CORE Insight

The Value of Predictive Security Intelligence

CORE Security
+1 617.399-6980
info@coresecurity.com
www.coresecurity.com
blog.coresecurity.com

Introduction

Ten years ago, Internet worms, e-mail spam and opportunistic hacks were the biggest threats to your corporate network. In response, a stateful inspection firewall, desktop antivirus software and spam filtering could reasonably be expected keep your corporate network protected. Times have changed.

Today, attacks against your organization are much more likely to be targeted, stealthy and slow moving. Starting with an initial compromise through targeted e-mail or Web attacks, sophisticated attackers move laterally and quietly within your organization, exploiting employees' access permissions, misconfigured servers and weakly protected assets to obtain sensitive data, including customer information, financial records and intellectual property.

Unfortunately, many organizations that are the targets of sophisticated attacks are fighting the last war when it comes to their IT security investments. As Frost & Sullivan noted in its 2011 (ISC)² Global Information Security Workforce Survey:

"While …changes in the threat landscape have been steadily occurring over time, many organizations continue to address security the same way they have for years. CxOs need to find a way to balance their existing budgets and security postures with the latest trends"[1]

Down in the trenches, that means security-conscious organizations need more than accurate virus signatures and firewall rules to block attacks. Sophisticated, security conscious organizations need to correlate many pieces of intelligence, often over days or weeks, to spot a successful breach, or the signs of a mounting attack. Intrusion prevention systems, endpoint and network based data leak protection, Web filtering as well as log management and security incident management tools may all be brought to bear in piecing through a successful or unsuccessful security incident. For successful attacks, weeks more are often needed to determine the extent of the attack and begin to recover.

But, as many organizations have by now discovered, layered security comes with hidden costs: IT staff or paid consultants who can install, update and manage the products; experts to fine tune configurations and still others to monitor and make sense of the products' often voluminous output. What they need is a single vision of security infrastructure that cuts through the noise and helps IT staff to understand what's happening, why and what actions to take. Above all both security and IT teams need to derive value from security investments they've already made. *Insight*, Core Technologies' fast evolving security platform is the answer.

The CORE Security Platform: Predictive Security Intelligence

CORE Security believes that the greatest risk your organization can take in the face of modern threats is to be complacent. It's no longer acceptable to merely react to incidents and threats. Instead, your organization has to go on the offensive: pre-empting attacks rather than waiting to deal with their aftermath.

CORE's products empower organizations to take control of their own security: improving the effectiveness of legacy security infrastructure by predicting likely attacks and pointing the way to thwarting them before they occur.

[1] Frost & Sullivan (ISC)² Global Information Security Workforce Survey, p. 5.

CORE's predictive security intelligence platform is a new approach that can identify critical risks within your organization based on the way your organization operates: its unique internal processes, business objectives, and regulatory mandates. We use real-time analytics to transform the raw and disparate output of your security tools into correlated, actionable information. Core's products allow your IT staff to get ahead – and stay ahead of the threats facing your organization.

CORE Insight Enterprise: Continuous Business Risk Assessment

CORE Insight Enterprise is the first enterprise security intelligence solution to give organizations the ability to continuously assess their business risks.

Used by Fortune 500 firms and other security-conscious organizations world-wide, Insight empowers executives to make informed choices about security by aligning IT security operations with their corporate goals and performance objectives. At the same time, it gives them a more accurate understanding of their organization's risk posture, which allows them to optimize their security budget and increase operational efficiency and streamlined compliance efforts.

CORE Insight combines advanced attack simulation with real-world security testing features. Insight integrates with leading network asset management tools and network and Web vulnerability scanners.

