

# MOVING BEYOND SECURITY POINT SOLUTIONS

Why real-world security testing is the best way to assess overall readiness against complex IT threats

## EXECUTIVE SUMMARY

This paper will highlight the challenges that exist for today's organizations in assessing threats that are able to circumvent traditional IT and networking defenses, in particular, those that take advantage of vulnerabilities that linger between widely-deployed defense mechanisms based on flaws in those products, points of failed integration in security infrastructure, and attacks designed specifically to evade widely-deployed network, endpoint, application and email security tools. It is meant to illustrate the critical risks that continue to plague organizations despite their best efforts and deep investment in defensive technologies, and the powerful role that comprehensive security testing plays in helping them identify and prioritize their most significant risks to drive remediation efforts, strategize future spending and prove due diligence to external auditors.

## SECURITY INFRASTRUCTURE OVERLOAD

Over the last ten years, most organizations have been faced with the challenge of installing and integrating many layers of complex security point products, a process that some vendors have attempted to address by piecing together packages of related solutions with varying degrees of success.<sup>1</sup>

In recognition of the difficult nature of this work -- in addition to integrating various technologies -- many security vendors have also begun building onboard diagnostic capabilities into their products to help customers ensure that their security systems are functioning properly.<sup>2</sup>

But this model has fundamental shortcomings, as these testing capabilities are typically designed to ensure that the products they live in operate smoothly and as such perform only the most rudimentary of status checks, rather than aggressively seeking out a full range of potential security risks.

And in addition to the individual vulnerabilities that still exist in each element of the security ecosystem,<sup>3</sup> despite the addition of onboard testing mechanisms, the complex nature of most organizations' security infrastructure has introduced the potential for many more gaps in protection.

Point solutions also fail to address the full impact of attack scenarios after a perimeter breach. Once a skilled attacker finds their way in, the chances are that they won't stop in the "courtyard" of your organization.<sup>4</sup> Using multi-staged techniques that allow them to navigate from one security failing point to the next, they will tunnel further into your systems to seek the crown jewels of your organization, including sensitive and valuable data.

From technologies made by different vendors that will never integrate properly, to packaged solutions that retain assailable weak points, and every variation thereof, the reality is that most organizations have unknowingly introduced many additional opportunities for potential security risks.

Today's attacks on IT and networking infrastructure are being designed with all of these specific weak points in mind.<sup>5</sup> From targeted attacks on both known and newly-discovered vulnerabilities in widely-used technologies, to those threats that seek to expose gaps existing between layers of security point products, cyber-criminals have cultivated the expertise to exploit a seemingly-endless range of assailable vectors.

## LOGS, SCANNERS AND THE SECURITY DATA AVALANCHE

Most IT and networking systems and specifically most security point products feature complex layers of logs and performance monitoring functions that produce extremely relevant and valuable data. In many cases after an organization discovers that it has been breached in some manner, forensics teams can dig through the mountains of data resident in these systems and discover just how an attacker successfully circumvented security controls to carry out their assaults.<sup>6</sup>

This process illustrates another significant problem with today's security infrastructure -- that IT organizations are simply too overwhelmed by the sheer volume of data produced by various point products to make sufficient use of the information and work more proactively to stay ahead of all potential threats.

---

<sup>1</sup> "Symantec launches Endpoint Management Suite," SearchSecurity.com, June 2008

<sup>2</sup> "Microsoft ISA Server firewall diagnostic tool gets an upgrade," SearchWinIT.com, July 2007

<sup>3</sup> "Vulnerabilities are leaving anti-virus software open to attack," Manufacturing Computer Solutions, July 2008

<sup>4</sup> "TJX's failure to secure Wi-Fi could cost \$1B," ZDNet, May 2007

<sup>5</sup> "Sophos Security Threat Report," Sophos, July 2008

<sup>6</sup> "Verizon Business 2008 Data Breach Forensics Report," Verizon Business, June 2008

In recent years, security technology vendors have begun building new technologies to help address these issues, including security event management (SEM) and security information management (SIM) tools. But these products, while helpful, have also fallen prey to the problem of producing so much information that even those forward-thinking organizations that have adopted the continue to struggle to keep up with the sheer volume of information that they emit.<sup>7</sup>

Even some newer technologies designed specifically to help organizations identify specific gaps in their security posture -- such as vulnerability scanners and application security inspection systems -- leave organizations unable to understand where their most significant weaknesses lie because they produce long lists of potential flaws that include false positives and offer little guidance regarding which faults are most severe.<sup>8</sup>

Based on all of these issues, security teams are most often forced to pick and choose which log files, status reports and scanner results they monitor closely, essentially guessing where their most significant risks may lie and hoping that they haven't missed anything critical.

