COVID-19 IMPACT ON SECURE REMOTE ACCESS REPORT

By Fudo Security
Only session management and recording can fully protect companies from these types of threats.

37% of respondents have these tools and 21.2% are considering adding them in the near term.

**Most desired features of a secure remote access solution:**

1. Authentication and authorization / MFA
2. Encrypted connection
3. Single Sign-on
4. User Access Gateway (website) to easy access
The world has experienced an unparalleled change in 2020. The global COVID-19 pandemic has affected our economy and our lives. It’s brought about changes to both the physical, as well as our digital world. The threat for cyberattacks continues to rise.

We’ve observed that since the onset of COVID-19, attacks and breaches have risen in all sectors and all across the globe. Cybercriminals have shown no mercy, and now even certain nation-state actors have escalated their activity in these times of crisis. Protecting and safeguarding data and businesses is a complex and never-ending challenge.

As one of the leading vendors in Zero-Trust and PAM industry, we’ve gone to the core of the issue and created a unique survey to more closely analyze and understand the link between secure remote access and the effects of the pandemic on businesses and organizations.

Our questions were answered by top tier cybersecurity managers, as well as senior executives and industry decision-makers. The majority of individuals we surveyed are based in the US, as well as Europe, Asia, and the MENA region.

We’ve been able to gain a dynamic insight into how top cybersecurity managers have been dealing with the changes to their remote access strategy in light of the COVID-19 impact.

This report explores the survey results around the ways of securing remote access and plans for future cybersecurity investments.

We are proud to present to you our: COVID-19 Impact on Secure Remote Access report.
PERCENTAGE OF EMPLOYEES ABLE TO WORK REMOTELY

Respondents were asked to report the percent of employees able to work remotely prior to the COVID-19 pandemic and during it. Statistical analysis showed a significant increase in the percentage of employees able to work remotely during the COVID-19 pandemic (77.3%). The bar graph below shows the average change across all countries.

Percentage of employees able to work prior to the COVID-19 pandemic and during it.

STATISTICAL ANALYSIS SHOWED A SIGNIFICANT INCREASE IN THE PERCENTAGE OF EMPLOYEES ABLE TO WORK REMOTELY DURING THE COVID-19 PANDEMIC (77.3%).
On top of the 27% increase in remote workers, some of the companies have stated their plan to not ask their employees to return to the office at all. While this certainly saves organizations money that they would normally spend on office costs, it imposes a number of risks, including unauthorized access, system breaches, and finally, efficiency control.

- **Approximately what percentage of your employees were able to work remotely before the COVID-19 pandemic?**
  - 39.3%
  - 60.7%

- **Approximately what percentage of your employees are currently working remotely?**
  - 22.7%
  - 77.3%

- **Approximately what percentage of your infrastructure is in the cloud?**
  - 46.6%
  - 53.4%
Respondents were asked to list which SRA tools their companies currently use. 

<table>
<thead>
<tr>
<th>Secure Remote Access Tool</th>
<th>Percent Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Factor Authentication</td>
<td>84.3%</td>
</tr>
<tr>
<td>SSL VPNs</td>
<td>81.9%</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>57.8%</td>
</tr>
<tr>
<td>Privileged Access Management</td>
<td>50.6%</td>
</tr>
<tr>
<td>Virtualization Systems with Remote access</td>
<td>49.4%</td>
</tr>
<tr>
<td>Session Monitoring and Recording</td>
<td>37.3%</td>
</tr>
<tr>
<td>Software Defined Perimeter</td>
<td>14.5%</td>
</tr>
<tr>
<td>Employee Efficiency Monitoring</td>
<td>7.2%</td>
</tr>
</tbody>
</table>

Multi-Factor Authentication and SSL VPNs are by far the most common SRA tools used. This is followed by identity and access management, privileged access management, virtualization systems with remote access, and session monitoring/recording. All other SRA tools were not endorsed by a large percentage of respondents. Respondents reported their greatest perceived security threats to be: Malware (28.9%), misuse by staff (26.5%), and threats related to vendors, third-parties or freelancers (21.7%). Deliberate actions of employees and contractors along with human error make up the biggest cybersecurity risk for any organization.
DELIBERATE ACTIONS OF EMPLOYEES AND CONTRACTORS ALONG WITH HUMAN ERROR MAKE UP THE BIGGEST CYBERSECURITY RISK FOR ANY ORGANIZATION.
Currently used tools do not relieve the fears of cybersecurity managers:

- VPN - lacks monitoring and full access control
- Password Manager - doesn’t provide network security
- IAM - takes time to deploy and is cumbersome

A PAM-based secure remote access solution would address the biggest risk - users with privileges.

When asked what features their ideal SRA tool would have, respondents reported endorsing the ones below:

<table>
<thead>
<tr>
<th>Ideal Remote Access Tool Features</th>
<th>Percent Endorsing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and authorization / MFA</td>
<td>78.3%</td>
</tr>
<tr>
<td>Encrypted connection</td>
<td>72.3%</td>
</tr>
<tr>
<td>Single Sign-on</td>
<td>60.2%</td>
</tr>
<tr>
<td>User Access Gateway (website) to easy access</td>
<td>42.2%</td>
</tr>
<tr>
<td>Session Recording and Monitoring</td>
<td>37.3%</td>
</tr>
<tr>
<td>Efficiency Analysis (how your remote employees/vendors perform)</td>
<td>31.3%</td>
</tr>
<tr>
<td>Prevention</td>
<td>28.9%</td>
</tr>
<tr>
<td>Ability of using standard client applications like Putty or MSFT RDP</td>
<td>26.5%</td>
</tr>
</tbody>
</table>

Has your company invested in any new secure remote access solutions during the COVID-19 pandemic?

- Yes: 71.1%
- No: 28.9%

Are you going to reevaluate your Secure Remote Access tools in the near future?

- Yes: 45.8%
- No: 21.7%
- Don’t know: 32.5%
COVID-19-RELATED BEHAVIORS

53.6% of respondents will abandon current systems.

22.9% of respondents were attacked during COVID.

42.2% of respondents’ priorities changed during pandemics.

19.3% Yes
38.6% No
53.6% Maybe
Overwhelmingly the world has seen a surge in attacks and breaches during the COVID-19 pandemic. More than a quarter of respondents indicated that they have taken steps to invest in new SRA tools. However, there’s still more that organizations need to do to ensure they are adequately protected against breaches both from internal and external threats. 22.9% had suffered an attack or disruption during the pandemic.

28.9% of respondents invested in new tools since COVID.

Are you going to reevaluate your Secure Remote Access tools in the near future?

- No plans to change: 45.8%
- Yes, looking for a better solution: 32.5%
- Undecided: 21.7%
22.9% of respondents reported experiencing a remote attack or disruption during the pandemic.
30% of respondents want better SRA solutions.
Which tools are being considered as a supplement to current solutions?

<table>
<thead>
<tr>
<th>Secure Remote Access Tool</th>
<th>Percent Considering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Systems with Remote access</td>
<td>49.4%</td>
</tr>
<tr>
<td>Virtual Desktop Infrastructure</td>
<td>39.8%</td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>26.5%</td>
</tr>
<tr>
<td>Session Monitoring and Recording</td>
<td>21.7%</td>
</tr>
<tr>
<td>Software-Defined Perimeter</td>
<td>20.5%</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>20.5%</td>
</tr>
<tr>
<td>Privileged Access Management</td>
<td>19.3%</td>
</tr>
<tr>
<td>SSL VPNs</td>
<td>18.1%</td>
</tr>
<tr>
<td>Employee Efficiency Monitoring</td>
<td>15.7%</td>
</tr>
</tbody>
</table>

Have your cybersecurity priorities for this year changed because of the pandemic?

- Yes: 42.2%
- No: 38.6%
- Not yet, but they may: 19.3%

What do you see as the greatest remote access cybersecurity challenge to your organization?

- Malware: 28.92%
- Misuse by staff: 26.51%
- Threats related to vendors, third-parties, freelancers: 21.69%
- Breaches by hackers: 12.05%
- Distributed Denial of Service (DDoS) attacks: 4.82%
- Phishing: 3.61%
- Smart card driver error causing RDS server crash: 2.86%
- C&C Bot activity: 1.2%
While most of the companies have their remote access secured in some way, it is rarely complete protection - while VPNs and multi-factor authentication are a good starting point, they both lack network monitoring and do not prevent human mistakes or access abuse. Both deliberate and accidental misuses by staff or remote subcontractors have been identified as the biggest cybersecurity threat. However, less than 37% of survey participants claimed they are actively using session monitoring & recording, which seems to be the key to secure remote access and implement a zero-trust environment.

Nearly one in every five companies surveyed has experienced a remote attack or disruption during the pandemic. 30% of respondents have invested in new security tools within the last six months, and the same percentage plans to reevaluate their SRA tools soon. This indicates the increased demand for remote access protection, not just for privileged users but also for regular staff and external contractors.

Almost half of the respondents claimed that despite having MFA, encryption, single sign-on, and user access gateways among their SRA tools, nearly half of all threats were either misuse by staff or 3rd party contractors. Only session management and recording can fully protect companies from these types of risks. That’s why nearly 60% of cybersecurity managers either have invested in such solutions already or plan to do so in the nearest future.

SUMMARY/ANALYSIS.
A survey regarding company-wide cybersecurity practices was administered to 83 individuals. Questions asked were related to current secure remote access (SRA) behaviors before and during the COVID-19 crisis. Collected data included responses from individuals located around the world, including the US, Europe, Canada, Africa, Asia, Central America, as well as the Middle East. The median company size of each respondent was 300 individuals, with 25% of respondents being part of companies with fewer than 81 individuals and 25% of respondents being part of companies with more than 1528 individuals. Respondents were all either C-level employees (44.6%), senior management (26.5%), management (16.9%), or an industry expert/specialist (12.0%).
ABOUT FUDO SECURITY

Based in Silicon Valley, Fudo Security is a leading innovator in the cybersecurity world. Deployed in more than 30 countries and trusted by hundreds of organizations, Fudo’s mission is to protect both large and small organizations against privileged user threats. Its solutions include Secure Remote Access, Privileged Access Management and Zero Trust Network Access. Fudo Security’s products allow monitoring the activity of users with access to critical assets. Additionally, Fudo’s solutions help manage password policies and alert immediately in case of any suspicious behavior.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NONINFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL FUDO SECURITY BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR FUDO SECURITY SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR RELIANCE ON THIS PUBLICATION, EVEN IF FUDO SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
FOR MORE INFORMATION VISIT fudosecurity.com

PHONE: +1 (408) 320 0980
sales@fudosecurity.com