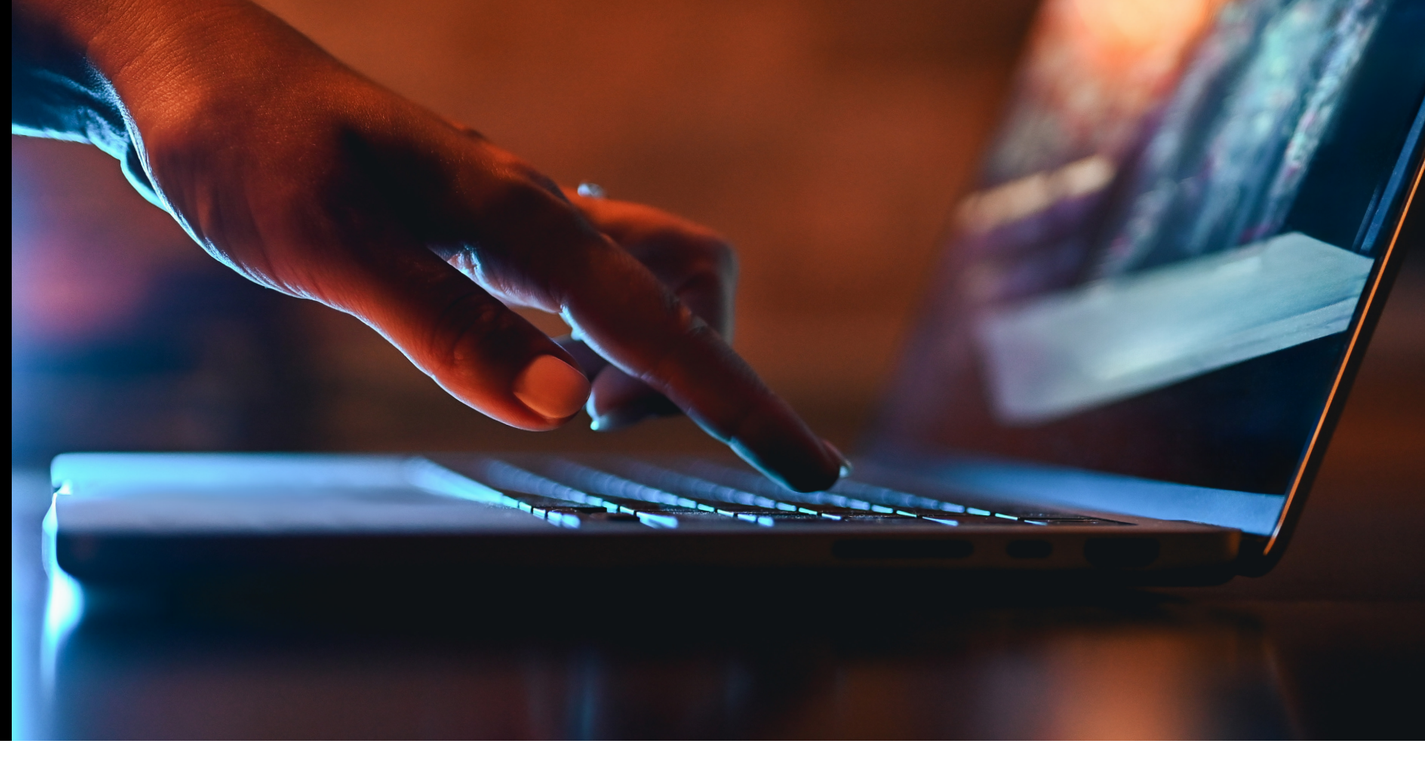
Industry Pulse

Enterprise Browsers: AI-Ready Security for a Modern Workforce

Powered by DIVEMARKETPLACE



Key Discussions

01

The End of Data Leaks: Modern Data Security Begins in the Browser

Palo Alto Networks

02

Enterprise Browsers: The New Standard for Security?

