anomalies from normal patterns of network or endpoint behavior, by detecting outbound connections to known bad entities, or by detecting sequences of events and behavioral signatures as potential indictors of compromise.

The continuous and pervasive monitoring at the heart of Figure 5 becomes critical to perform analytics on what is currently being observed versus what has been normal in the past so that the security operations analyst can identify anomalies. Going forward, the development of a continuous security operations center and skilled security operations analysts will become critical competencies for enterprises.

Confirm and prioritize risk: Once a potential incident has been detected, it needs to be confirmed by correlating indicators of compromise across different entities — for example, comparing what a network-based threat detection system sees in a sandboxed environment to what is being observed on actual endpoints in terms of processes, behaviors, registry entries and so on. This ability to share intelligence across networks and endpoints is one of the primary reasons cited by FireEye in its recent acquisition of Mandiant.[11] Based on internal and external context — such as the user, his or her role, the sensitivity of the information being handled and the business value of the asset — this issue should be prioritized by the risk to the enterprise, and be visually presented so that the security operations analyst can focus on the highest-risk priority issues first.

Contain incidents: Once an incident has been identified, confirmed and prioritized, this category works to contain the threat by isolating the compromised system or account from accessing other systems. Common containment capabilities are, for example, endpoint containerization, account lockout, network-level isolation, killing a system process, and immediately preventing others from executing the same malware or accessing the same compromised content.

Investigate/forensics: Once the compromised systems or accounts have been contained, the root cause and full scope of the breach should be determined using retrospective analysis of what exactly happened, using the data gathered from the ongoing and continuous monitoring at the core of Figure 5. How did the hacker gain a foothold? Was an unknown or unpatched vulnerability exploited? What file or executable contained the attack? How many systems were impacted? What specifically was exfiltrated? In some cases, enterprises may want to know more about the origin and motivation of the hackers — for example, Was this a nation-state-sponsored attack? If so, which nation? This category requires detailed historical monitoring information for the security analyst to answer these detailed questions. Network flow data alone may be insufficient for a complete investigation. More advanced security operations centers use full packet capture at the network (and the equivalent at the endpoint, in terms of system activity monitoring), along with associated advanced analytics tools, to answer these types of questions. Likewise, as new signatures/rules/patterns are delivered from the vendor's labs and research capabilities, they should also be run against historical data to see if the enterprise has already been targeted with this attack, and the attack has remained previously undetected.

Design/model change: To prevent new attacks or reinfection of systems, it is likely that changes to policies or controls will be needed — for example,

vulnerabilities closed, network ports closed, signatures updated, system configurations updated, user permissions modified, user training changed or information protection options strengthened (such as encryption). More advanced platforms should be capable of automatically generating new signatures/rules/patterns to address newly discovered advanced attacks — in essence, providing a "custom defense." However, before these are implemented, the change should be modeled against the historical data that has been gathered from the continuous monitoring to proactively test for false positives and false negatives.

Remediate/make change: Once modeled and determined to be effective, the change must be implemented. Some responses can be automated using emerging security orchestration systems, and policy changes can be pushed to security policy enforcement points, such as firewalls, intrusion prevention systems (IPSs), application control or anti-malware systems. For example, there are emerging security response orchestration solutions that are designed to automate and orchestrate this process.[12] However, at this early stage, many enterprises still prefer that security operations specialists, network security specialists or endpoint support staff members implement the change, rather than automated systems.

Baseline systems: Changes will be continually made to systems; new systems (such as mobile devices and the use of cloud-based services) will be continually introduced; user accounts will constantly come and go; new vulnerabilities will be disclosed; new applications will be deployed; and ongoing adaptations to new threats will be made. Thus, there must be a continuous rebaselining and discovery of end-user devices, back-end systems, cloud services, identities, vulnerabilities, relationships and typical interactions.

