2019 Cyberthreat Defense Report
Executive Summary
A CyberEdge Group Report

Platinum sponsor:

Gigamon®

Survey Demographics
- Responses from 1,200 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 17 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa
- Representing 19 industries

Notable Findings
- Cyberthreat trifecta. Of 11 categories of cyberthreats, malware is the greatest concern for responding organizations, followed closely by phishing and ransomware (see Figure 1).
- Healthy security budgets. The average security budget is increasing 4.9% in 2019 and represents 12.5% of an organization’s overall budget for IT.
- Threat hunting obstacle. The top inhibitor to achieving effective threat-hunting capabilities is the difficulty organizations are having implementing or integrating related tools.
- Security’s most wanted. Advanced security analytics tops the list as the #1 security technology planned for acquisition in 2019.
- Worsening skills shortage. More than four in five organizations (84.2%) are experiencing a shortfall of skilled IT security personnel, with the education (91.3%) and finance (87.5%) segments being the hardest hit.

Dealing With the Inevitable
The conclusion that no organization is immune from cyberattacks has never been clearer. When asked to estimate the number of times their organization’s network was compromised by a successful cyberattack within the past year, nearly four in five respondents (78%) admitted to at least one such incident, while nearly one third (32%) fell into the unenviable category of having been breached more than six times. The prospects for the coming year are equally daunting, as only 12% consider it “not likely” that their organizations will be breached in 2019. With successful attacks being pretty much inevitable these days, it is sensible – if not imperative – that organizations take meaningful steps to accelerate the processes for both threat detection and incident response activities.

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=1,193)

- Malware (viruses, worms, Trojans) - 3.74
- Phishing / spear-phishing attacks - 3.71
- Ransomware - 3.68
- Account takeover / credential abuse attacks - 3.68
- Denial of service (DoS / DDOS) attacks - 3.63
- Web application attacks (buffer overflows, SQL injections, cross-site scripting) - 3.62
- SSL-encrypted threats - 3.61
- Advanced persistent threats (APTs) / targeted attacks - 3.61
- Insider threats / data exfiltration by employees - 3.60
- Zero-day attacks (against publicly unknown vulnerabilities) - 3.60
- Drive-by downloads / watering-hole attacks - 3.59

Figure 1: Cyberthreats causing the greatest concern
Eliminating Blind Spots
Accelerating detection and response depends, in large part, on first establishing pervasive visibility. Without detailed information about what’s happening in those areas where threat actors and their “wares” could be lurking – which pretty much means every corner of an organization’s network – there is little assurance of being able to find them in the first place (not to mention stop them). Consistent, in-depth visibility across all of an organization’s physical, virtual, and cloud infrastructure holds the key to providing security teams with the network data that is essential to making a difference. Part of the challenge in this regard, of course, is the elimination of blind spots. And one big one that remains for many organizations is encrypted network traffic. When asked about the topic, a whopping 73.9% of our respondents agreed that efficiently decrypting SSL/TLS traffic so that it can be inspected for cyberthreats remains an issue for their organization. And let’s face it, the resulting need for decryption efficiency (and ideally centralization) is only going to grow as both the percentage and net volume of encrypted traffic continue to climb in today’s modern computing environments.

Increasing the Signal-to-Noise Ratio
Establishing pervasive visibility may very well be the key to accelerating detection and response capabilities, but organizations must take care to achieve this objective in a way that does no harm. In particular, the last thing today’s security teams need is another indiscriminate, mountain-sized haystack of security data to sort through. Just ask our survey participants, who identified having “too much data to analyze” as the #1 obstacle in their path to establishing effective cyberthreat defenses (see Figure 2). To be clear, too, the burden of excessive amounts of security data goes beyond the impact it has on overwhelmed SecOps personnel. The cost and complexity of an organization’s security tools/infrastructure is also driven upward with the ever-increasing need for greater performance/capacity. Successfully overcoming this complex web of challenges requires a solution – like a next-generation network packet broker – that is capable of providing complete coverage while minimizing the redundant distribution and processing of source data and the security events that are derived along the way. It’s all about getting the right intelligence and insights to your tools and teams, without overwhelming them.

Complimentary Report

About Gigamon
Gigamon is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise network. Our solutions accelerate threat detection and incident response times while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading Service Providers, Government Agencies as well as Enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100. Learn more at www.gigamon.com.

Figure 2: Inhibitors to establishing effective cyberthreat defenses

About CyberEdge Group
CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles. For information, connect to our website at www.cyber-edge.com.