IT Pro

03

The Browser Blind Spot: Hidden Security Risks behind Employee Web Activity

Digital Journal

04

Protect Your Network with an AI-Secure Browser and SASE Framework

TechRadar

Content brought to you by paloalto NETWORKS

Enterprise Browsers: AI-Ready Security for a Modern Workforce

Web browsers: they're a seemingly unassuming part of the technology stack that most average employees don't think about twice in their daily usage. To them, browsers are the workplace through which information is accessed, shared, and tasks are executed – they don't see them for the potential attack vector that they could be if not secured correctly.

With the number and sophistication of web-based threats only set to keep growing in the coming years, legacy security methods that rely on traditional VPNs, SWGs or VDI won't suffice to maintain security across mission-critical data for workforces, especially as AI adoption accelerates.

As a result, analyst firms like Gartner are predicting upwards of 1 in 4 organizations will adopt an enterprise browser, also known as a secure browser, as an alternative in the next couple of years.

In this trends report, you'll learn what security features enterprise browsers offer when compared to the traditional free or open-source browsers like Chrome that currently dominate the workplace. Find out how an enterprise browser can help control data access, prevent data loss, complement a Zero Trust SASE architecture, and contribute to a secure foundation for AI adoption.

01

The End of Data Leaks: Modern Data Security Begins in the Browser

Shlomi Zrahia, Andrew Huang, Carmine Clementelli
| Palo Alto Networks

Today's workforce is more distributed than ever. Hybrid workers, remote workers and contractors are using sensitive data in SaaS, web, email and GenAI applications, blurring the lines on where work is happening.

This flexibility enables employees and contractors to work productively. But it also introduces significant risk of both intentional and unintentional data loss, creating a complex and challenging landscape for data security.

Prisma® Browser helps organizations secure data in the modern workspace across all applications and traffic with Enterprise Data Loss Prevention, granular user controls and visibility into user activities on any device.

The Current Landscape

Traditional data security tools are often reliant on inline traffic decryption, agents and APIs.

This reliance means they can't:

- **Secure data across all applications and traffic.** 64% of web traffic remains encrypted. Although some solutions can decrypt traffic for inspection, many traffic remains encrypted due to privacy concerns and technically undecryptable protocols like QUIC, ECH and WebSocket. Because of this, most traffic remains unprotected, creating security blind spots where threats may hide and user activity remains unaccounted.
- **See how data is being used**. Most tools lack visibility and control over sensitive data use within applications, such as uploads, downloads, copying, pasting, clipping things to the clipboard, posting, printing, sharing and others. Without this context, how would organizations accurately assess risks to data and determine the best course of action?
- **Implement granular zero trust controls**. No visibility into how data is used makes it difficult to prevent data risks without hindering productivity. Traditional tools cannot provide effective context-aware controls, resulting in insufficient prevention of risky activities, inappropriate access to information and greater risk of false positives that create end-user frustration.
- **Accurately identify sensitive data.** Organizations that rely solely on traditional data security tools are plagued with false positives that hinder user productivity. On average, 80% of data is unstructured in 2025, making it difficult for organizations leveraging traditional data security tools to accurately identify sensitive data.
- **Quickly deploy without complexity.** Setting up comprehensive data security with traditional tools is often a complex, manual process that requires extensive time and resources.

On average, 80% of data is unstructured in 2025, making it difficult for organizations leveraging traditional data security tools to accurately identify sensitive data.

Modern Data Security Challenges Require a Shift in Focus

It's a challenge for data security tools to keep up with new types of data. Organizations are incrementally extending protection across sprawling cloud environments where data lives and flows — from new SaaS apps to GenAI tools, AI agents and copilots. Organizations should prioritize securing data where it is actually being used and where all apps and web activity converge. In today's modern work environment, this is the browser.

Browsers are the modern workspace, where 85% of a worker's day is spent. Browsers are also vulnerable, with 95% of organizations reporting a security incident originating from the browser. With data being used primarily in the browser, organizations face heightened data security risks.

While browser-based protection doesn't address every challenge, getting it right solves the most difficult and impactful problems. Organizations can start with browser-based data protection and extend this protection to a security service edge (SSE)-native data security model.

