Countering Escalating Cyberthreats with a New Security Architecture

CSO
Strategic Marketing Services

Leveraging next-generation network packet brokers can deliver business as well as security benefits.

Chief information security officers (CISOs) and other information security executives increasingly find themselves in the line of fire, and not just from cyberattackers. These security professionals are being bombarded with escalating demands and expectations from CEOs and corporate boards who find their digitally dependent organizations at significant risk from a wide variety of cyberthreats.

> **For enterprises, the average financial loss for a single cybersecurity event was $884,000 in 2017, up from $471,000 in 2016.**
>
> **— 2017 U.S. State of Cybercrime Survey**

The rapid emergence of cybersecurity as a critical business concern has thrust CISOs and their infosec teams into the spotlight. On the bright side, this new prominence gives security executives the opportunity to play roles that are more strategic and impactful within their organizations.

Conversely, CISOs who do not fully grasp the broad range of business objectives being pursued by the C-suite—objectives both within and beyond the security realm—risk being marginalized and may struggle to succeed.

The growing volume and diversity of cyberattacks aren't the only factors driving the rise of cybersecurity's strategic importance. Also at play is a rising recognition that cybersecurity is more than a discrete and isolated IT function. CISOs focused only on protecting data, repelling attackers, and providing other IT defenses are missing the bigger business picture.

Beyond delivering their core functions, security technologies, architectures, and policies have broader effects that can ripple throughout an organization. The ways in which cybersecurity is deployed can affect everything from an organization's IT budget to the complexity of its IT infrastructure and even a company's overall ability to be agile, efficient, and innovative.

As if these responsibilities weren't enough of a burden, many CISOs face a frightening reality: Their existing security tools and procedures are straining and breaking under the pressure of today's network speeds and data volumes, leaving their enterprise exposed to cyberthreats and malicious behavior. Further complicating things is the fact that corporate network operations have become more extensive and segmented. In response, many organizations have tried to bolster their defenses by adding new security elements. Often, however, these efforts have produced a sprawling patchwork of old and new tools that can be costly, difficult to manage, and (all too often) ineffective.

Faced with these challenges, CISOs and other infosec professionals need a comprehensive security solution that also delivers desired business benefits. As this paper explains, many organizations are turning to the leader in next-generation network packet brokers to meet these diverse and daunting requirements.

Cyberchallenges alter the business/security dynamic

Among the many reasons why cybersecurity has become a top CEO and business priority, one is readily apparent: financial risk. Overall, companies suffered $381,000 in monetary losses on average in 2017 due to cybercrime and other cyberthreats, according to the "2017 U.S. State of Cybercrime Survey." Conducted by the publication CSO with several partner organizations, the survey found that the average loss experienced by enterprise organizations in 2017 was $884,000, up from $471,000 in 2016.

Financial losses, of course, are just one potential consequence of cyberbreaches. Corporate victims can also lose intellectual property, business

> **Financial losses are just one potential consequence of cyberbreaches. Corporate victims can also lose intellectual property, business reputation, and customers and can suffer legal and regulatory penalties if their defenses and processes aren't up to snuff.**

Figure 1. Cybersecurity Becomes a Top CEO Priority

	2017	2016	2015	2014
TOTAL	**646**	**571**	**558**	**722**
Help reach specific goal for corporate revenue growth	32%	32%	40%	42%
Upgrade IT and data security to avoid cyber attack **< UP FROM #8 PRIORITY IN 2014**	32%	29%	23%	18%
Simplify IT	31%	23%	24%	22%
Lead a produc innovation effort	28%	22%	21%	28%
Reduce IT spending	22%	15%	16%	13%
Enable new plan for customer acquisition & retention	21%	19%	22%	30%
Enable global expansion	19%	11%	13%	19%
Collaborate with the CMO or Cheif Digital Officer on major customer initiative	17%	13%	18%	13%
Lead merger integration or due diligence on a potential acquisition	15%	12%	13%	12%
Strengthen business skills of IT staff	15%	16%	18%	
Fill technical skill gaps of IT staff	9%			
Partner with Chief Data Officer to identify new business or cost-saving opportunities	7%			

Q: What are the CEO's top three priorities for you in the coming year?

reputation, and customers and can suffer legal and regulatory penalties if their defenses and processes aren't up to snuff. These consequences have become direr as cyberattacks have grown in volume, diversity, and sophistication and as organizations have become ever more dependent on digitally based operations.

Long-standing threats including malware, phishing, and distributed denial of service (DDoS) attacks remain ongoing concerns but have often been superseded by or combined with new technologies. Among the more recent forms of cyberattack, ransomware has become a much feared scourge. Using ransomware, attackers encrypt files and demand a digital ransom to unlock them. In May 2017, one massive ransomware attack, using WannaCry malware, affected approximately 75,000 organizations in 99 countries.

