The Future of IT Network Security

Digital transformation and work-from-home policies are forcing organizations to choose between user experience and security.
Digital transformation has been accelerated by the COVID-19 global pandemic. Users are increasingly logging in to on-premises applications, cloud apps, and Software as a Service (SaaS) platforms from outside the data center in home offices, kids’ rooms, and the dining room table. During the past year, IT departments have scrambled to empower newly remote employees, seeking ways to enable ubiquitous application access and improve network performance.

But the acceleration of the “Future of Work” has come at a cost. Business continuity concerns have caused organizations to focus on improving the user experience for remote employees at the expense of security. Malicious actors have noticed, taking advantage of these gaps in cybersecurity policies to target users who now find themselves outside the organization’s security reach. Performance issues caused by latency are making IT professionals reluctant to impose the same security policies that existed inside the office to users who now work primarily from home.

Menlo Security conducted research to capture the concerns of IT professionals at U.S.-based organizations as they grapple with accelerated digital transformation. Here are the results:

**Key Findings**

- Digital transformation has led to the increasing popularity of SaaS, enabling more employees to access the network from any location.
- IT decision makers agree that new technologies should integrate seamlessly rather than impede existing network and security infrastructure.
- Eight out of ten IT decision makers have experienced a security breach of some kind, while 40 percent feel these threats are increasing in numbers.
- Despite the expectation of increased compliance and regulatory requirements over the next two years, IT decision makers recognize the need to support a hybrid IT model to accommodate a home office/work balance.
- IT decision makers are concerned that digital transformation is increasing the security risk, but they are more worried about how new security policies may impact employee productivity.
Whether through SaaS platforms, new cloud apps, or traditional on-premises solutions, each access point is a vulnerability that needs to be protected from malicious actors. This expanding threat surface will only expand as new technologies such as the Internet of Things (IoT) and artificial intelligence (AI) continue to mature. And it will become increasingly difficult to integrate these new technologies with existing network and security infrastructure. It’s possible that a new way to nondisruptively deliver security services to users will be needed.

The majority of IT decision makers agree: It’s very important that new technology doesn’t impact their security posture, and that it’s easy to integrate with their existing architecture (62%).

Digital transformation has seen an increased use of SaaS (68%) and enabled more employees to access the network from any location (66%).
Insight #2:
Things will get worse if changes aren’t made now

It’s clear that things will never go back to the way they were. The shift to remote work was already happening. It’s likely that a large percentage of the workforce will continue to work away from corporate headquarters, and the pressure to deliver office-like experiences at the expense of security will be enormous. This situation will greatly expand threat surfaces, create security gaps, and put tremendous strain on enterprise security teams. Breaches will continue to happen at an accelerated pace.

Roughly what % of the workforce is working remotely as a result of COVID-19?

<table>
<thead>
<tr>
<th>Percentage Working Remotely</th>
<th>Mean: 62%</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%-24%</td>
<td>8%</td>
</tr>
<tr>
<td>25%-49%</td>
<td>21%</td>
</tr>
<tr>
<td>50%-74%</td>
<td>38%</td>
</tr>
<tr>
<td>75%-100%</td>
<td>35%</td>
</tr>
</tbody>
</table>

For the majority (73%), at least 50% of their workforce is now working from home.

81% of employees have had their Internet access impacted by COVID-19, over half (56%) have experienced slow access speeds, and two fifths (40%) have had poor connectivity.

What impact has COVID-19 had on employees’ access to the Internet?

- Slow Access Speeds: 56%
- Poor Connectivity: 40%
- No or Loss of Access to Resources: 35%
- Decreased Productivity Due to Increased Security Process: 33%
- Downtime: 33%

81% of employees have had their Internet access impacted by COVID-19, over half (56%) have experienced slow access speeds, and two fifths (40%) have had poor connectivity.
Insight #2:
Things will get worse if changes aren't made now (continued)

81% of respondents have experienced a security breach of some kind, 41% of which feel that the number of threats is increasing.

