2016 Cyberthreat Defense Report

Executive Summary

A CyberEdge Group Report

Platinum sponsor:

CITRIX®

Survey Demographics

- 1000 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 10 countries across North America, Europe, Asia Pacific, and Latin America
- Representing 19 industries

"With a respectable 52.4% deployment rate, application delivery controllers (ADCs) are clearly recognized as having evolved beyond their load balancing and performance optimization roots to be worthwhile app/data security platforms."

CyberEdge Group's third 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 1000 IT security decision makers and practitioners conducted in November 2015, 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

- **Dwindling optimism.** More than half (62%) of respondents expect their organization to be compromised by a successful cyberattack in 2016, up from 39% two years ago.
- **WAF takes top spot.** With a deployment rate expected to surpass 90% within 12 months, web application firewall (WAF) is the top-rated application and data-centric technology cited by respondents for defending their organization's applications and data repositories.
- **Mobile threats on the rise.** Two-thirds (65%) of respondents indicated there had been an increase in threats targeting their organization's mobile devices over the past year.
- **Backpedaling on BYOD.** The percentage of organizations with active BYOD policies/programs has dropped for the third year in a row – from 31% in 2014 to 26% in 2016.
- **Endpoint non-protection.** For three consecutive years, respondents have expressed growing dissatisfaction with their current endpoint security solutions.

Moving Beyond Mobile Device Management (MDM)

Respondents identified mobile devices as the IT domain where their cyberthreat defenses are currently weakest, with laptops and desktops not far behind. In addition, despite apparent difficulties getting BYOD programs off the ground in the past – which we attribute to the discovery that such programs are harder to establish, manage, secure, and sell to users than initially thought – more than half (53.2%) expect their organizations to do just that within the next two years. Along with the cited rise in mobile threats encountered over the past year, these findings point to the need for further investments in mobile security. As for the specific nature of these investments, respondents selected containerization/micro virtualization (39.5%), VPN to a cloud-based gateway (35.3%), and desktop virtualization (34.9%) as the top choices to augment the MDM (58.4%) and anti-virus/anti-malware solutions (62.5%) they already have in place (see Figure 1).

Which of the following mobile security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard mobile devices (smartphones and tablets), and corporate data accessed by mobile devices, against cyberthreats? (n=981)

2016

	Currently in use	Planned for acquisition	No plans
Mobile device anti-virus / anti-malware	62.5%	27.3%	10.2%
Mobile device / application management (MDM/MAM)	58.4%	31.5%	10.1%
VPN to on-premises security gateway	57.1%	30.4%	12.5%
Network access control (NAC)	56.4%	31.5%	12.1%
Mobile device file / data encryption	55.2%	31.4%	13.4%
VPN to cloud-based security gateway	52.3%	35.3%	12.4%
Virtual desktop infrastructure (VDI)	49.8%	34.9%	15.3%
Containerization / micro-virtualization	40.2%	39.5%	20.3%

Figure 1: Mobile security technologies in use and planned for acquisition.

Targeting Web Applications

Web applications are a target of choice for threat actors for many reasons, not the least of which is their high likelihood of including vulnerabilities and serving as a direct conduit to sensitive data. It is not surprising, therefore, that web application attacks continue to be a significant concern for security professionals, who remain far from confident about their organization's security posture in this business-critical area (see Figure 2). Adding even more fuel to the fire is the rise of automated threats. Defined in detail by the Open Web Application Security Project in its recent handbook on the topic, this newly designated class of threats is the latest/greatest scourge plaguing the vast array of web applications upon which today's businesses have come to rely.

Seeking Endpoint Security Alternatives

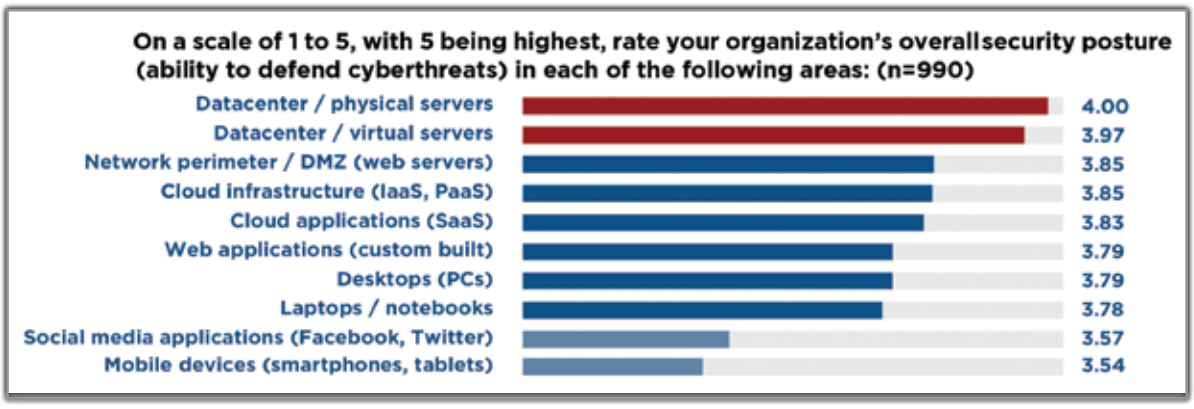

Figure 2: Perceived security posture by IT domain.

The effectiveness of traditional endpoint security solutions, especially those that rely on signature-based detection mechanisms, has been in question for some time. However, with advanced malware now featuring countless tricks – such as polymorphism, active sandbox deception, and the ability to erase all traces of its presence after striking – the verdict is clearly in. In fact, enterprise dissatisfaction couldn't be more clear, as a whopping 86% of respondents indicated their organization's intent to either replace (42%) or augment (44%) their current endpoint defenses. As for how they plan to remedy this situation, respondents selected containerization and micro/application virtualization (37.9%) as the top endpoint security technologies planned for acquisition in 2016. Solutions that enable self-remediation for infected endpoints were also designated as a high priority (35.9%).

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 74% of our survey respondents, is that their IT security budgets are expected to increase in 2016. When it comes to investing this windfall, some *additional* areas to consider include:

- User/entity behavior analytics and other user-centric security solutions;
- Advanced web application protection technologies capable of thwarting emerging automated threats; and
- Development of a formal cyberthreat hunting practice to better detect and isolate advanced threats.

Complimentary Report

For a complimentary copy of the full 2016 Cyberthreat Defense Report, connect to: http://more.citrix.com/cyberthreat.

About Citrix

Citrix is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. Citrix solutions are in use at more than 400,000 organizations and by over 100 million users globally. Learn more at http://www.citrix.com/appfirewall.

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.

CYBEREDGE GROUP