On another front, the emergence of millions of poorly secured Internet of Things (IoT) devices has enabled attackers to assemble massive botnets that can flood victims with crippling traffic volumes. A September 2016 DDoS attack leveraged more than 150,000 simple IoT devices, including Internet-connected cameras and DVRs, to deluge hosting provider OVH with 1 terabyte per second of data.

The speed and volume of network traffic—benign or not—have escalated so rapidly that many security tools and systems simply can't keep up. Consider that at 100Gb network speeds, the gap between data packets is just 6.7 nanoseconds, according to a Gigamon study. Security systems that can't keep pace with such traffic speeds can only try to monitor subsets of the full traffic volume and hope that malicious code doesn't slip through.

No surprise, then, that three-quarters of the companies surveyed for the latest "U.S. State of Cybercrime Survey" were more concerned about cybersecurity threats in 2017 than they were in 2016—an upward trend that is almost certain to continue. As shown in Figure 1, this concern has pushed security to the top of CEOs' priority lists. In 2014, by comparison, cybersecurity lagged behind seven other CEO priorities.

Predictably, the rising importance of cybersecurity to CEOs is influencing IT department priorities. Security initiatives are now the single most important technology project within IT departments, and meeting security, privacy, or compliance goals was tied with increasing productivity as a top organization objective, according to the "Computerworld 2017 Forecast Study." One other notable measure: Security spending, on average, consumes 13% of the total IT budget, reports IDG's "2018 State of the CIO" survey.

Perhaps most tellingly, security strategy and IT strategy, once largely separate, are increasingly integrated. In 2016 just 37% of those responding to IDG's annual CIO survey said that their IT security strategy was an integral part of their overall IT strategy and road map. That percentage has grown to 54%, according to the "2018 State of the CIO survey," with 82% of the participating CIOs expecting their IT and security

strategies to be tightly integrated within the next three years.

Architecting a security infrastructure for today's demands

With cybersecurity becoming an integral element of not just the IT strategy but also the overall corporate strategy, organizations require new approaches and tools. This is especially true, given that companies have long had a love-hate relationship with cybersecurity solutions, which have been costly, complex, and sometimes counterproductive.

Historically, in fact, companies have considered their security and business needs to be engaged in something of a zero-sum game. That is, as security controls became more effective, they also became more intrusive and disruptive to employees. Asking employees to remember too many passwords or jump through multiple security hoops hurts both worker satisfaction and productivity. Conversely, easing back on security controls could expose companies to the significant risks discussed earlier.

The volume and speed of digital traffic today have exacerbated this push-pull dynamic. Inline security tools that can't keep up either take data samples or slow the delivery of data so they can examine it fully. Both options are unacceptable.

At the same time, integrating a collection of diverse security tools comprising both legacy and next-generation solutions can be inefficient and error-prone. Sprawling security infrastructures have become too complex to easily manage and modify, which also results in their becoming inflexible and unreliable.

Fortunately, there's an effective solution for the security challenges today's organizations face, as well as for many of their related business needs. The solution leverages next-generation network packet brokers, which serve as central orchestrators and clearinghouses for the security activity across an organization, including its satellite operations.

Many tools that need to see network traffic are not deployed in all network segments, so they can analyze only a sample of the traffic. Because they lack pervasive visibility into the entire network, these security tools can't identify all potential threats. By contrast, a sophisticated network packet broker can provide granular visibility into all segments of the network: physical, virtual, on-premises, or in the cloud. Enlisting the aid of a next-gen network packet broker, however, requires a new architectural approach to delivering security. In contrast to a highly distributed infrastructure, whose individual inline security tools may often be overwhelmed, this alternative architecture positions the next-gen network packet broker as a centralized traffic cop for the security tool "farm." This architectural security hub can monitor and analyze every piece of network traffic and then distribute the required traffic to the array of security tools surrounding it.

One next-gen network packet broker, the Gigamon GigaSECURE Security Delivery Platform, provides several traffic intelligence capabilities for performing tasks such as traffic deduplication, load balancing, creation of metadata, and distribution of traffic and metadata to the appropriate security tools. By intelligently brokering and distributing traffic, the centralized GigaSECURE Security Delivery Platform can greatly ease the burden on network and security endpoints.

