

WORK-FROM-HOME ADOPTION IS INCREASING SECURITY RISKS, FINDS CATO NETWORKS SURVEY

Most companies fail to authenticate remote workers properly or inadequately inspect their network traffic for threats.

TEL AVIV, ISRAEL, May 14, 2020 /EINPresswire.com/ -- [Cato Networks](#), provider of the [world's first SASE platform](#), released today the latest survey results examining COVID-19's impact on enterprise readiness for work-from-home users. The "Enterprise Readiness to Support Widespread Work-from-Anywhere" survey found that most respondents (68%) indicate their organizations fail to deploy enough prevention or authentication technologies with remote users.

"A lack of security enforcement on remote access users should be of serious concern for IT managers. Enterprises cannot enable widespread remote access at the expense of security protections," says Yishay Yovel, CMO of Cato Networks. "This is why cloud-scale secure remote access, delivered as part of a SASE platform, is so important. Enterprises should be able to provide remote access for all users anywhere, in minutes, with the security protections and network optimizations they have in the office."

“

A lack of security enforcement on remote access users should be of serious concern for IT managers. Enterprises cannot enable widespread remote access at the expense of security protections."

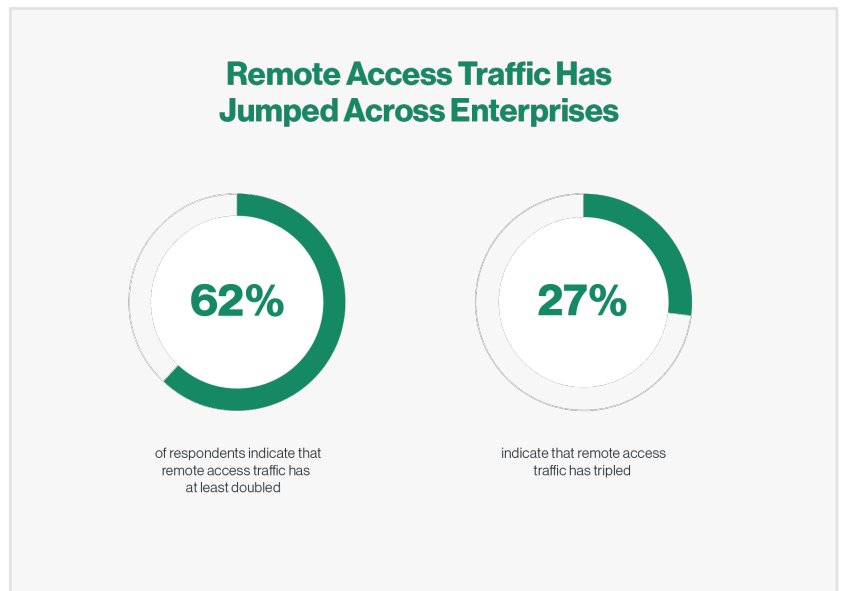
Yishay Yovel, CMO of Cato Networks

REMOTE ACCESS SURGES AS ENTERPRISES EMBRACE WORK-FROM-HOME

The survey assessed the impact COVID-19 is having on enterprise remote access. The survey was conducted in the first two weeks of April and answered by 694 respondents.

Since the outbreak, more than half of respondents (62%) have seen remote access traffic at least double, and more than a quarter (27%) have seen remote access traffic triple. The preferred remote access point-solutions continues to be VPN servers. More than half (64%) of respondents indicated they deployed VPN servers, followed by NGFWs (44%), and UTMs (17%).

But exactly how they're going to scale remote access to accommodate the triple-digit growth is still an open question. Nearly a third of respondents (31%) indicated they were going to incur the additional capital expense of adding VPN servers or upgrading to a large VPN server. A minority,



14%, indicated they planned on switching to a VPN cloud service. More than half of respondents (55%) indicated that they hadn't decided how to scale their remote access solutions.

SECURITY REMAINS THE WEAK LINK OF REMOTE ACCESS

Of critical concern is how enterprises enforce security policies on their expanded remote workforces. The survey found that most respondents fail to employ at least one key measure needed for enterprise-grade security:

- Multi-factor authentication (MFA) for validating user identity,
- Intrusion Prevention for identifying network-based attacks, or
- Antimalware for preventing threats posed by malicious content

While MFA has become standard even among consumers, more than a third (37%) of respondents don't use MFA when admitting remote users, relying on Single Sign On (SSO) or username and password. As for preventing attacks, more than half of respondents (55%) fail to employ Intrusion Prevention or antimalware. Even worse, 11% fail to inspect traffic altogether.

