CISOs Need More Than Perimeter Defenses in a World of Expansive Network Borders

MASERGY
Performance Beyond Expectations

Firewalls, intrusion detection, intrusion prevention, sandboxing, VPNs and endpoint protection: They're all critical to organizations' perimeter defenses. Equally important is having up-to-date security configurations and hardened policies for each of the multiple layers that comprise network security perimeter protection.

But it's time for enterprise CISOs to consider moving beyond these traditional approaches to security in a world of more expansive network borders and multiplying endpoints. Today's networks can't be contained. They reside across and are populated by:

- Multiple public and private clouds, data centers and carrier networks;
- In endpoints that include a variety of mobile devices, from smartphones to tablets;
- A multitude of connected devices that comprise the Internet of Things and the Industrial Internet of Things.

CISOs also must confront a world where threats loom large within and without the network's extended reach. In Understand the State of Network Security: 2015 to 2016, for example, Forrester Research has reported that the most common ways in which breaches occurred over the last 12 months were internal incidents within the organization – 38%. That was followed by external attacks targeting the organization, at 28%.

The Insider Threat Spotlight report, a crowd-based research project undertaken in cooperation with the Information Security Community on LinkedIn and Crowd Research Partners, finds trouble with insider threats, too, with 53% of these classified as malicious data breaches. That's just slightly less than those classified as inadvertent data breaches (57%). Among those insiders posing the greatest threats, it says, are privileged users, such as managers with access to sensitive material (59%).

Yet, more than half of organizations lack the appropriate controls to prevent an insider attack, the report reveals. Fewer than one-third use analytics to help detect such threats, for example, and under one-quarter continuously monitor the user behavior taking place on their networks.

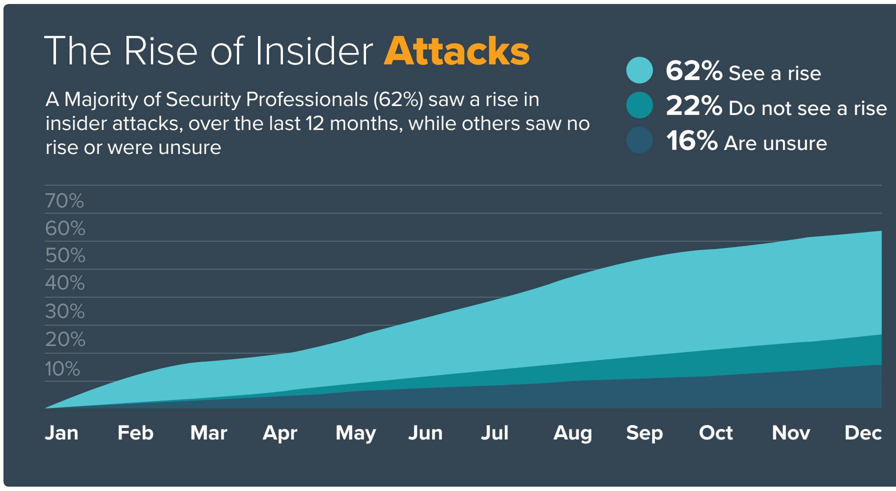
Where the Money Goes

IT system security seems a perpetual leader when it comes to tech budget spending, with network security often at the forefront of that spend. In 2016 the opportunity – and ideally the will – exist to take a much more sophisticated approach than standard perimeter defense mechanisms to tamping down risks and stopping threats before they do harm.

