Secure the Digital Transformation

Corporations are continually looking for ways to increase productivity and efficiency. Taking advantage of technology advances in their networks is a proven way to be more agile while reducing costs.
Customers, employees, vendors and partners use mobile applications, chat bots, online portals, email and other tools to interact with brands daily. Every touchpoint adds a layer of complexity to the network that can introduce new, risky attack vulnerabilities.

C-suite executives understand that, to transform their businesses, they must embrace the integration of new technologies while at the same time protect data privacy. According to Radware’s 2018 Executive Application & Network Security Survey, respondents ranked improvement of information security and business efficiency as their main goals. Creating a competitive advantage and improving the customer experience closely followed. Half of the executives (47%) also recognized that digital transformation activities place pressure on their organizations’ security planning and investment strategy.

**REGIONAL DIFFERENCES: AMER**

*Creation of New Revenue Sources*

Creating new sources of revenue was more important to AMER respondents versus other regions.

**RANKING OF NEW REVENUE SOURCES AS A TOP 3 GOAL**

- **AMER**: 32%
- **EMEA**: 13%
- **APAC**: 18%

**PERCENTAGE OF C-SUITE RESPONDENTS WHO ARE GREATLY CONCERNED ABOUT DATA PRIVACY**

- **70%** AMER AND EMEA EXECUTIVES
- **80%** APAC EXECUTIVES
MIGRATION TO MULTIPLE CLOUDS INTRODUCES NEW SECURITY CONCERNS

More than 90% of executives reported using multiple public and private cloud environments as part of their companies’ IT infrastructure. Responses indicated that most organizations host 25% to 50% of their business applications in the cloud.

KEY FINDING:

C-suite executives clearly understood that dispersing their network across multiple public and private clouds introduced security risks. The vast majority of respondents (96%) were “very” or “somewhat” concerned about network vulnerabilities.

PERCENTAGE OF BUSINESS APPLICATIONS THAT RUN IN A CLOUD ENVIRONMENT

<table>
<thead>
<tr>
<th>% OF APPLICATIONS RUNNING IN THE CLOUD</th>
<th>% OF RESPONDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>9%</td>
</tr>
<tr>
<td>50%</td>
<td>46%</td>
</tr>
<tr>
<td>25%</td>
<td>43%</td>
</tr>
<tr>
<td>0%</td>
<td>2%</td>
</tr>
</tbody>
</table>
READY TO TAKE ADVANTAGE OF AUTOMATION

As attack vulnerabilities multiply in increasingly complex networks, over the past two years the majority (71%) of executives reported shifting more of their network security budget into technologies that employ machine learning and automation. About 25% said that the focus of their budgets remained unchanged in this time period.

KEY FINDING:
Even though executives said that they were ready to benefit from automated security protections, manual processes are still a sizable part (46%) of policy enforcement, leaving them open to costly human error.

PERCENTAGE OF SECURITY BUDGET ALLOCATED FOR AUTOMATED SECURITY SYSTEMS

39%

Portion of the security budget across all regions devoted to security systems with automation

REGIONAL DIFFERENCES: APAC

Trust Factor

Globally, nearly four in 10 executives trust automated systems more than humans to protect them against cyberattacks.

In APAC, more than half of the respondents said that they trusted automated systems more than humans.
DevOps STAND ALONE

In the rush to bring new customer experiences to market, organizations may skip critical security checks, leaving them open to vulnerabilities that could have been mitigated. While some companies have implemented basic security measures, there’s a lot left to chance.

EXECUTIVES REPORTED THAT THEY ARE NOT YET INTEGRATING SECURITY PRACTICES INTO THE APPLICATION DEVELOPMENT CYCLE.

Companies that included security as part of their DevOps process reported a nearly even division between automated and manual policy enforcement.

UNCERTAINTY ABOUT ENCRYPTED TRAFFIC

As more transactions flood the internet, the volume of encrypted traffic is rising. According to Google’s Transparency Report, HTTPS encrypted traffic across all platforms (Windows, Android, Chrome, Linux and Mac) has grown about 50% since 2015.

The secure sockets layer (SSL) protocol has been the de facto encryption technology since the early 1990s. Highly publicized vulnerabilities resulted in the development of other protocols such as transport layer security (TLS).

According to the Radware 2017–2018 Global Application and Network Security Report\(^2\), 30% of businesses reported suffering an SSL-based attack, with another one in four not certain whether they had experienced such an attack. SSL-based attacks can take many forms, including encrypted SYN Floods, SSL Renegotiation, HTTPS Floods and encrypted web application attacks.

Executives included encrypted attacks on the list of cyberattacks that they viewed as most detrimental. Respondents from AMER (45%) were most likely to cite encrypted attacks as a concern, followed by EMEA (41%).

Many companies operate without protection from encrypted attacks. Part of the challenge they face is that they are unsure about the legalities of decrypting traffic for inspection because of government regulations such as HIPAA and the new GDPR requirements. Many organizations leveraged a WAF and/or ADC to monitor inbound traffic, particularly in AMER (47%).

**COMPLIANCE COMPLICATIONS**

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>22%</td>
<td></td>
</tr>
<tr>
<td>13%</td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td></td>
</tr>
</tbody>
</table>

SSL Web Policy

Still reviewing the legalities of decrypting traffic on their networks

---