Bit9 Parity Suite

Moving Beyond a Porous Perimeter

Deploying Bit9 Parity Suite extends threat detection to endpoints and provides the information the Security Information and Event Management system requires to live up to its full potential.

Bit9

Table of Contents

Overview

Enterprise IT security based on anti-virus (AV) software, firewalls, and "in motion" intrusion detection/intrusion prevention systems (IDS/IPS) are demonstrably ineffective. A class of cyber attacks today is more targeted, sophisticated, and stealthy. In 2010, data breaches alone cost the enterprise an average of $7.2 million.[1] In the Second Annual Cost of Cyber Crime Study (2011), the median cost of cyber crime was $5.9 million per year, a 56 percent increase over 2010.[2]

The recognition of the extent of cyber espionage and the emergence of the Advanced Persistent Threat (APT) require a more proactive approach to protecting enterprise intellectual property (IP), Personally Identifiable Information (PII), and the very viability of enterprise information systems. What is needed is more automated, effective correlation and intelligent analysis of the overwhelming quantity of system data. *In other words, today's security professional needs more actionable data for faster insight into system usage and activity.*

Real-time, endpoint executable identification and event profiling are blind spots within current Security Information and Event Management (SIEM) platforms. The Bit9 Parity Suite automatically profiles endpoint activity and provides a live inventory of every file and executable on the system. The real-time profiling of endpoint activity can be customized to a specific security policy and is transparent to the end-user so it does not impede legitimate enterprise activity.

Most importantly, used in conjunction with in-motion data from firewalls and IDS/IPS, endpoint data collected by Bit9 Parity can help filter the vast amount of SIEM data – improving the signal-to-noise ratio – so that false positives are reduced and genuine threat escalation is timely and appropriate. A more complete picture of system activity and potential vulnerabilities allows the security professional to more efficiently detect, identify, and mitigate threats – *before propagation and data exfiltration*.

Automatic and intelligent correlation of endpoint data reduces enterprise risks and costs. By building a library of event correlation experiential knowledge, the enterprise can better adapt to evolving threats and prevent future attacks. Such a holistic and adaptable security posture is required to successfully address today's APT-laced environment and protect your business.

A Changing Threat Environment

The value of the information managed by IT – Intellectual Property (IP) in the form of blueprints, formulas, source code, etc., and customer information, including Personally Identifiable Information (PII) – has increased dramatically. Predictably, the efforts to gain illegitimate access to this information have grown in scope and sophistication.

MONEY AND POLITICS

Cybercrime is a transnational growth business. The U.S. Treasury Department estimates that cybercrime costs the global economy $300 billion: more criminal revenue than international narcotics cartels.[3] See below for a few recent examples:

- The Coreflood botnet targeted bank accounts by infecting over two million PCs with malware to record keystrokes, retrieve PII, and wire transfer money to overseas accounts. Suspected of being in operation since 2002, Coreflood resulted in an "unknown number of U.S. bank accounts being broken into with losses that could be in the hundreds of millions of dollars."[4]
- A group of cybercriminals was arrested in September, 2010, for having deployed ZEUS malware, available online as an attack toolkit, to steal "more than $70 million from online banking and trading accounts over an 18-month period."[5]

The motivations behind some cyber attacks are political, rather than financial. "Hacktivism" activities include distributed denial-of-service (DDOS) attacks, web site defacement, and the leaking of potentially embarrassing stolen information, e.g., Anon/HBGary, Wikileaks, and Anon/Stratfor attacks.

Of course, hacktivism can also be costly. In early 2011 Sony's PlayStation Network (PSN), Qriocity, Sony Online Entertainment, and other sites experienced multiple data breaches. (Sony is still struggling to get some sites back online.) Sony estimates the cost to be "at least $171 million," and those costs could climb if stolen data is misused in the future.[6]

CYBER ESPIONAGE

State-sponsored cyber espionage is a real and increasing threat to enterprise security – the depth, extent, and timeframe of which are only now becoming clear. In 2010 "Google was subject to a highly targeted attack originating in China, which aimed to steal information about human rights activists from the company's Gmail service."[7] The Stuxnet attack allegedly targeting Iranian centrifuges represents another high-profile example.

