2019 Cyberthreat Defense Report

Executive Summary

A CyberEdge Group Report

Platinum sponsor:

imperva

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

"Purchasing a separate product to complement an existing SIEM is the top approach for adding security analytics to an organization's cyberthreat defenses."

– 2019 CDR

CyberEdge Group's sixth annual Cyberthreat Defense Report provides a penetrating look at how IT security professionals perceive cyberthreats and plan to defend against them. Based on a survey of 1,200 IT security decision makers and practitioners conducted in November 2018, the report delivers countless insights IT security teams can use to better understand how their perceptions, priorities, and security postures stack up against those of their peers.

Notable Findings

- **Ruling the roost.** For the second year in a row, web application firewall (WAF) is identified as the most widely deployed application and data security technology.
- **Process insecurities.** Secure application development and testing is the security process organizations struggle with the most, followed by detection of insider attacks.
- **Powerful pairing.** Security analytics join threat intelligence services as top security management and operations technologies planned for acquisition in 2019.
- **Bringing the heat.** More than four in five respondents believe machine learning and artificial intelligence technologies are making a difference in the battle to detect advanced cyberthreats.
- **Under pressure.** At the same time that more than four in five organizations (84.2%) are experiencing a shortfall of skilled IT security personnel, security teams are struggling to deal with a growing mountain of security data.

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 ensuing response activities.

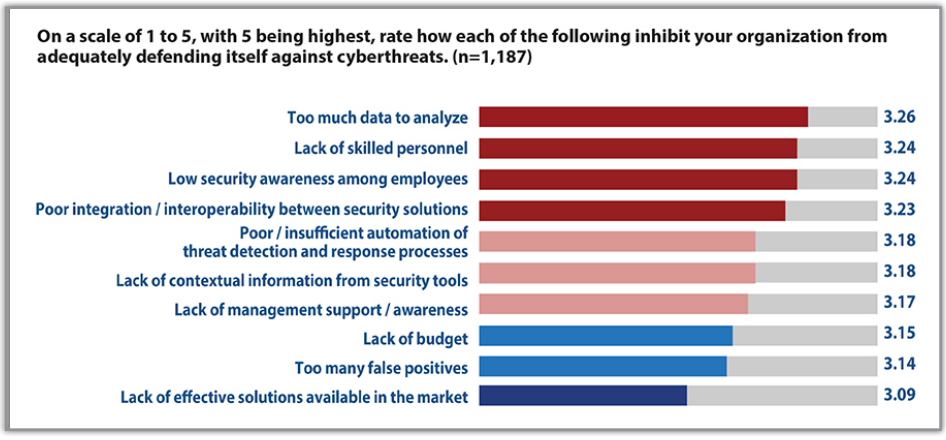

Figure 1: Inhibitors to establishing effective cyberthreat defenses

Answering the Call

The best way to accelerate one's detection and response capabilities becomes clear upon consideration of another problem: the mountains of security data with which today's security teams need to contend. Indeed, having "too much data to analyze" has been a top-three inhibitor to establishing effective cyberthreat defenses for all six years of the CDR. And, this time around, it finally claimed the top spot (see Figure 1). Based on anecdotal information we've been hearing for years about the "security data/event tsunami," this finding is not surprising to us. Neither are the related findings of advanced security analytics topping 2019's most wanted list for all technologies in this year's report, along with user and entity behavior analytics (UEBA), and threat intelligence services following close behind. Related solutions hold the promise not only of efficiently processing mountains of security events and other telemetry, but also of uncovering hidden threats and reducing the frequency of false positives. Add in the powerful benefits of rapidly maturing machine learning and artificial intelligence technologies and enterprise security teams could very well pull their collective heads above the waterline, finally.

Closing the Loop

To be clear, the value of threat intelligence and advanced analytics goes beyond the acceleration of detection and response capabilities. Consider the case of the most widely deployed application and data security technologies among our respondent organizations: web application firewalls (WAFs), database firewalls, and database activity monitoring (see Figure 2). Armed with the powerful combination of proactive intelligence and ongoing findings derived from advanced analytics engines, these crucial prevention and policy enforcement – focused defenses are also significantly enhanced. The gains are even multiplicative; as more threats are stopped in the first place, the result is less event "noise" to deal with, as well as fewer incidents requiring investigation and response.

Which of the following application and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard enterprise applications and associated data repositories against cyberthreats? (n=1,153)

	Currently in use	Planned for acquisition	No plans
Web application firewall (WAF)	63.0%	27.5%	9.5%
Database firewall	62.1%	27.2%	10.7%
Database activity monitoring (DAM)	56.1%	31.8%	12.1%
Database encryption / tokenization	55.6%	32.8%	11.6%
Cloud access security broker (CASB)	52.7%	32.1%	15.2%
File integrity / activity monitoring (FIM/FAM)	52.6%	34.0%	13.4%
API gateway / protection	51.2%	38.8%	10.0%
Container security tools / platform	50.5%	35.0%	14.5%
Runtime application self-protection (RASP)	49.9%	33.9%	16.2%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	49.3%	35.2%	15.5%
Application delivery controller (ADC)	48.1%	36.0%	15.9%
Deception technology / distributed honeypots	45.0%	36.8%	18.2%

Figure 2: Application and data security technologies in use and planned for acquisition

The Road Ahead

Security teams must ensure their organization's defenses keep pace with changes to both the IT infrastructure and the threats acting against it. The good news, at least for 84% of our survey respondents, is that their IT security budgets are expected to increase in 2019. When it comes to investing this windfall, some additional areas to consider include:

- Rapidly maturing risk quantification solutions that help optimize IT security decisions and investments;
- A container security platform (CSP) that provides full lifecycle security coverage for your burgeoning population of containerized apps and services; and
- A full-featured security orchestration, automation, and response (SOAR) solution capable of delivering faster incident response times while reducing the demands on your overburdened SecOps team.

Complimentary Report

For a complimentary copy of the full 2019 Cyberthreat Defense Report, connect to: www.imperva.com/cdr2019.

About Imperva

Recognized by industry analysts as a cybersecurity leader, Imperva champions the fight to secure data and applications wherever they reside. In today's fast-moving cybersecurity landscape, your assets require continuous protection, but analyzing every emerging threat taxes your time and resources. For security to work, it has to work for you. By accurately detecting and effectively blocking incoming threats, we empower you to manage critical risks, so you never have to choose between innovating for your customers and protecting what matters most. At Imperva, we tirelessly defend your business as it grows, giving you clarity for today and confidence for tomorrow. Imperva—Protect the pulse of your business. Learn more at www.imperva.com.

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.