This approach will allow data protection to span networks, email services, cloud platforms, SaaS applications and on-premises repositories—including private apps—via a unified solution that provides a single policy framework, unified incident response and a single console for management and visibility.

Browsers are the modern workspace, where 85% of a worker's day is spent. Browsers are also vulnerable, with 95% of organizations reporting a security incident originating from the browser. With data being used primarily in the browser, organizations face heightened data security risks.

See and Protect Anything: Secure Data Across All Applications and Devices

Palo Alto Networks Prisma Browser solves data security risks in the modern workspace, bringing built-in enterprise DLP capabilities right to where data is used to secure the workspace and protect data on any device for any user.

Prisma Browser solves the challenges of traditional data security tools by:

- **Eliminating blind spots from encrypted traffic.** The secure browser shifts data inspection from the network directly to the browser itself, providing complete visibility into all web, SaaS, GenAI and private application traffic before encryption. This enables comprehensive data security, compliance and policy enforcement. The built-in Enterprise DLP engine can enforce data security policy without violating user privacy or facing undecryptable protocols.
- **Gaining visibility into user activity.** Gain unmatched visibility into user activity with sensitive data on any device. Prisma Browser provides a unified management console with a dedicated AI security dashboard and executive reports. Capture data snippets, crucial evidence of policy violations, and most important, full session recordings for threat hunting and compliance purposes across SASE, next-generation firewalls (NGFWs) and software firewalls in addition to the browser.
- **Enforcing granular control over user actions with sensitive data.** Implement Zero Trust access and granular controls over user actions with continuous evaluation of context based on user identity, device posture, location and the application being used. Enable risk-based controls—like applying just-in-time (JIT) coaching or inline MFA —to prevent data risks without frustrating users or hindering productivity.
- **Identifying sensitive data with high accuracy.** Prisma Browser leverages built-in Enterprise DLP, which utilizes AI and LLMs for advanced accurate data classification with over 1,000 data classifiers. This technology goes beyond pattern recognition, comprehending content and context to accurately identify intellectual property, confidential business information and personally identifiable information.
- **Quickly deploying corporate data policies organization-wide on any device.** Prisma Browser can be downloaded and set up in only minutes, enabling organizations to deploy consistent organization-wide data security policies immediately with little complexity. Secure data from exfiltration on any device, managed and unmanaged.

Implement Zero Trust access and granular controls over user actions with continuous evaluation of context based on user identity, device posture, location and the application being used.

Prisma Browser is not just preventing data leaks; it's modernizing data security. It's creating a proactive, intelligent and user-centric approach that ensures sensitive data is protected at its most vulnerable.

Secure Data In the Browser-Based Workspace and Browse Bravely with Prisma Browser

Prisma Browser is not just preventing data leaks; it's modernizing data security. It's creating a proactive, intelligent and user-centric approach that ensures sensitive data is protected at its most vulnerable point—in the browser.

Schedule a demo today to see how Prisma Browser extends Enterprise DLP into the browser to stop data loss, protect sensitive information, and enable safe generative AI use so that your organization can Browse Bravely.

02

Enterprise Browsers: The New Standard for Security?

Stephen Pritchard | IT Pro

The web browser is a vital, but largely commoditized, part of IT infrastructure. But that could be about to change with the growth of enterprise browsers.

For the last two decades or more, businesses seem to have been happy enough with the default browser bundled with their operating system, or with Google Chrome.

Almost all browsers cost nothing to use. Netscape made its Navigator browser free (and open source) as far back as 1998. That, in turn, was in response to Microsoft bundling Internet Explorer with Windows.

And Chrome, with by far the largest current market share of any browser, is a free download.

Research by YouGov round that *58% of internet users in the United States use Chrome*, with its nearest competitor, Apple's Safari, on 15%. Statcounter, a tool that allows website users to monitor visitor statistics, puts Chrome's UK market share a little lower, at *51.8% and Safari at 30.5%*, across all device platforms.