Predict attacks: This category is emerging and growing in importance. Based on reconnaissance of hacker attention, hacker marketplaces and bulletin boards; on vertical industry interest; and on the type and sensitivity of the data being protected, this category is designed to proactively anticipate future attacks and targets so that enterprises can adjust their security protection strategies to compensate. For example, based on intelligence gathered that indicates a likely attack on a specific application or OS (see Note 4), the enterprise could proactively implement application firewalling protection, strengthen authentication requirements or proactively block certain types of access.[13]

Proactive exposure analysis: With the latest intelligence gathered internally and externally, exposure and risk to enterprise assets must be continually assessed against predicted and anticipated risks, and adjustments to enterprise policies or controls may be needed. For example, when consumption of new cloud-based services is discovered, what risk does this represent?[14] Are compensating controls, such as data encryption, needed? The same is true for new applications that are discovered, whether they are enterprise applications or applications on mobile devices: What risk do these represent? Have they been scanned for known and unknown vulnerabilities? Are compensating controls, such as application firewalls or endpoint containment, needed?

Capabilities Must Work Together as a System

The end result should not be 12 silos of disparate information security solutions. The end goal should be that these different capabilities integrate and share information to build a security protection system that is more adaptive and intelligent overall. For example, while the enterprise may not have had a "signature" to prevent a breach initially, after the attack is discovered, the enterprise can use the knowledge gained by a forensic analysis of the attack to block further infections, in essence developing a "custom defense" against

the attack. Thus, the notion that "signatures are dead" is misguided hyperbole. Signature-based prevention techniques still play a useful role in the process, even if the "signature" to block the attack from spreading comes after the initial breach. In another example, a network-based advanced threat detection appliance can exchange indicators of compromise with endpoints to confirm whether an attack has taken hold on enterprise systems.11 Thus, the adaptive protection architecture works throughout the life cycle of an attack (see Figure 6).

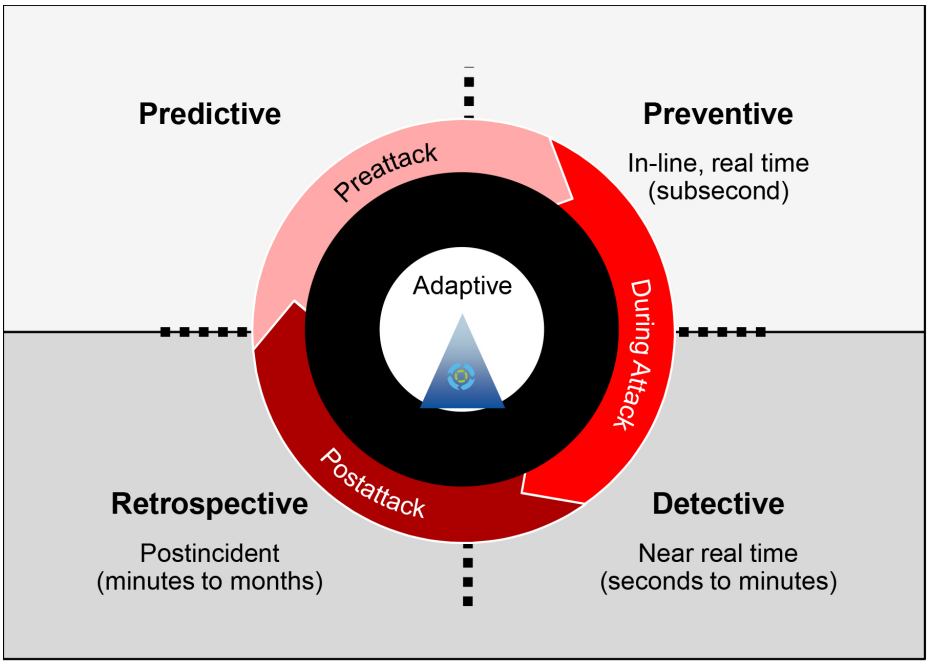
Security intelligence emerges from this continuous process as the categories of capabilities and different layers of security controls exchange intelligence, creating a need for a new generation of Intelligence-Aware Security Controls (IASC; see "Agenda Overview for TSP Security Solutions, 2014"). Like integrating threads of fiber in a rope, the integration of the capabilities, the exchange of intelligence between them, and the exchange of intelligence to and from the community and threat intelligence providers deliver overall greater protection.