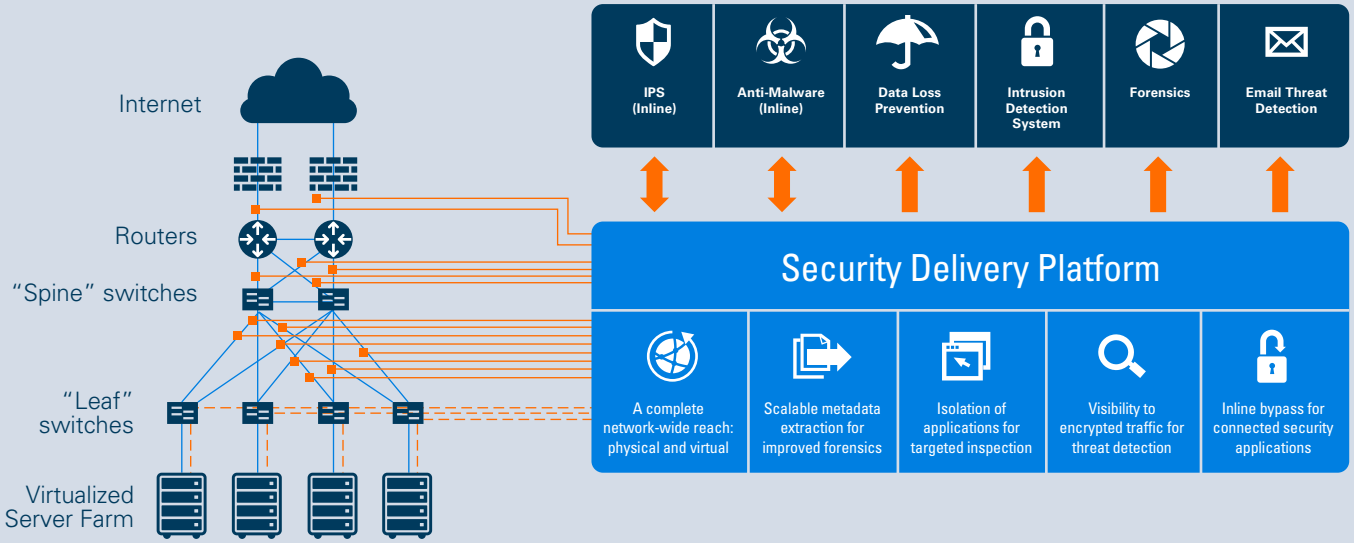
The Gigamon GigaSECURE Security Delivery Platform delivers both security and business benefits. On the security side of the ledger, it:

- Can monitor all network traffic across all network segments, rather than just partial traffic samples.
- Eliminates the problem of inline security tools becoming bottlenecks or being overwhelmed by large traffic volumes and speeds.
- Load-balances and distributes traffic, eliminating duplicated information and ensuring that each security tool and system receives only the data it needs in order to perform its function.
- Simplifies security infrastructure modifications and management, making it easy to add, integrate, or drop security tools from those distributed around the centralized security delivery platform.

Among the business benefits the GigaSECURE Security Delivery Platform confers:

- Complexity is reduced by individual security tools being integrated with the central platform rather than directly with one another. This architecture reduces development and management costs and delivers IT budget savings.

Figure 2. An Architectural Approach to Security



- IT and security personnel are freed from deploying and managing more-complex security environments and can devote their time to other strategic security needs.
- Companies can extend the life of legacy security systems and introduce next-gen tools and solutions, providing greater operational agility and effectiveness.

Gigamon Security Delivery Platform delivers cutting-edge security

Gigamon is the leading provider of security delivery platforms. The Gigamon platform provides comprehensive and consistent network visibility across an organization's entire network—whether physical, virtual, or in the cloud. Companies can deploy this solution on-premises or can tap a cloud-based version.

The Gigamon GigaSECURE Security Delivery Platform represents a next-gen network packet broker created from the ground up to provide a holistic view of network traffic and to distribute it to the appropriate security tools. Among its many functions, the GigaSECURE Security Delivery Platform can rapidly decrypt SSL traffic for inspection by security tools such as intrusion prevention systems and then re-encrypt it as needed.

By offloading many processor-intensive tasks, filtering traffic to targeted devices, and load-balancing traffic, the GigaSECURE Security Delivery Platform can enable organizations to cut the number of security devices installed by as much as 75%. In a total economic impact study conducted by Forrester, the analyst firm estimated that a typical organization of 5,000 employees could save $1.1 million on security hardware and software, plus an additional $1.5 million on staffing, over a three-year period.

Many companies already know that their current security tools and architectures can't keep pace with today's traffic volumes and speeds. That untenable situation means that too many organizations' cyberdefenses are porous and too many assets—and reputations—are at risk. CISOs find themselves in the hot seat, trying to patch together a security infrastructure while also fielding escalating demands from CEOs and other business executives.

Growing numbers of CISOs are coming to recognize that centralized architectures based on a security delivery platform can help them solve the bulk of their security and business challenges. Perhaps most importantly, this architectural approach can grow and evolve, both to respond to emerging cyberthreats and to accommodate new security tools and technologies.

For further information about the Gigamon GigaSECURE Security Delivery Platform, go to **https://www.gigamon.com/.**