Interest in other browsers remains low. Firefox, for example, registered just 1.9% of users in August this year, and Edge 8.6%, again according to Statcounter.

The majority of browsers in use today are, in any case, based on the open source Chromium technology. This includes Google's Chrome, but also Microsoft Edge, and Opera; Apple's Safari is the most widely-used exception.

These stats include both consumer and business usage – but the use of consumer-grade browsers within the enterprise is common. Increasingly, however, software vendors have launched new browsers aimed specifically at enterprise users, with added capabilities such as enhanced data security and access controls.

Gartner predicts that by 2028, 25% of organizations will deploy at least one enterprise browser in the pursuit of better security. Are enterprise browsers on the cusp of widespread adoption – and what are their chief benefits?

Gartner predicts that by 2028, 25% of organizations will deploy at least one enterprise browser in the pursuit of better security.

Enterprise browsers on the rise

The reasons for enterprise browsers are twofold.

First, the way businesses deploy and use enterprise applications has changed. Applications increasingly run in web browsers, so the browser is the front end for most day to day activities.

And organizations are increasingly concerned about security, privacy and data protection, not least because of the proliferation of generative AI tools.

The enterprise browser, its advocates argue, offers much more granular control over how users access data – enterprise browsers tie directly into data loss prevention and security tools. Unsurprisingly, some of the companies now offering enterprise browsers are, first and foremost, security vendors.

"Fundamentally, enterprise browsers offer deeper levels of security protection than the consumer grade ones used for casual web browsing," Will Townsend, VP principal analyst at Moor Insights and Strategy tells *ITPro*. "This is an important consideration given the fact that generative AI applications use a browser as the interface."

Townsend comments on the number of enterprise browsers on show at Black Hat USA earlier this year, and labels 2025 as "The Year Of The Enterprise Browser". He flags Island, Google, with its enterprise versions of Chrome, Mammoth Cyber and Palo Alto Networks' Prisma browser as technologies to watch.

What makes enterprise browsers stand out for Townsend is their control over data access and data leakage. "Many are architected with zero trust least privileged access constructs and deeper security provisions including identity access management and improved data observability," he says.

But enterprises are not just using enterprise browsers to improve security. These applications are also being used as a cheaper, easier to manage alternative to *virtual desktop infrastructure (VDI)*, especially where *chief information officers (CIOs)* need to manage third parties, such as contractors, on their networks. Island especially promises "virtualization-like functionality", Townsend says.

The enterprise browser, its advocates argue, offers much more granular control over how users access data – enterprise browsers tie directly into data loss prevention and security tools.

No more VDI

This use case allows IT teams to manage just the browser, without all the other overheads of full-blown VDI, or the cost and inconvenience of issuing a physical, corporate device.

“In extreme examples, contractors would be shipped physical laptops that have the golden build on them,” Scott McKinnon, chief security officer for UK and Ireland at Palo Alto Networks, tells *ITPro*.

“That’s obviously very, very expensive for the organization.

“Now, if you can effectively introduce a new level of abstraction and treat everybody the same from a platform perspective, you don’t care whether they’ve got an HP or a Dell, or whether they use a Mac, or a tablet or a phone, or whether they are a contractor or an affiliate or a customer,” he says.

“You can have that kind of consistency, and treat everybody the same from that operational perspective, which streamlines things, reduces cost and helps business on the bottom line.”

At Palo Alto Networks, all company business is now done within its Prisma enterprise browser, though McKinnon adds he still uses Chrome for non-corporate tasks such as Gmail or LinkedIn.

At Palo Alto Networks, all company business is now done within its secure browser - Prisma Browser.

Browsers, and plug ins

Palo Alto offers its Prisma enterprise browser as a standalone product, controlled via a cloud portal. This allows IT and security teams to use isolated profiles and policies for Prisma.

But the real benefit, McKinnon suggests, comes when enterprises steer all their web traffic from the browser to Palo Alto Networks' secure access service edge (SASE) platform. This provides data loss prevention and data plane isolation in a way that is simply not practical with third-party browsers.

But standalone enterprise browsers face competition from enterprise versions of regular browsers, and from extensions that add security features to control how browsers handle data.

"From the enterprise browser standpoint, here, we've two elements," explains Oliver Madden, an enterprise browser specialist at Google.

"One is a core element which allows you to manage some policies, configurations, and generate reports. And then we've the premium piece that allows you to set zero trust, access controls and threat intelligence directly into the browser."

The advantage here is that users can continue with the browser they know, but IT teams can add additional controls. For example Paul Stringfellow, CTO at IT consultants Gardner Systems, tells *ITPro* that security teams looking to sandbox malware or malicious websites are turning to enterprise browsers.

"What I am seeing increasingly from cybersecurity vendors is the deployment of browser agents, which allow them to enforce granular controls on users accessing the internet. This ensures that users always have consistent controls applied to their devices."

Whether enterprise browsers become mainstream will depend largely on whether those security and data access controls are enough to overcome the existing browsers' vast installed base.

03

The Browser Blind Spot: Hidden Security Risks behind Employee Web Activity

Dr. Tim Sandle | Digital Journal

Web-based threats are a key cybersecurity concern, and recent headlines on malicious browser extensions have highlighted that the browser has become an attack vector.

However, according to Andrius Buinovskis, a cybersecurity expert at NordLayer, these are not the only threat security teams need to watch out for, since dangerous employee activity can result in data leaks, GDPR violations, and industry secret disclosure.

According to Buinovskis, organizations are embracing the shift to a web-based environment. However, with limited observability and control over what employees are doing, the browser has created a security blind spot, often allowing dangerous activity undetected.

Enterprise reliance on browsers is growing, and so are the associated risks stemming from dangerous employee web behavior. Research has found that 80 percent of employees can complete 80 percent of their work tasks using the browser. While the shift to the browser can increase productivity and collaboration by speeding up processes, this is also accompanied by risks.

"Companies are embracing web-based software as a service (SaaS) applications for various benefits, such as cost reduction and increased efficiency. However, due to increasing dependency, the browser is becoming a significant cybersecurity concern," says Buinovskis in a statement provided to Digital Journal.

He continues: "Aside from attracting the attention of cybercriminals, it's also become a hub for insider threats or employee error, which can result in devastating security breaches. The most concerning element is the lack of observability security teams might have into employee activity in the browser, creating an alarming blind spot."

Traditional browsers are not built with security and observability in mind — their primary target is to provide a user-friendly interface.

Can security teams see what employees are doing in the browser?

According to Buinovskis, if employees use a traditional browser, security teams' observability of what people do in the browser is existent yet limited. Solutions like ADR (automated detection and response) and XDR (extended detection and response) can incorporate TLS (transport layer security) inspection and provide extensive activity monitoring and securing capabilities. However, they require significant financial and human resources to implement and maintain. The hefty price tag might ward off small to medium-sized businesses from the investment, exposing them to browser-based threats.

"Traditional browsers are not built with security and observability in mind — their primary target is to provide a user-friendly interface. These capabilities are more or less sufficient for personal use but are inadequate to safeguard a business," Buinovskis explains. "Even if a company has an extensive cybersecurity strategy and a large team of security experts at their disposal, the lack of built-in security and monitoring features in a traditional browser still leaves them vulnerable and more likely to experience a safety incident."

The most dangerous threats to look out for

According to Buinovskis, the most dangerous threats that can result from employee activity in the browser include:

- **Data exfiltration.** Ill-intended employees can use the browser's limited observability to steal confidential company information, such as industry secrets or client data stored on web-based apps, and share it through email or social media without being detected.
- **Install unauthorized browser extensions.** Some of these extensions are malicious and prey on unsuspecting users to collect sensitive data, modify browser behavior, and create security vulnerabilities. If a company uses a traditional browser, it's challenging to monitor and control which extensions employees can download and minimize the risk of them installing malicious add-ons.
- **Engage with unauthorized browser-based applications (shadow IT).** Not all web-based SaaS applications are safe to use — some might have significant security vulnerabilities, resulting in data leaks or compliance violations. Without proper monitoring, these applications can go undetected, expanding the scope of unmanaged apps (shadow IT).
- **Other insider threats.** The traditional browser's lack of observability and behavioral analytics makes it easier for malicious employees to fly under the radar and access sensitive data or converse with third parties. Depending on the scope, these actions can have dire consequences, such as industry secrets ending up in the hands of the competition.