Evaluating Vendors and Solutions Against This Architecture

Complete protection requires prevention, detection, retrospective analysis and predictive capabilities. More capable security protection platforms will include competencies in more stages and more of the specific drill-down capabilities in each stage. For example, the next generation of network security platforms should include firewalling, intrusion prevention capabilities and detection capabilities, such as content analysis capabilities.[15]

Furthermore, there is an opportunity for vendors that span different layers in the stack to provide a more integrated offering across different layers of the IT stack. For example, a vendor that has network-based protection and endpoint protection capabilities may link these for improved overall protection (see "Five Styles of Advanced Threat Defense"). Where a vendor doesn't directly have capabilities in an area, it should partner to improve the protection capabilities of its offerings.

Figure 6. Mapping the Adaptive Protection Process to the Life Cycle of an Attack



Source: Gartner (February 2014)

The ability to integrate with external context and intelligence feeds, as shown in Figure 4, is also a critical differentiator. For example, what types of context — location, time of day, device, reputation and so on — can the vendor understand and incorporate into its security decision making? Does the vendor support and nurture a robust cloud-based community of its customers for the exchange of community security intelligence? What types of reputation feeds can the platform support for improved security protection — for example, taking into consideration IP, URL, device, file and user reputation — in the security decision-making process?

Finally, we believe that leading next-generation security platforms should provide risk-prioritized actionable insight derived from embedded domain-specific analytics capabilities within the platform. The built-in analytics capabilities will work against the data gathered from the continuous monitoring at the center of these platforms to deliver the actionable insight at the top of the pyramid in Figure 2.

The goal is not to replace traditional SIEM systems, but rather to provide high-assurance, domain-specific, risk-prioritized actionable insight into threats, helping enterprises to focus their security operations response processes on the threats and events that represent the most risk to them. SIEM systems will still be needed to support near-real-time detection of threats across different layers of monitoring data, and, rather than blindly consuming all events, these systems will consume the prioritized, domain-specific intelligence produced by the next generation of security protection platforms, thus providing more effective SIEM results as well.

Evidence

[1]Industry data shows that it takes an average of 243 days to detect a breach (see Mandiant's "M-Trends 2013: Attack the Security Gap" at www.mandiant.com/resources/mandiant-reports).
[2]Visibility into cloud-based services can be achieved in a variety of ways. A cloud access security broker (see "The Growing Importance of Cloud Access Security Brokers" [Note: This document has been archived; some of its content may not reflect current conditions]) is one way to gain visibility. Alternatively, the cloud provider may make logs available for analysis, such as Amazon Web Service's (AWS's) recent announcement of CloudTrail. Visibility may be provided by security controls that run in the cloud itself — such as CloudLock for Google Apps and salesforce.com or Alert Logic for AWS. In other cases, agents running within the virtual machines in cloud-based infrastructure-as-a-service offerings can deliver the same visibility as workloads in enterprise data centers, such as those from CloudPassage, Dome9 and Trend Micro.
[3]See Financial Services Information Sharing and Analysis Center (FS-ISAC).
[4]See Imperva's ThreatRadar Reputation Services and HP Threat Central.
[5]An entire set of vendors is appearing to deliver isolation and sandboxing capabilities on Windows and mobile devices.