With CORE Insight, your IT security staff can:

- **Understand your infrastructure** – You can't defend what you can't see. That's why even sophisticated organizations fall victim to attacks that spread by way of undocumented test- and development servers, rogue wireless access points and other shadow infrastructure. Insight's infrastructure mapping and analysis features reveal and track IT assets on your infrastructure, including those that you may not have known existed. And Insight automatically senses and adjusts to changes in your infrastructure, mapping the ways that newly deployed devices connect with existing IT assets.
- **Connect your IT security efforts to your business goals –** IT security is often divorced from IT operations, let alone the front office and an organization's business objectives. CORE Insight bridges that divide, providing measurable improvements in areas such as customer retention, and cost avoidance in areas such as compliance, brand- and intellectual property protection.
- **Satisfy compliance mandates** – Federal, state and industry regulations require different but overlapping sets of IT security controls to protect critical assets and data. Vulnerability scanning, penetration testing, patching and security awareness training are common elements of regulations ranging from the Payment Card Industry's Data Security Standard (PCI DSS), to FISMA/NIST guidelines to industry specific regulations like HIPAA and SOX. Insight can help your organization comply with those mandates by automating much of the process.
- **Validate critical vulnerabilities on your infrastructure** - Modern security tools produce a flood of data and alerts. CORE Insight increases the efficiency of your vulnerability management program by teasing out critical and exploitable vulnerabilities from the confusion of scan results and other security data feeds. It then helps IT administrators and executives connect the dots between assets, exploitable vulnerabilities, and critical systems and data, making it easy to focus the energy of precious IT staff where it's needed the most.
- **Determine which security investments are working for you** – It's easy to justify new security purchases in the abstract. It's much harder to determine, after the fact, whether that investment is paying off. CORE Insight can help your IT staff test whether specific controls are helping to block attacks or ameliorate the danger posed by known vulnerabilities. By understanding the cost of a real or potential attack, and the value of blocking it, Insight makes it easier to understand whether the cost of the security control is balanced by the protection it provides.

- **Scale security assessments to cover your entire enterprise –** Too often, critical security assessments fail to happen for lack of resources, not desire. CORE Insight allows your IT staff to take previously manual activities, such as security testing, and roll them out enterprise-wide using documented, repeatable and scalable processes, all without adding staff or expensive consultants.
- **Improve the security awareness of employees –** Employees are the Achilles Heel of every sophisticated IT operation. Spear phishing e-mail attacks and sophisticated scams circulating on social networks like Facebook and Twitter have proven to be a powerful lure for even well-meaning employees. CORE Insight is one of the only enterprise-ready security platforms that let you address problems like security awareness and sloppy security practices amongst your end users, thereby reducing your organization's threat surface and risk.

Here are some examples of how CORE Insight can help your organization make the most of its key security investments.

Streamlining Vulnerability Management

These days, it is not uncommon for organizations to maintain two or more vulnerability scanning platforms internally, each with dedicated staff to manage it and help make sense of the results of scans.

However, organizations that have deployed network and web vulnerability scanning products quickly come up against their limitations. Namely: vulnerability scanners were designed to find every potential threat to your IT assets. But simply knowing which systems on their network are potentially vulnerable to attack isn't enough. With limited time and resources, organizations also need to focus their resources on their most critical IT assets with exploitable weaknesses that require immediate attention.

"My first day on the job, I had to validate 300 vulnerabilities. If Insight can do that for me, I get 20% of my time back"--Jeff Norem, Senior Security Manager, FICO.

CORE Insight offers an antidote for the data overload that's common with vulnerability scanners. Insight creates a closed loop between vulnerability scanning, security testing, analysis and remediation.

Out-of-the-box integration with leading infrastructure vulnerability testing platforms means that Insight can be configured to start analyzing your organization in minutes, not days. Insight's integrated penetration testing and attack simulation features reduce the testing and validation of vulnerabilities, allowing your staff to see which combinations of vulnerabilities increase your risk and which paths might be used to exploit a known vulnerability.

Boosting ROI of VM with CORE Insight

Founded in 1956, FICO pioneered the development and application of technologies like predictive analytics, business rules, management and optimization to help the improved precision of complex, high-volume decisions.

With four data centers serving clients across the globe and a diverse IT infrastructure, FICO relies on an extensive vulnerability – and patch management program that includes network and web application scanning.

FICO invested in CORE Insight to boost the effectiveness of their existing security testing and vulnerability scanning efforts using Rapid7's Nexpose.