No matter how much money organizations invest in perimeter defenses to help assure their network security, that by itself is clearly not enough to do the

The Rise of Insider **Attacks**

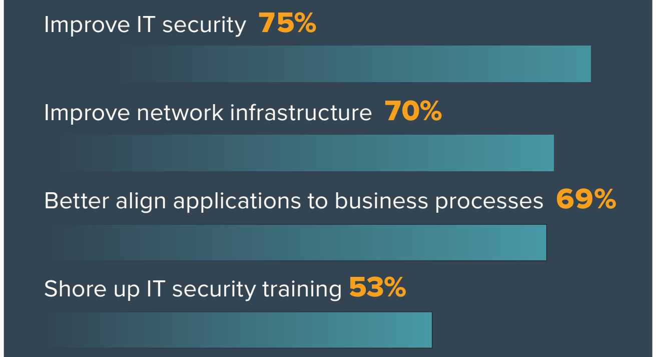
A Majority of Security Professionals (62%) saw a rise in insider attacks, over the last 12 months, while others saw no rise or were unsure



THE INSIDER THREAT: What good are perimeter defenses alone when it comes to users who can exploit their legitimate access to an organization's systems and sensitive information?

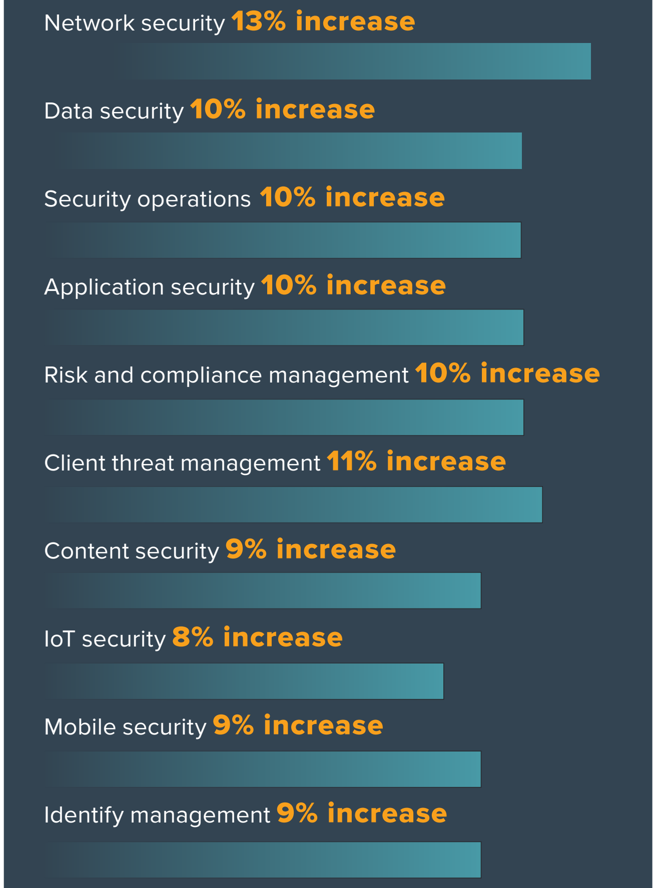
Source: LinkedIn Information Security Community and Crowd Research Partners

IT Investments Planned for 2016



Source TechPro Research

Security Spending Priorities



Source Forrester Research

job. The data breach of millions of employee records at the U.S. Office of Personnel Management that was announced last June, for example, had its source in a vendor's stolen credentials, and experts have commented that perimeter defenses are ineffective in the face of such exposures.

Once a hacker is credentialed to access one system, it becomes easy to become similarly credentialed to access others, moving laterally and stealthily through the network in pursuit of their ne'er-do-well goals.

A Sure Thing by No Means

Perimeter defense security is a good first line of defense. But that's all. And, even as a first line of defense, disappointments can result from issues such as neglecting to ensure that each layer of security is running the most recent software and operating systems.

The misalignment between budgets and areas of greatest risk is great, according to a Ponemon Institue study. Some 84 percent say their organizations are investing in intrusion detection or prevention systems – major perimeter defense technologies – but only 41 percent say it is a top performing technology in terms of economic benefits.

Indeed, the 2015 Data Security Confidence Index finds a dichotomy between how well respondents believe perimeter security systems are working and whether they really are performing at desired levels:

87% The percentage of respondents who believe that their organizations' perimeter security systems are effective at keeping unauthorized users out of their network.

54% The percentage of respondents who report that their organizations' perimeter security systems have been breached in 2015, which compares to 22% in 2014.