Application-layer containment:

- Blue Ridge Networks AppGuard Enterprise
- Bromium micro-virtualization vSentry
- MirageWorks vDesk and iDesk
- Trustware BufferZone
- Invincea Enterprise Edition
- Sandboxie

Browser isolation via sandboxing:

- Check Point WebCheck Endpoint Software Blade
- Quarri Protect On Q
- Sirrix Browser in the Box
- Dell KACE Secure Browser
- Light Point Web Enterprise

Browser isolation via remote presentation:

- Armor5
- Light Point Security
- Spikes Security

[6]See Juniper Networks' Mykonos Web Security.
[7]See SANS Institute's "Intrusion Detection FAQ: What Is a Honeypot?"
[8]See Unisys Stealth Solution Suite.
[9]See "Cyber Attackers Don't Fight Fair. Why Should You?" from CSG International about Invotas.
[10]See Shape Security.
[11]See "FireEye Computer Security Firm Acquires Mandiant," by Nicole Perlroth and David E. Sanger, nytimes.com, 2 January 2014.
[12]See NetCitadel and Intelliment Security.
[13]Several vendors' research organizations are actively researching malware ecosystems (also referred to as "malnets" or "darknets") to gain an early understanding of attackers, malware and malware delivery networks in development before they are released. By understanding attackers, attacks and attack infrastructure earlier in their development, this intelligence can be used to provide proactive protection once the attack is released. Examples include Blue Coat's malnet research ("Blue Coat Malnet Dashboard"), Juniper's Spotlight Secure attacker intelligence service, Norse's darknet research and OpenDNS's Umbrella predictive intelligence service.
[14]Risk I/O, for example, provides a risk processing engine for this type of analysis.
[15]There are many examples of network, email, Web and endpoint security protection platforms adding integrated detection capabilities, such as:

- Sourcefire's FireAMP and Advanced Malware Protection for Networks technologies, now acquired by Cisco
- Check Point's ThreatCloud Emulation Service and devices
- Blue Coat's Advanced Threat Protection offering, and its acquisitions of Solera Networks and Norman Shark
- Proofpoint's advanced threat discovery capability
- Palo Alto Networks' integration of its WildFire technology
- McAfee's acquisition of ValidEdge
- Trend Micro's Deep Discovery

Note 1. "Advanced Attacks"
Most enterprises consider an attack to be "advanced" when it bypasses their traditional blocking and prevention controls. The reality is that many of these attacks are not advanced in techniques; they are simply designed to bypass traditional signature-based mechanisms. What enterprises need and what this research describes is an architecture for an adaptive protection process that is capable of addressing all types of attacks, advanced or not. It must be assumed that some of these attacks will bypass the traditional blocking and signature-based protection capabilities of the upper-right quadrant in Figure 1.

Note 2. Gartner's Definition of Context-Aware Computing
Context-aware computing is a style of computing wherein situational and environmental information is used to proactively offer enriched, situation-aware and usable content, functions and experiences. Context-aware security is the use of this context for improved security decision making.

Note 3. Techniques for Detecting Indicators of Compromise (IOCs)
Monitoring at all layers will be needed, as shown in Figure 3. This includes the following:

- Monitoring outbound network traffic to detect the network signature of malware command-and-control traffic, or traffic with a destination IP address of known botnets, is an effective way to detect resident malware. Representative vendors include Damballa and leading secure Web gateway vendors (see "Magic Quadrant for Secure Web Gateways"). Next-generation firewalls and IPSs also support integration with reputation services for this type of monitoring.
- An emerging approach is to monitor network activity and compare it with normal traffic patterns, looking for suspect bursts of traffic volume or destinations, or new ports and protocols. Vendors that can help with network analysis include Blue Coat (via its acquisition of Solera Networks), RSA (via its acquisition of NetWitness), Fidelis Cybersecurity Solutions (acquired by General Dynamics), Lancope, TraceVector and Sourcefire's Advanced Malware Protection (AMP; acquired by Cisco).
- Continuous monitoring of user activities, logins, system access and behaviors, and analyzing this information for indications of account compromise or insider threats — examples include Click Security, Fortscale, GuruCul and Securonix.
- Comprehensive monitoring of endpoints — such as monitoring applications executed, processes launched, network connections, registry changes and system configuration changes — is a good way to detect indicators of compromise. For example:
  - Application control solutions, such as those from vendors Bit9, Kaspersky Lab, McAfee, Trend Micro and Lumension, are useful for this purpose by monitoring which applications have been executed at an endpoint.

