CyberEdge Group’s seventh 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 2019, 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**

- **No rest for the weary.** A record 81% of organizations experienced at least one successful cyberattack last year, 35% suffered six or more, and 69% expect to be compromised this year.

- **Diverse threats.** IT teams worry about a wide range of cyberthreats, led by malware, phishing, ransomware, account takeover, and denial of service attacks.

- **Help wanted.** The vast majority (85%) of organizations are experiencing an IT security skills shortfall, and the gap grew in all but one job category.

- **Network security plans.** Network security technologies planned for acquisition in 2020 include network behavior analysis (NBA), SSL/TLS decryption, and denial of service (DoS/DDOS) prevention.

- **Decryption deficit.** Surprisingly, only 34% of SSL/TLS-encrypted web traffic is decrypted for inspection.

**Challenges Collecting and Analyzing Security Data**

The top two barriers to establishing effective cyberthreat defenses are people-related: lack of skilled personnel and low security awareness among employees. But the next four key challenges (too much data to analyze, insufficient automation of threat detection and response, lack of contextual information, and poor integration between security solutions) relate to collecting and analyzing huge quantities of security data scattered across the enterprise. CyberEdge believes enterprises will be addressing these challenges in the coming year.

### Inhibitors to Establishing Effective Cyberthreat Defenses (Scale of 1 to 5, with 5 Highest)

- **Lack of skilled personnel**: 3.59
- **Low security awareness among employees**: 3.59
- **Too much data to analyze**: 3.55
- **Poor / insufficient automation of threat detection and response processes**: 3.54
- **Lack of contextual information from security tools**: 3.53
- **Poor integration / interoperability between security solutions**: 3.52
- **Lack of management support / awareness**: 3.52
- **Too many false positives**: 3.51
- **Lack of effective solutions available in the market**: 3.50
- **Lack of budget**: 3.45
Encrypted Web Traffic Remains an Issue
Today 56% of organizations have technology for SSL/TLS decryption, but only 35% of SSL/TLS traffic is actually decrypted for inspection. Given that threat actors are concealing malware and command and control messages in encrypted web traffic, this leaves way too big a blind spot! The decryption deficit is caused by IT teams turning off decryption in web gateways and devices that perform decryption inefficiently, and by SPAN (Switched Port Analyzer) connections that drop traffic to security tools when switches are overloaded. We expect to see the percentage of SSL/TLS traffic decrypted and inspected go up in coming years as organizations deploy technologies that collect and decrypt network traffic more efficiently.

Security Analytics Surging
In last year’s survey, advanced security analytics was installed in 41% of organizations. This year it was in use in 57%. IT is extremely rare for a security technology to be deployed in so many new organizations (16%) over just one year. Behind this surge is the fact that security analytics has been found useful (really, essential) to help IT security teams dig through masses of data and respond quickly to threats. The top use cases include detecting insider threats, investigating incidents, analyzing network traffic for anomalies, identifying compromised accounts, detecting data exfiltration, and hunting for cyberthreats.

How My Organization is Using Security Analytics Products

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detecting insider threats</td>
<td>47.0%</td>
</tr>
<tr>
<td>Investigating security events / incidents</td>
<td>46.8%</td>
</tr>
<tr>
<td>Analyzing network traffic for anomalies that may indicate a potential attack</td>
<td>46.1%</td>
</tr>
<tr>
<td>Identifying accounts that may have been compromised</td>
<td>45.3%</td>
</tr>
<tr>
<td>Detecting data exfiltration</td>
<td>44.7%</td>
</tr>
<tr>
<td>Detecting improper user account usage, such as shared accounts</td>
<td>44.7%</td>
</tr>
<tr>
<td>Hunting for cyberthreats</td>
<td>44.0%</td>
</tr>
<tr>
<td>Demonstrating compliance during audits</td>
<td>38.4%</td>
</tr>
<tr>
<td>Conducting forensic investigations</td>
<td>32.8%</td>
</tr>
</tbody>
</table>

Complimentary Report

About Gigamon
Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

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](http://www.cyber-edge.com).