Insight allowed FICO's staff of two full time employees to work 20% faster: automating what had been a manual process of testing the output of vulnerability scans for exploitable holes. With Insight, FICO has been able to automate scans against more than 80,000 known vulnerabilities each week. From those scans, Insight boils down the results to no more than 10 to 20 exploitable items affecting deployed systems on the FICO network.

And the improvements aren't limited to vulnerability scanning. "Being able to prove exploitability also makes patches happen faster," says Vickie Miller, Senior Director of Information Security at FICO. She was also able to achieve enterprise wide visibility, enterprise wide risk assessment, business alignment, threat modeling, and predictive security intelligence through proactive automation testing.

With the help of Insight, your staff can focus their energies on analyzing and remediating threats, or implementing new security controls, while requiring far fewer FTEs and person hours to manage those products. Finally, by automating the process of identifying exposures and potential threats in your IT environment, CORE Insight increases the speed, reach and consistency of your entire vulnerability management process.

Reigning in the cost of GRC (Governance Risk and Compliance)

Today, private and public sector organizations across industries are bound by regulations that require stronger data security measures, faster detection of security breaches and disclosure of leaked or stolen data. Often, these regulations prescribe specific investments, as well.

The payment card industry (PCI) Data Security Standard (DSS) requires investments in technology like endpoint protection (antivirus) software and log management to help organizations that accept credit cards to detect attacks. Federal regulations like Sarbanes Oxley and HIPAA require a different but overlapping set of controls for their covered entities, which represent a broad swath of for profit and non-profit organizations across industries. Finally, state laws like Massachusetts' 201 CMR 17 can effectively mandate practices from organizations nationally, as they carry the possibility of stiff fines and don't apply merely to in-state firms.

This web of regulations have put a premium on organizations to conduct meaningful security testing of their IT infrastructure, and on repeatable, consistent and effective security auditing and testing practices. The stakes, and costs, are high. A 2010 Ponemon survey of Qualified Security Assessors (QSAs), found that typical costs to prove compliance with PCI DSS for Tier 1 credit card merchants was $225,000, with 10% paying over $500,000 annually for mandated audits. And that's a figure that doesn't include the cost of internal staff, technology and operating costs.[2] Data from the research firm Gartner from 2008 found that audit costs for Tier 2 merchants can spend as much as $100,000 on internal audits, and double that to achieve compliance. More recent data from Gartner suggests that, if anything, costs for PCI compliance have increased since 2008, especially among smaller (Level 2-Level 4) merchants.[3]

The market has responded to these organizations with so-called Governance Risk and Compliance (GRC) tools that promise to be a central repository for corporate-wide policies and compliance measurement. Too often, however, GRC solutions are little more than compliance trackers, without logical links to key IT security assets and, therefore, no ability to provide IT staff with what they need: situational awareness. The costs of compliance vary greatly depending on the complexity of the IT environment, the number and scope of regulations and varying labor and operational costs but it is seen a necessary cost in absence of more actionable solutions. In such situations, CORE Insight customers report that, on average, they realize savings of up to 30% on their compliance efforts, mainly through increased operational efficiency and productivity.

For organizations that are looking for ways to reign in GRC efforts and costs, Insight is an investment that quickly pays for itself:

- First, Insight addresses specific testing requirements dictated by regulations such as PCI, HIPAA, SOX, FISMA / NIST 800-53A, GLBA and can generate reports to satisfy any reporting requirements. By using Insight, organizations put themselves a step ahead of auditors: finding (and fixing) vulnerabilities before the guys with the clipboards do, and lessening the chances of unexpected surprises after an audit has concluded.
- Second, Insight connects the dots between network assets, vulnerabilities, compliance mandates and risk calculations. By adding Insight to an existing GRC program, organizations can automate compliance testing

[2] Ponemon Institute PCI DSS Trends 2010: QSA Insights Report
[3] Gartner Survey: PCI Compliance Activity Shifts Downstream as Aggressive Enforcement Continues, June 2011

and achieve "continual compliance." Furthermore, GRC efforts are informed by meaningful risk ratings that are grounded in up to the moment data from their own network.