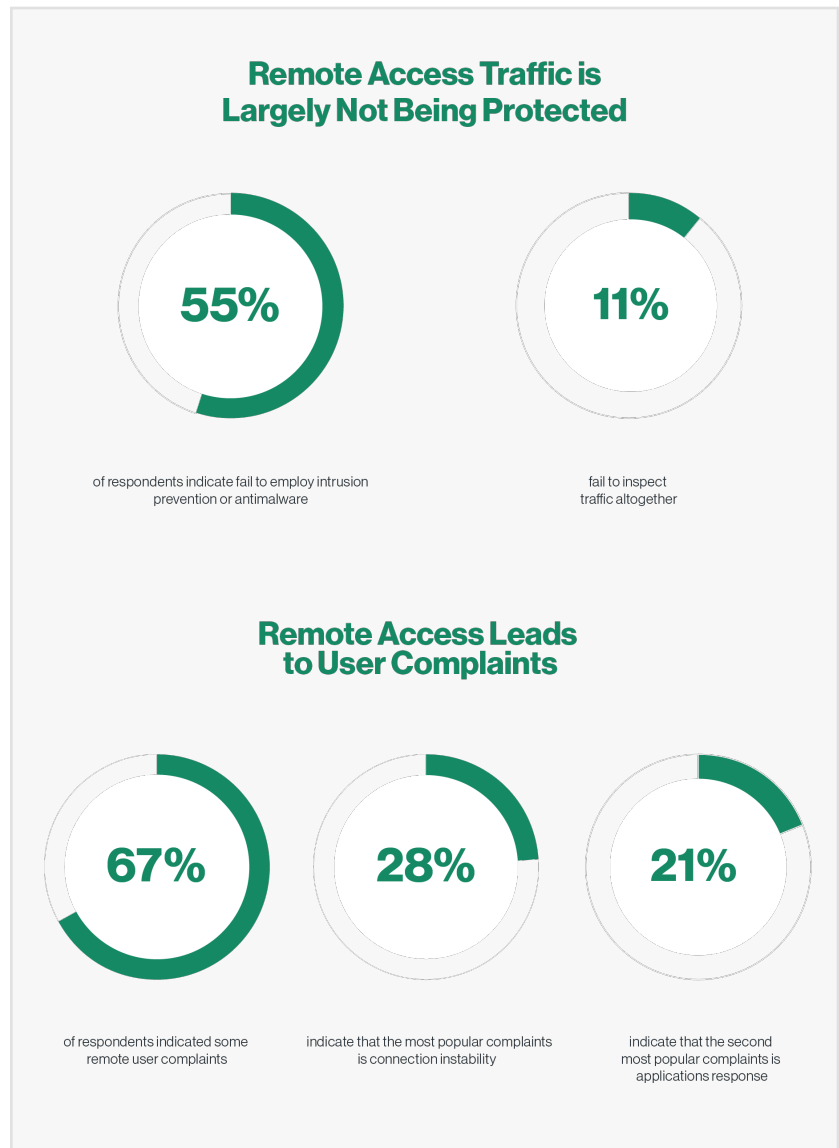
To compound matters, should attackers bypass authentication measures, they'll have access to the entire network. Overall, more than half (57%) of respondents indicated that they managed remote user permissions at the network level and not specific applications. For those who did not employ MFA, the number was even higher (63%). The risk of remote penetration is very, very high.

REMOTE ACCESS CONTINUES TO INSPIRE USER COMPLAINTS

Most respondents (67%) indicated some remote user complaints. Most of those complaints (60%) relate to the performance or stability of the network. More than a quarter (28%) indicated that remote users complained of connection instability, 21% complained about slow application response, 14% experienced poor voice/video quality, and 5% indicated that remote access was difficult to use.

To learn more about the survey and how Cato addresses the challenges posed by widespread, global remote access, [read our blog](#).

Dave Greenfield
Cato Networks
press@catonetworks.com
[email us here](#)



This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2020 IPD Group, Inc. All Right Reserved.