continue

- Likewise, more detailed monitoring can provide more data for detecting indicators of compromise (for example, which network ports/protocols and IP addresses were contacted). There is an emerging group of dedicated IOC detection solutions from vendors like Carbon Black, CounterTack, CrowdStrike, Cybereason, RSA ECAT, Ziften and ZoneFox.
- Another useful way to detect indicators of compromise is to monitor all changes on a system. Triumfant uses this approach in its solution and then analyzes the data for meaningful patterns.
- Some IT operational tools that perform continuous endpoint monitoring are also turning their attention to security use cases (for example, ExtraHop, Promisec and Nexthink).
- Other monitoring capabilities that previously focused on forensic use cases are also evolving to support monitoring for IOCs, including Mandiant (acquired by FireEye), HBGary (acquired by ManTech), Guidance Software and AccessData Group.

Note 4. Example of Predictive Capabilities
A new industry-specific attack tool, discovered in a hacker marketplace, targets unpatched Windows XP machines. This intelligence and subsequent exposure analysis result in the enterprise making proactive configuration changes to Windows XP machines. It also results in a discovery activity to see if variants are already present in the organization.

Source: Gartner Research, G00259490, Neil MacDonald, Peter Firstbrook, 12 February 2014

About Targeted Attack Protection

Proofpoint Targeted Attack Protection™ is the industry's first comprehensive solution for combatting targeted threats using a full lifecycle approach, monitoring suspicious messages containing malicious URLs or malicious attachments, and observing user clicks as they attempt to reach out. Proofpoint Targeted Attack Protection uses Big Data analysis techniques with Cloud Architecture to add additional layers of security that cannot be matched by traditional security solutions and gateways.

Why Proofpoint Targeted Attack Protection?

Advanced targeted attacks represent one of the most dangerous advanced threats facing enterprises today. Many of these threats, begin with a spear-phishing attack: a single, carefully crafted email that tricks a recipient into clicking a link to download malware or open a malicious attachments. Proofpoint Targeted Attack Protection provides real time threat prevention against these kind of targeted attacks and defends against these threats with a full lifecycle strategy that includes:

Next Generation Detection

Proofpoint Targeted Attack Protection uses sophisticated techniques to evaluate advanced threats that are traditionally missed by signature-based and reputation-based solutions.

These techniques include:

- Malicious List Check - Check for emerging campaigns and known new malicious websites
- Code Analysis Check – Check for suspicious behavior, obfuscated scripts, malicious code snippets, and redirects to other malicious sites
- Dynamic Analysis – Sandbox a destination or sandbox a suspicious attachment to simulate a real user to a machine to observe changes made to a system

Predictive Defense

Proofpoint Targeted Attack Protection uses Big Data techniques and machine learning heuristics to predictively determine what 'could likely' be malicious, and take preemptive steps before any user clicks on it. It is achieved by:

- Modeling every user's email patterns and building behavioral history of that specific user to determine which email is suspicious and anomalous.
- Building Cloud based statistical model using history, Alexa ranking, IP block reputation, velocity of email sent from an originating IP, and a set of other criteria. Predicting malicious URLs, and proactively sandboxing with the help of real time scoring against this statistical model.

Follow-Me Protection

Proofpoint Targeted Attack Protection enables the solution to provide protection on any device, at any time, from any location, by following the email and checking for the URL destination's safety in real-time. A frequent technique used by hackers has been to drive recipients to click on a link directing them to a website which is initially harmless but turns malicious after a period of time. With Proofpoint Targeted Attack Protection, users are still protected: whether they access the message from the corporate network, home network, mobile device, or a public network.

