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

- **Inevitable breaches.** Nearly four in five organizations (78.0%) were victims of at least one successful cyberattack in 2018, while nearly two-thirds (65.2%) expect to get hit again in 2019.

- **Cyberthreat trifecta.** Of 11 categories of cyberthreats, malware is the greatest concern for responding organizations, followed closely by phishing and ransomware.

- **Process insecurities.** Secure application development and testing is the security process organizations struggle with the most, followed by detection of insider attacks.

- **Burgeoning biometrics.** Biometrics is the most sought-after identity and access management technology in 2019.

- **TIPping the scales.** Enterprises are sourcing threat intelligence platforms (TIPs) to improve cyberthreat detection and validate security alerts.

Data/Apps Remain Center Stage

Every high-profile breach and exposure of customer or proprietary information brings renewed pressure to ensure the protection of not only the sensitive data in your organization’s possession, but also the business applications that provide access to and/or rely on it. At the same time, achieving compliance with applicable data security and privacy regulations requires complete visibility and control of which data and applications are being accessed by which users and systems. It is not surprising, therefore, to see organizations focusing heavily on the areas of application and data security, once again. Related findings include (a) data encryption and tokenization being among the most widely deployed application and data security technologies, and (b) the emergence of the API gateway as one of the top technologies planned for acquisition in 2019 (see Figure 1).

![Figure 1: Application and data security technologies in use and planned for acquisition](image)
Cutting Through the Noise
Having “too much data to analyze” has been a top-three inhibitor to establishing effective cyberthreat defenses for all six years of the CDR. This time around, it finally claimed the top spot (see Figure 2). Based on anecdotal information we’ve been hearing for years – for example, 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), full-packet capture and analysis, 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 – which a whopping 81% of respondents believe are materially helping to defeat advanced cyberthreats – and enterprise security teams could very well pull their collective heads above the waterline, finally.

Overcoming the Skills Shortage
With 84% of organizations experiencing a shortage of IT security talent, it makes sense to see “lack of skilled personnel” near the top of Figure 2. This pervasive short-handedness emphasizes the need for security products that, simply put, get the job done. Enter security orchestration, automation, and response (SOAR). Emerging offerings promise to do everything from stitching together all of an organization’s disparate policy enforcement infrastructure and event management systems, to handling playbook coding and execution. The general idea is to bring a new level of automation, speed, and accuracy to every corner of the security operations landscape – from vulnerability and patch management to incident response. Of course, engaging outside assistance – in the form of seasoned consulting firms and/or managed security service providers (MSSPs) – is another practical way to address the security talent shortfall. In fact, with nine on 10 respondents’ organizations leveraging an external provider for one or more security services, it’s more than just a practical approach for filling one’s gaps; it’s a proven one.

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

About DXC Technology
As the world’s leading independent, end-to-end IT services company, DXC Technology (NYSE: DXC) leads digital transformations for clients by modernizing and integrating their mainstream IT, and by deploying digital solutions at scale to produce better business outcomes. The company’s technology independence, global talent, and extensive partner network enable 6,000 private and public-sector clients in 70 countries to thrive on change.

Together DXC and Micro Focus help organizations worldwide transform their IT and business processes to reap the benefits of a secure, productive and profitable digital future. Learn more at www.dxc.technology/microfocus.

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.

© 2019 CyberEdge Group, LLC. The CyberEdge Group name and logo are trademarks of CyberEdge Group, LLC. All other trademarks and service marks are the property of their respective owners.