- Third, Insight can lower the cost of compliance by spotting specific violations before your auditor does, avoiding costly penalties and streamlining preparations for and response to audits.
- Fourth, Insight assesses the effectiveness defenses such as intrusion prevention systems and firewalls against real-world network and web application attacks, thereby validating the effectiveness of existing controls.

Increasing effectiveness and efficiency of SIEM and Log Management

Properly deployed and configured, Security Information and Event Management (SIEM) and log management products help you manage the output of security products and give you insight into what's going on in your environment. SIEM products can save you thousands or tens of thousands of dollars merely by culling out duplicate and low priority events, aggregating data feeds and filtering out false positives, leaving your IT staff to deal with the dozens or hundreds of events that actually matter.

Despite their promise, however, these powerful tools often fall short of customer expectations or stall after their initial deployment, failing to realize the true potential.[4] Why? One problem is information overload. SIEM products attempt to correlate vast amounts of reactive security data. But they can only point IT staff in the direction of a critical issue. They can't identify the exact problem that needs to be addressed. In fact, a recent SANS Institute survey of SIEM and log management customers found a strong majority struggle to make sense of the voluminous output of these systems. Fully 64% of respondents reported that analysis and reporting of collected data was the most challenging aspect of operating their SIEM and log management platforms.[5]

SIEMs also provide only a historical account of what has happened in your network. Your incident response team must then investigate the alert to see what happened, and take action to improve the threat.

Finally, SIEM platforms come with considerable costs prior to- and after deployment. In addition to start-up costs like software licensing, hardware purchases and third party licensing fees, organizations investing in SIEM encounter down-the-road costs that are often considerable and poorly understood prior to deployment. They include vendor services and professional services costs for custom development and integration, training and expanded deployments. Internally, organizations must find trained and knowledgeable staff to operate their SIEM infrastructure: running and then reading reports and escalating alerts and warnings generated by the SIEM. Over time, reports and alerts must be revamped, recreated or otherwise adjusted to suit changes in customer needs or infrastructure.

Staffing for these various tasks may range from partial FTE (full time equivalent) positions at small organizations to two, three or more FTEs at large organizations. Behind the scenes, database administrators, system administrator and in-house development staff are needed to keep SIEM deployments humming.

How much does all this cost? By one estimate, the total hard and soft costs of a SIEM project range from 10% of SIEM license costs to 20x the total license costs for large and complex deployments.[6]

Faced with considerable and hard-to-predict costs like this, organizations are using CORE Insight to bring SIEM costs in line. Most important: CORE Insight provides context for SIEM and log management systems: identifying

---

[4] Gartner "How to deploy SIEM Technology, Dec. 2011
[5] SANS Log Management Survey 2010, p.9
[6] Anton Chuvakin, Siemusers.org http://siemusers.org/, March, 2011.

exploitable vulnerabilities on critical business assets, or on other systems – both network and endpoint - that could plausibly be used as part of a multi stage attack.

Armed with CORE Insight's database of exploits and attack simulation technology, IT staff can stop sifting through mountains of alerts and log data from their SIEM system and focus on what they know are the most likely-to-be-exploited vulnerabilities on the most mission critical systems. With Insight, your staff can connect the dots between security events and the IT assets that are critical to your business. Once you use Insight's analytics to understand the potential impact of an event on your business, the product makes the job of responding to and escalating alerts internally more efficient, too. Using CORE Insight in concert with your SIEM deployment will boost the effectiveness and efficiency of your overall monitoring operation, saving you both in labor costs and sparing you the cost and burden of adverse events or audit results.

Insight Tomorrow

CORE Insight adds value throughout your security ecosystem, but improving the accuracy and efficiency of key technologies like vulnerability management, log management, SIEM and GRC. But CORE Insight's long term unifying platform value extends well beyond integrations with those platforms, allowing your organization to consolidate its security investments and improve ROI by adding security intelligence that makes those products and your IT staff smarter and more efficient.