- Protects users and organizations on and off the corporate VPN across all devices including Mobile, Tablet and Laptops.
- Architected to help comply with existing corporate security controls and acceptable use policies by redirecting the user's browser to safe destinations rather than acting like a proxy service.

End-to-End Insights

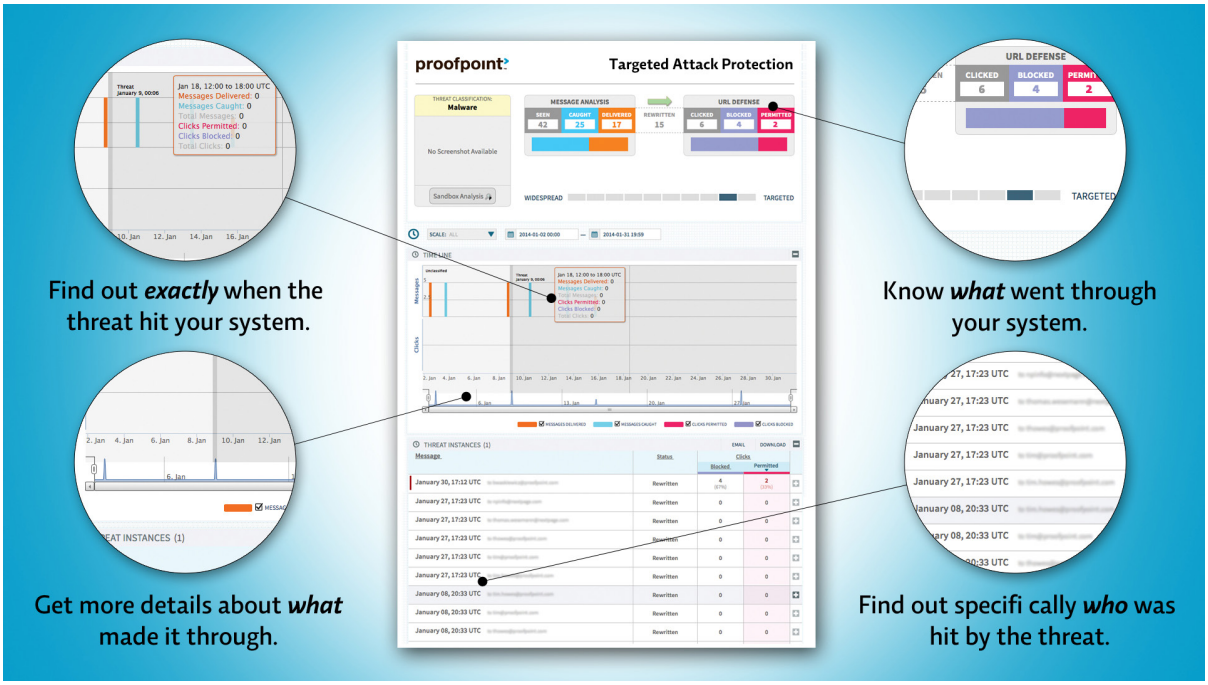
Proofpoint Threat Insight Service provides increased visibility and a real-time view to administrators and security professionals, to see how many and what types of threats are currently being received. It includes a web-based graphical threat analysis dashboard that provides data at an organizational-level, threat-level, and user-level helping to take immediate action, if required. Proofpoint's Threat Insight Service dashboard enables organizations to know critical information like:

- Is our organization under attack?
- Who is being targeted and what threats have been received?
- What is the status of each threat? Have we blocked it? Or, have they been neutralized? Or, are they still valid threats?

Sign up for live demonstration.

Source: Proofpoint

Figure 1. Proofpoint Threat Insight Service



Source: Proofpoint

About Proofpoint, Inc.

proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving and governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at www.proofpoint.com.