A recent report by Bloomberg documents that 760 U.S. "companies, research universities, Internet service providers, and government agencies were hit over the last decade by the same elite group of China-based cyber spies."[8] These attacks have been occurring for years, if not decades. Some estimates of the damage are alarming. Richard Clarke, former special adviser on cybersecurity to U.S. President George W. Bush, has stated:

> "What has been happening over the course of the last five years is that China – let's call it for what it is – has been hacking its way into every corporation it can find listed in Dun & Bradstreet…Every corporation in the U.S., every corporation in Asia, every corporation in Germany. And using a vacuum cleaner to suck data out in terabytes and petabytes. I don't think you can overstate the damage to this country that has already been done."[9]

Though it is difficult to put a dollar figure on the damage, Representative Mike Rogers, a former agent for the Federal Bureau of Investigation and chairman of the Permanent Select Committee on Intelligence, states: "They are stealing everything that isn't bolted down, and it's getting exponentially worse…Based on what is known of attacks from China, Russia, and other countries, a declassified estimate of the value of the blueprints, chemical formulas, and other material stolen from U.S. corporate computers in the last year reached almost $500 billion."[10]

Stealthy Penetration through Endpoints

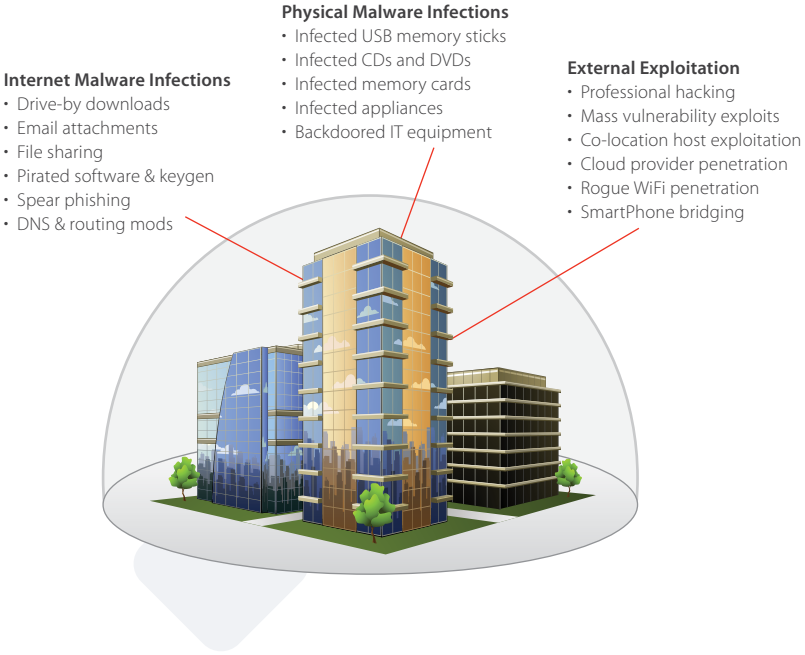
The focus and sophistication of advanced threats to enterprise IT security far exceed the likes of the ILOVEYOU worm of 2000. Today's advanced attacks are frequently multi-staged and employ a combination of hacking methods tailored to a specific target. They are designed to steal valuable information and/or seriously disrupt, if not destroy, your IT infrastructure.

The use of multiple techniques customized for a specific target, stealthily executed with remote command and control over a period of time, has led to the use of the term Advanced Persistent Threat (APT).

APT attacks involve reconnaissance via social engineering, for example "whaling." Whaling is a specific form of electronic communication "phishing," or "spear phishing," targeting top executives and individuals of high value to attackers. Reconnaissance was used against RSA: specific, identified executives were emailed a spreadsheet entitled "2011 Recruitment plan.xls" with a zero-day executable that then installed a backdoor through a known Adobe Flash vulnerability (CVE- 2011-0609).[11] Gathering social intelligence has also been suggested as the motivation behind the recent hacking of the iBahn networks, an Internet service provider to hotels.[12]

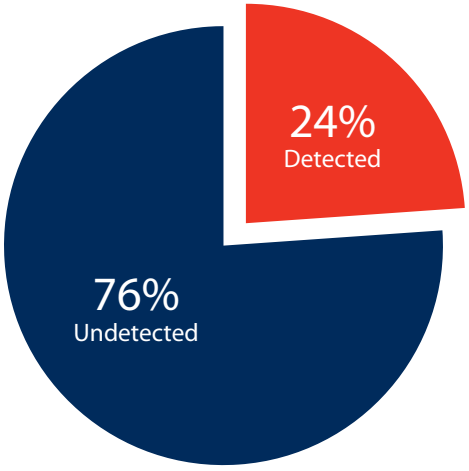
The majority of APT penetration vectors involve establishing a beachhead on an endpoint, where they can hijack credentials and frequently go undetected. Whether they exploit recognized vulnerabilities that have been overlooked (e.g., SQL injection), exploit zero-day vulnerabilities, or use social engineering intelligence to exploit human operators (e.g., spear-phishing or whaling), APTs gain a foothold via malware on an endpoint and continue to "fly under the radar." Existing endpoint security technologies are insufficient at detecting the more sophisticated, customized APT attacks. This lack of actionable, endpoint data is a blind spot for SIEM platforms.[13]