Have you or your organization experienced any of the following when it comes to the security around accessing the Internet since COVID-19?

- Increased Number of Threats: 41%
- Increased Complexity of Threats: 36%
- Difficulty Containing/Resolving Threats: 35%
- Lack of Awareness/Oversight of Security Threats: 30%
- None of the Above: 19%

Base: All respondents (200)/All who have experienced some kind of threat (163)

Which of the following threats have you experienced?

- Email and Web Threats: 60%
- Internet of Things (IoT)-Based Threats: 42%
- Cloud Application Attacks: 42%
- Open Source Software-Based Attacks: 34%
- Public Cloud Misconfigurations: 26%

N.B.B. Other = 1%

Base: All respondents (200)/All who have experienced some kind of threat (163)

Email and web threats are still causing the most damage (60%).
Insight #3:

**User experience is the priority**

Nearly everyone agrees that compliance and regulatory requirements are likely to get tougher in the next two years. Coupled with the pressures resulting from accelerated digital transformation and work-from-home policies, security teams are well aware that they’re going to have to up their security game. However, the user experience will continue to be the priority. Striking the balance between accessibility and security will depend on the adoption of new cloud-based security solutions.

In addition to anticipating an increase in compliance and regulation over the next two years, IT decision makers recognize the need to support a hybrid IT model to accommodate a home/office work balance (80%).

**To what extent do you agree with the following statements?**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Agree</th>
<th>Strongly Agree</th>
<th>% Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Will Need to Better Support the User Experience</td>
<td>46%</td>
<td>41%</td>
<td>87%</td>
</tr>
<tr>
<td>We Will See an Increased Level of Compliance and Regulations for Internet Access in the Next 2 years</td>
<td>45%</td>
<td>37%</td>
<td>82%</td>
</tr>
<tr>
<td>IT Will Have to Support a Hybrid IT Model to Accommodate a Home/Office Work Balance</td>
<td>35%</td>
<td>45%</td>
<td>80%</td>
</tr>
<tr>
<td>Direct-to-Cloud Connectivity Will Be Required in the Next Two Years</td>
<td>34%</td>
<td>44%</td>
<td>78%</td>
</tr>
<tr>
<td>We Will Need to Rethink Remote Access/VPN in the Future</td>
<td>42%</td>
<td>36%</td>
<td>78%</td>
</tr>
<tr>
<td>Circuit and Network Equipment Will Be Cheaper</td>
<td>40%</td>
<td>28%</td>
<td>68%</td>
</tr>
</tbody>
</table>

**Which of the following are your top priorities for the next five years?**

- Improve Security: 56%
- Increase Efficiencies: 51%
- Increase Profits: 42%
- Reduce Costs: 41%
- Grow the Team: 30%
- Expand Skills: 22%
- Be More Compliant: 19%

N.B.B. Other = 1%

Improving security (56%) and increasing efficiencies (51%) are the top two priorities for business in the next five years.
Insight #3:  
**User experience is the priority (continued)**

Private access to the public cloud and a cloud-level security model will be priorities in the short term, while growth or deployment of CASB is a longer-term priority.