The indirect costs of a data breach includes reputational damage and loss of business opportunities – and may even result in a fall in share price, Accenture says.

More to the point, just over one-third of respondents are not confident that their organizations' data would be secure if unauthorized users penetrated their network perimeter. This likely speaks to organizations not taking all the right steps that enhance an enterprise's protection beyond deploying perimeter defenses alone.

Other research confirms the struggle. In the report, State of Perimeter Security Defenses, Time to Think Different?, research on gateway solutions in Fortune 2000 company environments revealed that the very best performing secure gateway allowed 15% of the infected devices to communicate out to the perpetrator's command and control servers. Three of the six gateways observed allowed 90%-plus of the infected devices to send communications to the malware's perpetrators.

Get Past the Perimeter Mindset

IT departments need to do a better job protecting what is essentially an enterprise without perimeters, populated by threats that lurk everywhere.

Security experts even estimate that over 40% or more of the threats facing the enterprise comprise at least five separate components. Nemertes Research has pointed out that these threats are particularly hard to protect against.

On its own, each component of the threat may look harmless but once inside and combined with other components, a deadly concoction may result.

Was it ever possible to stop each network threat, halt every breach, fight back any intrusion? Not really, but IT security leaders likely had a little more confidence in their security posture back in the days of better-defined network borders and fewer endpoints – and when signs weren't pointing to a growing threat of malicious insiders as well as bad-guy outsiders using unwitting insiders to get into their corporate networks.

Things have changed, and not only with network architectures and access. CISOs also should expect to be under greater pressure to build digital trust among customers around data use. In its report, Guarding and Growing Personal Data Value, Accenture warns that customers will avoid dealing with companies they don't believe will keep their data secure.

A Smarter Security Approach

It's time to get smarter about detecting intrusions that make it through perimeter defenses, and more intelligent about dealing with breaches quickly. What's needed: a unified approach to enterprise security. Perimeter defenses, as well as log and vulnerability management, will always have a place in the enterprise. But they need to be part of a holistic security framework – not a compilation of discrete point solutions that are incapable of working together to provide preemptive remediation information across the enterprise network, from on-premise to the cloud.

A holistic framework that brings that vision to life must combine an integrated security architecture with the adaptive and predictive data sharing, tracking and analysis capabilities of a network behavior analysis and correlation engine. Keeping the perimeter safe from breaches as best as possible matters, yes, but protecting the network from dangerous threats already on board and in progress, such as insider and advanced persistent threats, matters more in the current environment.

Masergy and its Unified Enterprise Security solution take on that challenge. UES employs employs machine learning to improve cyber security by providing detection based on hidden variables that are difficult for humans alone to analyze. Combining machine learning with human judgment, different attacks planned for a network can be detected using previous network data, even if the new attacks use different vectors.

Machine learning in Masergy's approach handles big data problems such as network behavioral analysis. It detects and thwarts network reconnaissance activity prior to an attack by building a highly sophisticated behavioral profile, one that exceeds traditional frequency, threshold, and netflow-based detection methods.

With Masergy's patented security platform that includes continuous monitoring, CISOs will understand where their business is vu.lnerable, who is trying to attack it and how before threats can be triggered.

Masergy's security architecture also is extensible, modular, centrally manageable, and scalable. Its integrated design makes it possible for IT security leaders to ensure that their teams are able to discover even very subtle anomalous network behaviors and address threats in as efficient, rapid and durable a manner as possible.

Masergy's UES solution is the smart way for enterprises to take their security strategy beyond stacking up layers of perimeter defenses to building up predictive intelligence that stops network hacks in their tracks. Better yet, thanks to its machine learning, it gets smarter about the job every day.

MASERGY
Performance Beyond Expectations

+1 (866) 588-5885

44 (0) 207 173 6900

To learn more about how your company can move beyond perimeter defenses and engage with a Unified Enterprise Security solution, **visit Masergy.com.**