APT attacks are stealthy and remain undetected long after penetration. In January, 2009, Heartland Payment Systems, the fifth largest payment card processor in the U.S., acknowledged a breach impacting 130 million credit cards. The theft began in December, 2007, when SQL injection was used to compromise the corporate network (taking advantage of a web form vulnerability that had existed for eight years). The attack then stealthily progressed to the processing network, bypassing anti-virus defenses and installing "sniffer" software to "capture payment card data, including card numbers, card expiration dates, and, in some cases, cardholder names as transactions were processed."[14]



Perimeter Status Quo is Ineffective

Anti-virus (AV) perimeter defenses quite simply *do not recognize an APT penetration*. The APT is tailored to its target and by design is not used in widespread attacks – hence very likely unknown to any AV library. Dynamically created, or "polymorphic" malware, can avoid detection of even the most sophisticated AV algorithms.



Advanced Malware Detection by AV[15]

Furthermore, AV signature-based libraries are growing at 50,000 a day, with current libraries anywhere from 6 to 20 million signatures. At this pace, basing endpoint security solely on AV libraries is unsustainable in terms of sheer volume and efficient endpoint scanning – as well as a drain on IT resources. Some AV vendors now recommend downloading selective signature packs, belying the scalability problem. But more important is currency: *No endpoint security paradigm looking for known malware can detect the not-yet-known, dynamically changing, advanced threat.*

Current in-motion sensors, such as those as in firewalls or intrusion detection/intrusion protection systems (IDS/IPS), are useful and necessary components in a security architecture. The next generation firewalls, or application firewalls, are able to recognize applications traversing the network, regardless of port or protocol.

Still, it is extremely difficult to distinguish between legitimate and illegitimate network traffic stemming from an advanced attack. IPS/IDS do not profile executable files, nor do they address advanced attacks early at endpoints. IPS/IDS alerts are notoriously "noisy" and prone to false positives because of the sheer quantity of data and lack of meaningful context.

The signal to noise ratio of IDS/IPS data challenges the security analyst to identify deliberately stealthy attacks. The APT will naturally circumvent IDS/IPS by ensuring that network traffic appears normal, by encoding payloads – making it indistinguishable from legitimate HTTP – or even by hiding it in stealthy channels, such as packet timing jitter or via steganography. IDS/IPS might recognize an attack in progress – if you are clever enough to spot it – but cannot effectively track root cause, nor prevent future attacks from similar sources.

Cyber Attack Costs: Time Equals Money

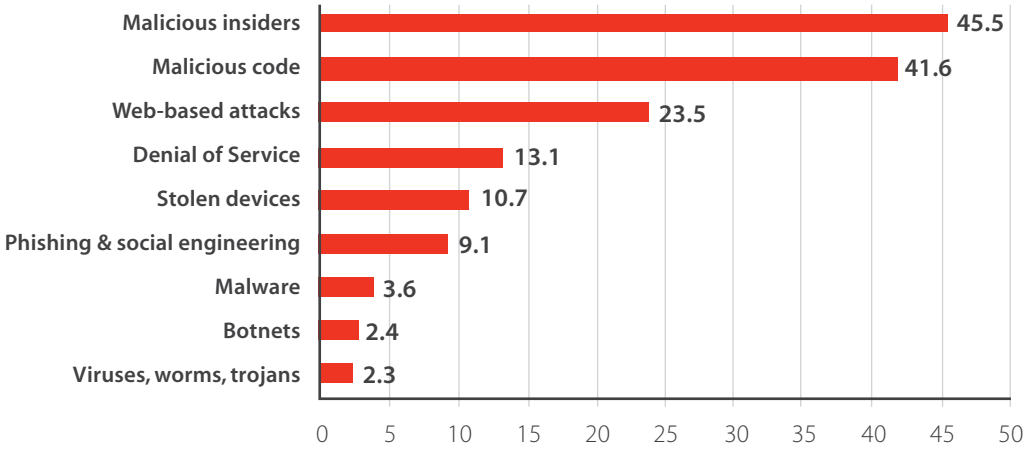
The Coreflood, ZEUS, and Sony cyber attacks cited above are dramatic examples of the costs to the enterprise. But it can be especially costly to detect, contain, and recover from APT attacks in particular due to a few key characteristics.

A recent Ponemon survey of 50 organizations indicated that costs vary considerably by the type of attack, mostly related to time: "Cyber attacks can get costly if not resolved quickly. Results show a positive relationship between the time to contain an attack and organizational cost." In the Ponemon survey, advanced attacks stemming from malicious code (i.e., malware that has avoided detection at endpoints) were second only to insider attacks in average days required to resolve.

In fact, detecting, mitigating, and resolving the effects of malicious code from an advanced attack represent the highest cost by attack type.[17]

The stealthy nature of APTs not only increases the time and cost to detect and contain an attack, it also can complicate system recovery. Without solid identification and tracking of malware propagated within the system – malware designed to be hidden – recovery might involve completely rebuilding multiple systems to guarantee security.

Average days to resolve attack for seven attack types[16]



Adaptive Application Control (Whitelisting)

Bit9 Parity technology provides deeper visibility into endpoint file and executable activity, resulting in real-time, actionable threat indicators. Adaptive application control extends detection to endpoints with indicators of new, zero-day threats and other leading-edge components of APT attacks. And, as we'll see below, these "intelligent" endpoint indicators provide critical insight the SIEM operator can leverage to more fully exploit the volume of firewall and IDS/IPS data.

BUILDING TRUST

The Bit9 Parity Suite conducts a "live inventory" across every endpoint, including servers, system-wide. The Bit9 Parity Knowledge Service provides a threat, trust, and reputation matrix for each file. These trust-level indicators can be tailored to dynamic, enterprise trust policies. For example, it encompasses such IT-driven software as trusted directories for a PC Lifecycle Management (PCLM) system or trusted application updates from the likes of Microsoft, which can occur automatically via the Internet.

In effect, establishing trust levels automatically filters out a significant quantity of noise (i.e., files that are recognized as low risk).

INTELLIGENT ENDPOINT INDICATORS

Parity monitors all endpoint file and executable arrivals and activity. It provides visibility into, and protection against, such malicious script execution as Python, Perl, .bat, etc. It automatically identifies potential security events: for example, the downloading of, and attempting to launch, an (un-trusted) Portable Executable (PE) or attaching a USB stick containing a file with hashes that correlate with intelligence indicators.

Not all endpoint sensor data is necessarily indicative of malicious activity. The context of an operational event, or a sequence of events, can provide important indicators of risk. For example, a computer restart is not generally considered a "security" event. However, if that event occurs multiple times within a short period of time, it might be indicative of a security situation.

Parity provides provenance data for activity on the endpoint: who introduced this file/country of origin, where the file was dropped, what other files were created, and where else this file resides within the larger system. Data on executables is available even if malware attempts to hide its tracks.

Endpoint sensors have not only extended detection capability to look for malware "at rest" on endpoints before put into action, but also provided some concept of the business value of the event: what user, what group, what security policy or level. In fact, *the endpoint activity intelligence provides critical perspective on system activity that cannot be obtained from anywhere else.*

It is this deeper visibility, combined with user- and application-level context, that helps filter out more of the noise. Endpoint indicator intelligence provides crucial insight for the SIEM operator and allows for real-time application controls and protection against advanced and zero-day attacks.

TAILORING PROTECTION TO THE ENTERPRISE

Endpoint-intelligent sensors need to adapt to changing security environments and be tailored to evolving threats. The 180 basic Parity security events can be customized to align with enterprise security policy and extended to accommodate new threat information.

Endpoint security postures can be synced with rights and permissions in the enterprise Active Directory, thereby tying user rights and privileges to actual system activity. A security policy view based on actual, relative risk metrics allows for more informed, targeted policy creation and enforcement.

Executable permissions can be tiered: banned, default-deny posture with local user prompt, monitored (e.g., alert the SIEM), or customized to enterprise policy (e.g., email ticket to support to provide justification).

By identifying higher risk endpoint files and processes, adaptive application control quickly provides more actionable security event insight. It provides the capability, unlike AV or IPS/IDS, to detect advanced threats at rest before they propagate and exfiltrate valuable information. When threats are identified sooner, there is less potential for information compromise and fewer costs to the enterprise.

Feeding the SIEM Correlation Engine

The next step is correlating the filtered and intelligent endpoint event data with in-motion network data, primarily from firewalls and IDS/IPS, in the SIEM. Parity provides deep integration with SIEM platforms, such as ArcSight ESM® or Q1 Labs®' QRadar®. Integration is provided using native CEF and LEEF support – or with other SIEM products using a generic syslog interface.

STANDALONE EVENTS

Parity event data can be filtered within the SIEM in different ways. Certain events are readily identifiable as a threat, or deemed actionable standing alone, such as:

- **Actionable Events by Class:** Some Parity events, depending upon the security policy and posture of the enterprise, may require no further filtering than their class to have security value. Such endpoint events as "Malicious file detected," "Potential risk file detected," or "Banned file written to computer" might be immediately actionable.
- **Suspicious Files by Location:** Simply knowing the filename or path of a file might be enough to warrant a security escalation. A file attempting to exploit the Alternate Data Streams (ADS) capability of storing data with an existing file or folder, but without being visible to the end user within Explorer or most file browsers. ADS are referenced by their associated file/folder, a colon, and then their actual filename. So, the file "c:\windows:foobar.exe" is an example of a "foobar.exe" file hiding within the Windows folder. Another example would be a file named "svchost.exe" located in the Windows folder (rather than the Windows System folder).
- **Suspicious Files by Installer:** A common entry point for targeted malicious software is through malformed documents that exploit a vulnerability to drop some unauthorized payload. Since the Parity events contain the name of the process creating or launching the unapproved file, these potential entry vectors can be mapped against the available endpoint event data. Parity looks for any unapproved executable or script content being created by Adobe Reader, Microsoft PowerPoint, Microsoft Word, and Microsoft Excel.

Other stand-alone events defined as actionable may include the arrival of unapproved executables or the attachment of a removable device. Such defined stand-alone events allow Parity to alert, in real time, SIEM or SOC teams to potential entry vectors of an advanced attack. This information can be acted upon immediately or drawn upon later during an incident response and recovery.