Today, organizations in fields like healthcare, finance, retail, and government need a layered security strategy that will shield their employees, IT assets and intellectual property from sophisticated, stealthy hackers, malicious insiders, industry competitors and even nation-state backed hacking groups.

Firewalls, endpoint security software, vulnerability scanning software, intrusion detection- and intrusion prevention tools, security information and event management (SIEM), log management and patch management are must-have tools today.

Already, though, security-conscious organizations are broadening the scope of monitoring they do to include activities such as data leak protection, privileged user management and more comprehensive network monitoring. As attacks continue to become more complex, those organizations will shift IT security spending to a new generation of tools that can spot sophisticated attacks in the making, or connect the dots between individuals and groups, attack types and vulnerabilities both inside and outside your organization. Similarly, already deployed technologies will be harnessed to focus on sophisticated threats and attacks. In one recent example of this, a SANS Institute survey of users or log management technology found that 63% ranked "detecting/preventing unauthorized access and insider abuse" as the top reason to collect logs in the first place, far about the desire to "meet regulatory requirements" (the first response of 40% of respondents).[7]

In the coming years, security infrastructure investments need to shift and focus more on data protection than perimeter defenses. As your security infrastructure evolves to address changes in both the threat and regulatory landscape, Insight is architected to absorb and enhance each new component. Here are some applications of Insight that stand to benefit your organization down the road:

[7] SANS Sixth Annual Log Management Survey Report, April 2010, p.5

Network Monitoring and Incident Response

Burned time and again by low and slow moving "advanced" attacks, security-conscious organizations have already made the leap from legacy IDS and IPS systems to network monitoring systems that can do real-time, full packet capture and analysis. Products by firms like RSA/NetWitness, Solera Networks and Palantir provide IT and incident response teams with automated analytics and real-time forensics that touch all the data in your enterprise across all key points of presence, uncovering the trail of stealthy, data stealing Trojans or the activities of malicious insiders. But, powerful as these tools are, they only solve part of the problem. Organizations benefit little from the (considerable) investments in such platforms if they can't learn from the information they uncover, repair the damage done by breaches, and train their staff. Combining Insight's security testing capabilities with the event capture and replay features of platforms like NetWitness and Solera allows incident responders to get a full view of historical network events. Insight's campaign and automation features allow your staff to quickly act on intelligence gained from network monitoring and full packet capture platforms, testing your entire network for other possible targets and attack paths.

Enhanced Education and Employee Training

A lack of effective training and user education is a common element in many high-profile data compromises. Sophisticated attacks almost always begin with so-called phishing e-mails or, increasingly, appeals via Facebook, LinkedIn, Twitter and other social networking sites. Once attackers have access to even a low level user's endpoint within your network, they can move silently and laterally within your organization to gain control of critical assets and data.

Despite that, recent data suggests that spending on training has taken a hit during the recent economic recession, as companies were forced to curtail investment in all but the most critical systems.[8] Going forward, organizations in the public and private sector will need to reverse that trend – and more – to make sure that their most vulnerable assets – their employees – are hardened against attack. The Whitehouse, in its National Initiative for Cybersecurity Education (NICE) has called on the government and private sector to expand cyber education and personnel development.[9]

CORE Insight offers a number of tools to aid organizations that want to increase employee education around cyber security. For end users, Insight allows organizations to construct sophisticated and automated campaigns that include social engineering and phishing attacks on end users. The regular use of such campaigns can help educate employees and make their employers more resistant to the early stages of sophisticated attacks.

And, as organizations and government agencies look to expand their ranks of IT security and incident response teams, CORE Insight allows them to put powerful penetration testing and security analytics into the hands of IT generalists, lowering the cost of security testing internally, while helping to educate a wider swath of IT staff about how to detect and respond to sophisticated attacks.

41 Farnsworth Street | Boston, MA 02210 | USA | Ph: +1 617.399.6980 | www.coresecurity.com
Blog: blog.coresecurity.com | Twitter: @coresecurity | Facebook: Core Security | LinkedIn: Core Security

[8] Frost & Sullivan, page 6.
[9] Comprehensive National Cyber security Initiative: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf