RISKS OF THE BROWSER-DRIVEN WORKSPACE

The way we work has fundamentally changed. Organizations worldwide have pivoted to hybrid work, significantly increasing reliance on unmanaged personal devices. Mix this with an increasing reliance on inherently vulnerable web browsers and complex cloud adoption, and there's a new landscape of risk. With security teams grappling for visibility and control, Palo Alto Networks commissioned research to delve into the nuances of today's challenging environments.

The Modern Workforce

50%

Increase in web/SaaS app use over the next 24 months.

An expanding, complex workspace requires a critical rethinking of cybersecurity measures, securing sensitive data in the browser.

85%+

Portion of workday taking place in a web browser, with 11% personal browsing.

A web browser with robust security safeguards this new work environment. This includes proactively enhancing visibility into browser activity.

~90%

Organizations that had employees and contractors access corporate apps from personal devices.

The prevalent use of personal devices is a serious challenge for security teams. They must strengthen security policies and tools to secure data on these unprotected endpoints.

Risks of the Modern Workforce

95%

Percentage of respondents who reported browser-based attacks in the last 12 months. This included account takeovers, malicious extensions, etc.

This glaring security gap requires organizations to fortify their web browser and enforce stringent device management.

53%

Organizations that weren't confident in their ability to address security issues in unmanaged/poorly managed devices. Only 6% were very confident.

Organizations concerned with device threats need to embrace advanced visibility and control mechanisms.

~33%

Respondents with higher financial cost/business impact caused by threats on unmanaged/poorly managed devices, compared to all other security incidents.

An upgrade in tactics is required for device security and management to address these risks.

94%

Organizations that experienced a phishing attack over the last 12 months.

CONCLUSION

Prisma Access Browser extends the robust protection of SASE to the browser and personal devices. It offers security features such as browser-based DLP, Zero Trust, SaaS visibility, and AI-powered threat protection in real time. It's essential to dramatically reduce risks from cloud migration and hybrid work. Explore how it ensures your organization thrives in the new era of work.

Survey Methodology

Technology consultancy firm Omdia fielded a custom research study. Surveys were fielded in a double-blind methodology to ensure respondents did not know they were partaking in Omdia/Palo Alto Networks research. The survey included a total of N=514 respondents in senior IT, cybersecurity, workplace provisioning, incident response, and network security roles at enterprises of over 2,500 employees in a variety of industries across the United States, Canada, and Europe.

3000 Tannery Way, Santa Clara, CA 95054
Support: +1.866.898.9087
www.paloaltonetworks.com