

Menlo Security Research Shows 75% of Organisations Re-evaluating Security Strategy as Remote and Hybrid Working Set to Remain

Submitted by: Origin Comms Ltd

Thursday, 14 October 2021

- Three-quarters rely on traditional VPNs for remote access while a third also use zero trust as part of their remote access strategy
- Over half plan to reduce third party/contractor access to systems due to security risks

Bracknell, UK - A report launched today by Menlo Security (<https://www.menlosecurity.com>), a leader in cloud security, highlights growing concerns about securing users as the trend for hybrid and remote working is set to remain. The new report – which surveyed 500+ IT decision makers in the U.S. and the U.K., including a third at C-level – looks at attitudes to securing remote access to applications and resources and the adoption of zero trust solutions.

While most respondents (83%) say they are confident in their strategy for controlling access to applications for remote users, three-quarters are re-evaluating theirs in the wake of new ways of working and the growth in cloud application use. While half of employees are currently working remotely or adopting a hybrid approach, around two-fifths (42%) are expected to continue in 12 months' time.

According to the findings, three-quarters (75%) of organisations continue to rely on VPNs (virtual private network) for controlling remote access to applications, which rises to 81% for organisations of 10,000+ employees. For around a third (36%) of organisations a zero trust approach also forms part of their remote access strategy.

“It seems that most businesses are confident in their remote access security, yet are still relying on a traditional and inherently insecure way of doing things using VPNs, which give access to everything on a network,” said Mark Guntrip, senior director, cybersecurity strategy at Menlo Security. “With only a third currently using zero trust network access, there’s a real opportunity to provide users with access to only those applications and resources needed to do their job. When you start to adopt this approach across everything you do then your whole security mindset changes.”

The top reason for implementing a zero trust solution is improved security, according to 60% of respondents, regardless of whether they are using it or not. One third (32%) point to ease of use, while speed of access and scalability are both more widely recognised among those already adopting a zero trust approach. Significantly, 40% of respondents believe that implementing a zero trust solution places less pressure on IT.

Despite overall confidence by global IT decision makers in the robustness of their strategy for controlling application access for remote users, Menlo Security’s research also shows that:

- Three-quarters of respondents believe that hybrid and remote workers accessing applications on unmanaged devices poses a significant threat to their organisation’s security. Despite this, around a fifth still allow unmanaged devices – laptops, desktops and mobile devices – to connect to corporate applications and resources.

- While the majority (79%) of respondents have a security strategy in place for remote access by third parties and contractors, there are growing concerns about the risks they present, with just over half (53%) planning to reduce or limit third-party/contractor access to systems and resources over the next 12–18 months.

Menlo's Mark Guntrip adds: "As the internet becomes the new corporate network, controlling user access to private applications has become more important than ever. Organisations need to evolve their thinking from providing connectivity to the entire network to segmenting access by each individual application. The right zero trust approach will ensure seamless access between users and the applications they are authorised to use, while all other applications are invisible, preventing lateral discovery across the network."

An infographic to accompany the report can be found here (<https://resources.menlosecurity.com/infographics/securing-the-new-workplace-reality>)

Menlo Private Access

Menlo Security has a clientless-first approach to implementing Zero Trust Network Access, enabling organisations to secure access to applications from all devices – including managed, unmanaged and mobile devices. This approach minimises the workload on IT and security for deployment, while maximising the security posture of the company. The clientless-first approach can be augmented with a client for use cases that specifically require client-based access.

Unlike many ZTNA solutions that cannot monitor traffic being sent and received between an end user and a controlled application, Menlo Private Access ensures that security policy is always enforced by remaining inline between the end user and protected applications; utilising our Elastic Isolation Core as a control point to prevent sensitive data loss and stop potential malware from reaching the endpoint.

Ends

Survey Methodology

The survey was conducted among 545 IT decision makers from organisations with 1,000 or more employees across the U.S. (265) and U.K. (280). One third of respondents (31%) were C-level and the top three industry sectors were Manufacturing (15 percent), Banking & Finance (14%) and Healthcare (14%). Sapio Research conducted interviews online during August and September 2021 using an email invitation and an online survey.

About Menlo Security

Menlo Security protects organisations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered cloud security platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and eight of the ten largest global financial services institutions, and is backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit www.menlosecurity.com.

Media Contact
Louise Burke
Origin Communications
menlo@origincomms.com
020 3814 2940