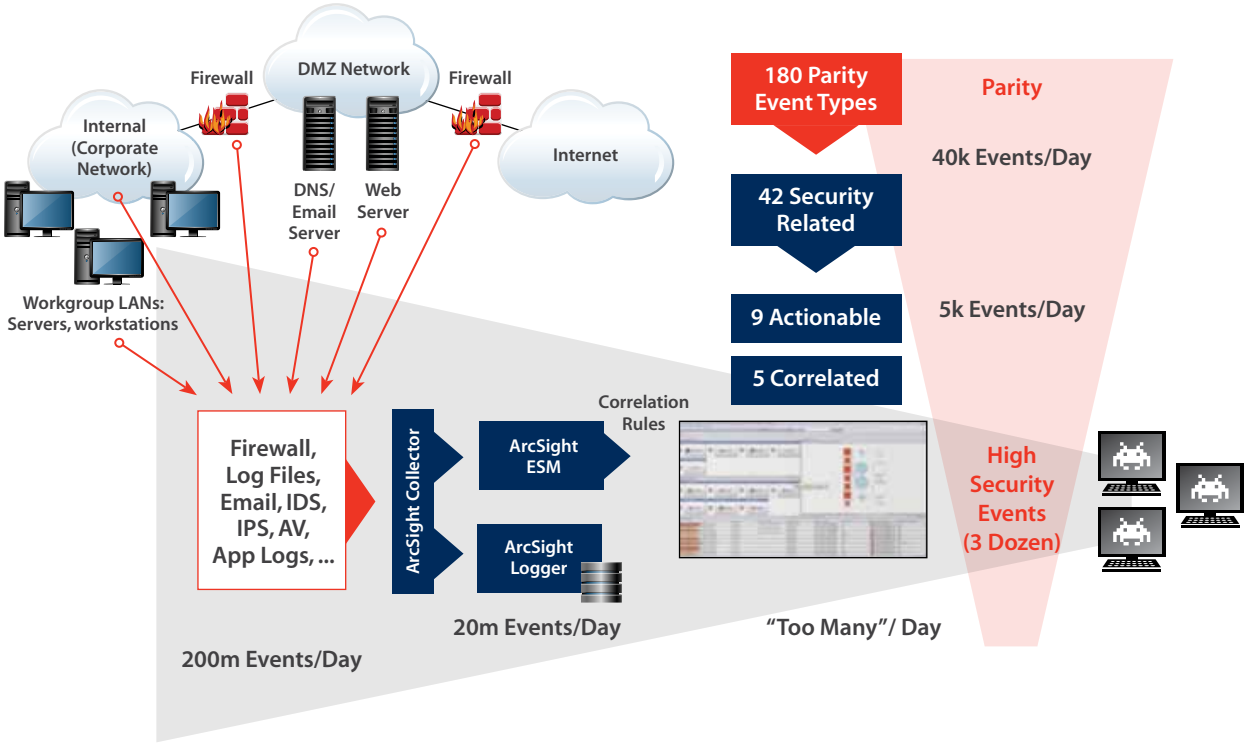
CORRELATING EVENTS

The challenge within the SIEM is the sheer volume of non-contextual data presented to the operator. Down at the network and infrastructure layers it is extremely difficult to winnow out genuine threats. Network traffic data flowing into the SIEM from firewalls and IDS/IPS is in the hundreds of millions daily; even eliminating simple log data will not bring this data within reach of real-time threat assessment. On the other hand, endpoint event data – depending on the number of endpoints, nature of endpoint activity, event definitions, and security posture – can be in the hundreds, if not tens, per day.

The correlation of Parity identified security events with in-motion data in the SIEM can dramatically improve the real-time threat signal-to-noise ratio. Visibility on events at the application level (i.e., what's running and what users/applications are doing) allows the SIEM operator to make real security contributions in a more holistic context. Correlating these detection sensors together, the SIEM operator can actually "do more with less" or, more accurately, analyze better and faster with more focused, contextual data.

Of course, every organization is unique, so the correlation rules developed must be specific to the SIEM data sources, including endpoint usage. A correlation rule that works with Snort events, for example, may or may not work with NetWitness. In developing correlation rules an organization should ask:

- What types of threats does the organization want to monitor?
- What are the typical attack patterns for such threats?
- What are the sources and types of events currently being tracked within the SIEM?
- Which of these events are used most often in monitoring for potential threats?



- What is the current signal-to-noise ratio the security analysts are facing when monitoring these events? (How often do the investigations or deeper dives result in false positives?)
- When investigating an event, what pieces of additional information does the analyst need?

Below are some examples of correlation rules.

- **Suspicious Files from Internet:** IDS are designed to sit on the wire and monitor suspicious Internet activity, but with executable content transmitted over the network hundreds of thousands of times every day, it is impossible to identify high-risk threats. Correlating IDS events with Parity endpoint events provides a more focused and effective data set. One of the events generated by Snort is "PE Header download," indicating that potentially executable content has been detected. (Other executables could include Java, Flash, PERL scripts, etc.) The event includes information about the source address (i.e., the attacker) and the target address. An activity watch list can be generated based on Parity events (e.g., show all computers and files where a file came in over the Internet and, within 10 minutes, an unapproved file landed on the target computer). The watch list could be refined even further: for example, if the results were filtered to only files that subsequently attempt execution.
- **Suspicious Files from Removable Media:** Downloads from a removable device represent another common attack vector. Similar to the example above, instead of looking for new files or new executions after a transfer over the Internet, this correlation filter looks for executions of unknown files from a removable drive after a device attach. A filter is used to identify all "First execution on network" events where the file path is from a removable, non-network drive. The idea is to capture scenarios where a never-before-seen file is being launched within moments of a removable drive insertion.
- **New Files with Blocked Outbound Activity:** By creating a list of the local IP addresses and host names of all Parity events, such as "New pending files to computer," "New file on network," and/or "First execution on network," correlation can be done with subsequent suspicious behavior related to the arrival of unapproved or new software in an environment: for example, correlation with a filter to look for "Outbound Deny" events from the firewall, such as attempting to send data to a DNS "blackhole." This "Outbound Deny" event filter can include an "InActiveList" clause matching suspicious outbound traffic with new software.

Correlation with Parity endpoint events allows the SIEM operator to analyze in-motion data in greater context (i.e., look at actual, real-time usage at application levels). It is precisely this endpoint file and process intelligence that is critical for effective, cost-efficient threat mitigation. The security professional gains more insight into system activity, not just raw data, and the enterprise gains more actionable information with fewer false positives.

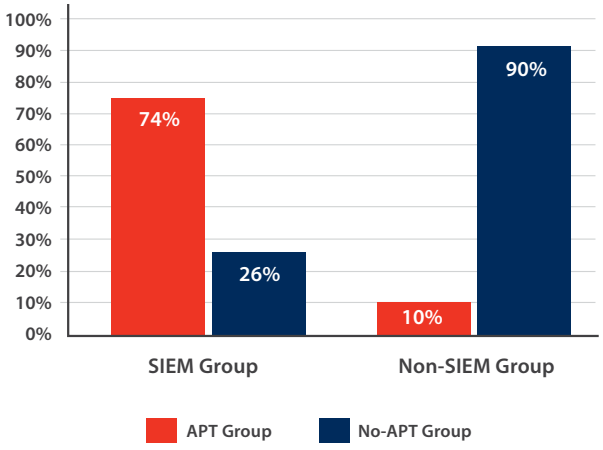
Benefits of Extended Detection and Correlation

Correlation allows overwhelmed SIEM or SOC teams to detect threats sooner, reducing enterprise risks and costs. With the context and provenance information embedded in Parity events, the origination or "root cause" of a security risk can be quickly identified and eliminated in many cases.

With greater visibility (not more raw data) in a "single pane of glass" within the SIEM, the operator can quickly remediate, ban unauthorized or malicious files, lock down specific machines, and confidently know the extent of malware propagation.

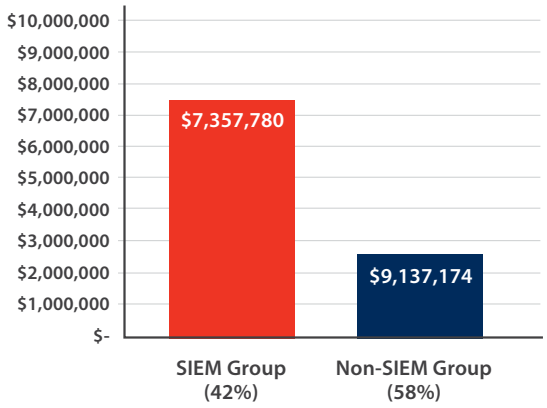
A significant relationship already exists between companies that use SIEM and their ability to recognize APTs. Using SIEM technology during a four-week benchmark period, only 10 percent of non-SIEM organizations even recognized they were under attack, whereas 74 percent of those with SIEM systems recognized the APTs.

Comparison of APT and no-APT by SIEM and non-SIEM sub-samples[18]



The companies that leveraged SIEM technology also reduced costs:

Comparison of SIEM and no-SIEM sub-sample on average cost of cyber crime[19]



When these cost benefits are broken down into recovery, detection, and containment, they are consistent across the board: The deployment of a SIEM system helps the enterprise not only detect advanced attacks, but better contain and recover. It should be noted that these savings do not (yet) represent the benefits of endpoint detection as provided by the Bit9 Parity Suite.

"Security improves through greater situational awareness."[20] Enterprise security professionals need to match wits with ongoing, multi-stage threats that are remotely controlled and attempt to cover their tracks. Incorporation of external information sources, such as NIST's National Software Reference Library or FS-ISAC, help the enterprise adapt to, or even anticipate, changing threats. By building a library of experiential knowledge, the enterprise can better adapt to changing threats, update policies or Parity event definitions, and take a proactive approach to security.

Conclusion

Adaptive application control (whitelisting) extends detection and control to the endpoints, providing more genuine, defense-in-depth security. Parity has the capability to discover malware at rest before execution, saving time and money in an advanced attack. Intelligent endpoint indicators provide a context of user and application activity crucial for enterprise security *that cannot be obtained from anywhere else*.

The real-time profiling of endpoint activity can be customized to enterprise security policy, tying user rights and privileges to actual system activity. A security policy based on actual, relative risk metrics allows for more informed, targeted policy creation and enforcement. Parity is substantially transparent to the end-user; it does not impede legitimate enterprise activity.

More automatic and intelligent correlation of endpoint data reduces enterprise risks and costs. Used in conjunction with in-motion data from firewalls and IDS/IPS, endpoint intelligence collected by Parity can help security analysts filter the vast amount of SIEM system data. The improved signal-to-noise ratio allows for real-time application controls and protection against advanced and zero-day attacks.

By building a library of event correlation experiential knowledge, the enterprise can better adapt to changing threats and prevent future attacks – thereby avoiding cost and service repercussions. Such a holistic and adaptable security posture is required to successfully address today's APT-laced environment and protect your business.