For many obvious reasons, the present security data avalanche fails to provide the most effective method for protection of organizational assets and offers little guidance about prioritization of risk.

## INDEPENDENT SECURITY ASSESSMENT

All of these aforementioned problems play directly to the strengths of comprehensive, independent testing technologies that aim to provide IT and compliance management professionals with increased visibility into their organization's overall security standing, and to help staffers understand where gaps in their security point solutions still exist.

Just as military units drill regularly to ensure that their equipment is functioning properly, that plans have been drawn up for any possible battlefield scenario, and that their communications systems allow them to stay in close contact to share crucial information about the landscape unfolding around them, IT security teams need additional methods for ensuring that their existing defenses are working, and to respond to potential threats as they emerge.

Driven by government and industry mandates requiring them to do so,<sup>9</sup> IT security and regulatory compliance teams are already being ordered to conduct more frequent reviews of the networks, devices and end users for whom they are responsible to protect against the existence of potential security gaps -- and being actively monitored in this process by both internal risk managers and external auditors.

In direct response to this challenge, a wider variety of commercial-grade security testing technologies have been introduced to help organizations seek out potential weak points that exist among their IT defenses to determine where they may still face cyber attacks or potential data loss.

The promise of these IT security assessment platforms is roughly the same as the exercises carried out by military units to assure that they won't be outflanked on the battlefield -- to identify any strategic weaknesses or failures in existing equipment.

Security testing solutions can also be fed with much of the data emitted by security point products to help sort out false positives and garner actionable information from the avalanche of content those systems provide to prioritize risks and enable subsequent remediation efforts.

By engaging in ongoing, proactive testing, organizations have found that they can isolate points of failure in their security infrastructure and address those issues quickly, instead of spending longer period of time analyzing point product log files to garner less conclusive results.

---

<sup>7</sup> "Security Manager's Journal: Frustrations mount from lack of resources," Computerworld.com, July 2008

<sup>8</sup> "The Best Web Application Vulnerability Scanner in the World," Jeremiah Grossman, Oct. 2007

<sup>9</sup> Information Supplement: "Requirement 11.3 Penetration Testing," PCI Standards Board, April 2008

And with the sizeable investments that organizations have already made in amassing point products to foster the broadly-endorsed “layered security” approach,<sup>10</sup> IT managers and line of business leaders are demanding new methods for gauging the value of those systems before committing to future spending plans.

Security industry experts, including analysts and consultants, have recognized the need for comprehensive testing capabilities delivered independently of defensive technologies to provide the most comprehensive and objective view into potential risks.<sup>11</sup>

As security point products continue to proliferate -- exemplified in the arrival of newer technologies including data loss prevention (DLP) tools, network access control (NAC) systems and behavior-monitoring applications -- even more pressure will likely be applied to those teams responsible for installing and maintaining the technologies to ensure that they are meeting goals and delivering sufficient return-on-investment.

Industry experts and customers that have already adopted the systems agree that the most effective method for assessing an organization’s overall security posture, testing the efficacy and ROI of defense mechanisms, and proving the value of future point product investments is by adopting more consistent, comprehensive security testing to address all these aforementioned challenges.

## CONCLUSION

Organizations that truly desire to do the best possible job of protecting their IT assets and sensitive data must ask themselves a battery of important questions, including:

- “Do we have a firm grasp on our most significant risks and vulnerabilities, and how frequently are we assessing these issues?”
- “If we were targeted with an attack, would we be able to prevent it, and could we even detect it?”
- “How do we know if our existing security systems are functioning effectively and delivering return on investment, and how do we gain better visibility into this?”
- “Are our employees following security policies and procedures, are those rules sufficient in their makeup, and how consistently do we enforce them?”
- “Will industry or government regulations change the manner in which we protect our IT assets and electronic data, and how must we prepare for this likelihood?”

In consideration of all these critical questions, organizations that are truly committed to proactively meeting the changing dynamics of the security and compliance landscape must ask themselves how comprehensive, independent security testing will improve their overall standing and rapidly move to adopt such technologies.



For additional information on CORE IMPACT, please contact us at 617-399-6980 or via email at [info@coresecurity.com](mailto:info@coresecurity.com). You can also visit our web site at [www.coresecurity.com](http://www.coresecurity.com).

<sup>10</sup> “Rising Security Concerns and Concept of Multi-Layered Security Promotes Convergence,” Reuters, Jan. 2008

<sup>11</sup> Gartner Case Study: “Penetration Testing Tool Use,” April 2008