### Which of the following use cases does your organization plan to address in the next two to five years?

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Within the Next 2 Years</th>
<th>Within the Next 5 Years</th>
<th>No Plans to Implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Access to Public Cloud Development Environments</td>
<td>62%</td>
<td>31%</td>
<td>8%</td>
</tr>
<tr>
<td>Adopt a Cloud-Level Security Model</td>
<td>59%</td>
<td>23%</td>
<td>9%</td>
</tr>
<tr>
<td>Users’ Access to Internal Apps Like Salesforce, Bamboo, G Suite, etc.</td>
<td>56%</td>
<td>32%</td>
<td>13%</td>
</tr>
<tr>
<td>Adopt a New Web Application and API Protection (WAAP)</td>
<td>55%</td>
<td>31%</td>
<td>14%</td>
</tr>
<tr>
<td>Move to a Cloud-Based Firewall as a Service (FWaaS) for Branch-to-Branch Connectivity</td>
<td>52%</td>
<td>36%</td>
<td>13%</td>
</tr>
<tr>
<td>Endpoint VRF Replacement (Zero Trust Network Access)</td>
<td>48%</td>
<td>40%</td>
<td>13%</td>
</tr>
<tr>
<td>Remote, Third-Party Contractors Accessing Internal Resources</td>
<td>47%</td>
<td>36%</td>
<td>17%</td>
</tr>
<tr>
<td>Move to a Cloud-Based SWG/Proxy</td>
<td>45%</td>
<td>40%</td>
<td>16%</td>
</tr>
<tr>
<td>Public Internet Access to Allow Access to Rolly Websites</td>
<td>45%</td>
<td>27%</td>
<td>25%</td>
</tr>
<tr>
<td>Implement SD-WAN Across the Network</td>
<td>44%</td>
<td>39%</td>
<td>18%</td>
</tr>
<tr>
<td>Deploy or Grow CASB Deployment</td>
<td>39%</td>
<td>43%</td>
<td>19%</td>
</tr>
</tbody>
</table>

Base: All respondents (200)

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Within the Next 2 Years</th>
<th>Within the Next 5 Years</th>
<th>No Plans to Implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000–2,999 Employees</td>
<td>44%</td>
<td>33%</td>
<td>23%</td>
</tr>
<tr>
<td>3,000–4,999 Employees</td>
<td>46%</td>
<td>32%</td>
<td>22%</td>
</tr>
<tr>
<td>5,000–10,000 Employees</td>
<td>46%</td>
<td>32%</td>
<td>22%</td>
</tr>
<tr>
<td>10,000+ Employees</td>
<td>45%</td>
<td>43%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Larger Organizations More Likely to Have Fully Implemented SASE

Base: All respondents, excluding “I don’t know” (192)

### Where are you on your SASE (Secure Access Service Edge)-based architecture?

Overall, 79% have fully or partially implemented SASE.

### Which of the following do you see as challenges in your digital transformation journey?

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased Security Risk Due to Increased Remote Working</td>
<td>52%</td>
</tr>
<tr>
<td>Budget Constraints</td>
<td>50%</td>
</tr>
<tr>
<td>Reduced Employee Productivity Due to Increased Security Measures</td>
<td>39%</td>
</tr>
<tr>
<td>Not Being Able to Provide a Rich User Experience (Fast Access)</td>
<td>27%</td>
</tr>
<tr>
<td>Lack of Oversight on Security Due to Direct Cloud Access</td>
<td>22%</td>
</tr>
</tbody>
</table>

Base: All respondents (200)
Rethink IT network security

Enterprises are facing a major dilemma: Expand accessibility to remote users or clamp down on growing cybersecurity threats. What if you could do both? It’s possible, but it’s going to take a radically new approach to delivering security services to distributed users, applications, and devices.

Many organizations are moving security to the cloud as part of the network itself, making it infinitely scalable and adaptable to wherever users log in. Policies can be applied through the cloud in a seamless, frictionless way—essentially extending data center visibility and control to home offices.

Learn more at www.menlosecurity.com
Menlo Security surveyed 200 IT decision makers in the U.S. who work for companies with more than 1,000 employees. The firm sent invitations via email in October 2020 and followed up with a link to the survey for targets who responded. Results are accurate to ±6.9 percent at 95 percent confidence limits, assuming a result of 50 percent.

**Business Size**

- 10,000+ Employees: 31%
- 5,000–10,000 Employees: 19%
- 3,000–4,999 Employees: 19%
- 1,000–2,999 Employees: 32%

**Job Role**

- CIO: 12%
- CISO: 3%
- IT Manager: 66%
- Other IT Role: 15%
- Non-IT-Related Executive Role: 5%

**About Menlo Security**

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It’s the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2021 Menlo Security, All Rights Reserved.