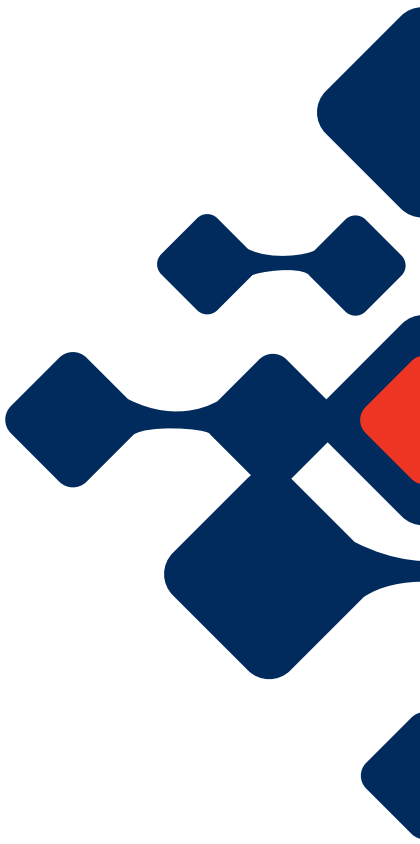
ABOUT BIT9

Bit9 is the market leader in advanced threat protection and server security software. The company's award-winning endpoint protection solutions provide total visibility and control over all software on endpoints, eliminating the risk caused by malicious, illegal, and unauthorized software. Bit9 specializes in protecting organizations against Advanced Persistent Threats.

The company's global customers come from a wide variety of industries, such as government, financial services, retail, healthcare, e-commerce, and education.

Bit9 is privately held and based in Waltham, Mass. For more information, visit http://www.bit9.com, follow us on Twitter @Bit9, Facebook, and Google+, or call +1 617.393.7400.

1. 2010 Annual Study: U.S. Cost of a Data Breach, Research Conducted by Ponemon Institute, LLC, March, 2011.
2. Second Annual Cost of Cyber Crime Study, Sponsored by ArcSight, an HP Company, Ponemon Institute, LLC, August, 2011.
3. "Conversation with Richard Clarke," Veracode & Bit9 Webcast, November 22, 2011.
4. "Feds Take 'Coreflood Botnet': 'Zombie' Army May Have Infected 2 Million Computers, Stolen Hundreds of Millions of Dollars," Jason Ryan, ABC News, Washington, April 13, 2011. http://abcnews.go.com/Technology/feds-crush-coreflood-botnet-infected-million-computers-stole/story?id=13369529
5. "Cyber Attack Toolkits Dominate Internet Threat Landscape", Information Policy, January 23, 2011. http://www.i-policy.org/2011/01/cyber-attack-toolkits-dominate-internet-threat-landscape.html
6. "Sony Data Breach Cleanup To Cost $171 Million", Mathew J. Schwartz, InformationWeek, May 23, 2011. http://www.informationweek.com/news/security/attacks/229625379
7. "E-mail accounts of senior US officials targeted in Chinese hack attack", Kathleen Hall, ComputerWeekly News, Thursday 02 June, 2011. http://www.computerweekly.com/news/1280095998/E-mail-accounts-of-senior-US-officials-targeted-in-Chinese-hack-attack
8. "China-based hacking offers evidence of global cyber war", Michael Riley and John Walcott, Bloomberg News December 13, 2011. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html
9. Ibid.
10. Ibid.
11. "Advanced Persistent Threat: Are You the Next Target?", Imperva whitepaper, 2011, p. 5.
12. "Breaking into iBahn's networks, according to a senior U.S. intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations." Washington Post, "China-based hacking offers evidence of global cyber war", Michael Riley and John Walcott, December 13.
13. Graphic from http://www.damballa.com/knowledge/advanced-persistent-threats.php.
14. "Heartland Payment Systems: Lessons Learned from a Data Breach", Julia S. Cheney, January, 2010. Discussion Paper, Payment Card Center, Federal Reserve Bank of Philadelphia. http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf
15. Gartner – Burton IT1 Research. ID# G00208636 – 10 March, 2011. "Application Control and Whitelisting for Endpoints."
16. Second Annual Cost of Cyber Crime Study, Sponsored by ArcSight, an HP Company, Ponemon Institute, LLC, August, 2011. p. 20.
17. Ibid. p. 9.
18. Ibid. p. 19.
19. Ibid. p. 16.
20. "Advanced Threats: The New World Order", RSA APT Summit Findings, October, 2011, p. 9.



266 Second Avenue Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com

About Bit9, Inc.

Bit9 is the leader in Advanced Threat Protection. The company's award-winning Application Whitelisting solutions provide total visibility and control over all software on endpoints, eliminating the risk caused by malicious, illegal, and unauthorized software. Bit9 specializes in protecting organizations against the Advanced Persistent Threat.