"To safeguard against browser-based threats, companies need to invest in building and maintaining a comprehensive cybersecurity strategy that would provide a higher level of observability into employees' activity on the browser or opt for browsers with built-in monitoring and security features," Buinovskis recommends.

Buinovskis highlights that cybersecurity awareness training for employees is also a worthwhile investment. It helps to minimize the possibility of user error, such as interacting with unauthorized apps or downloading malicious browser extensions.

He further advises: "However, it's worth noting that even with comprehensive cybersecurity measures, monitoring browser usage across an organization remains challenging if it lacks built-in security features. This gap allows certain user activity to go undetected."

04

Protect Your Network with an AI-Secure Browser and SASE Framework

Matt Dykes | TechRadar

Cybercrime has accelerated and IT departments are struggling to protect their networks. Cobalt stated that global cybercrime was forecasted to cost $9.5 trillion this year and will continue to escalate.

Coupled with the rising costs of global ransomware that has surged by 400% to $2 million over the past year with recovery costs increasing by approximately 50% to $2.73 million (National Crime Agency) these statistics are shocking. The threats to companies' networks and disrupting business, leaking data and the costs faced are colossal. The more sophisticated AI gets the more this will happen.

Now is the time for businesses to invest in next generation cybersecurity methods to protect and enhance their network and implement an AI-Secure Browser and SASE framework.

AI the superhero

Artificial Intelligence (AI) has superpowers to analyze masses of data in seconds surpassing human capabilities. AI-secure browsers can constantly monitor and identify threats in real time such as malware, phishing attempts, and unauthorized access. Through machine learning algorithms, they can identify threats or different behavior on the network at a far greater speed than traditional methods. Responding to new and evolving threats before they cause damage. All without the need of the IT team stepping in.

Unrivalled security

The combination of the SASE network and AI-secure browser offers unrivalled levels of network security. The SASE network provides firewall, secure web gateway (SWG), and zero trust into a single, cloud-delivered service. While an AI-secure browser ensures consistent policy enforcement and increases levels of security, making the network more robust irrespective of where users are based.

Remote and hybrid workforce

A secure network is critical as our workforce has become more disparate over the last few years with 28% of people hybrid working and 13% working from home (The Times) and accessing the corporate network. Some may access the corporate network or systems from personal devices which can threaten the integrity and safety of the corporate network. This is because the personal devices do not have the same security protocols. Employees may also visit unsecure public Wi-Fi networks where hackers can intercept data. Also, data leaks can occur leaking personal or corporate data.

An AI-secure browser in a SASE network enhances the security of remote users without compromising on performance or user experience.

Providing zero trust access ensuring that only authenticated and authorized users can access resources. There is no need for traditional VPNs which can be slow and vulnerable to attacks.

The SASE architecture provides flexibility because it is cloud based, providing the ability to scale up and down when required. Supporting growing remote, hybrid or office-based workforces without compromising on security.

In the shadows

Shadow IT is where employees use unauthorized applications, software and devices without approval from the IT team. Threatening the security of the network as the IT team are unaware of 'shadow IT' activities and therefore cannot monitor or secure the network. Risks posed are that data maybe being stored or compromised. It also increases the access of entry points for cyber-attacks making it difficult for repair and recovery.

The AI-secure browser and SASE network can protect networks against shadow IT as it provides visibility of all traffic, user activity, websites and applications. These can then be monitored by the AI-secure browser in real time and if issues are identified they can be resolved and the IT team alerted.

Restrictions can be implemented so employees cannot bypass the corporate systems or access areas that are not sanctioned. SASE can restrict these areas very easily as it is cloud based, and the AI-secure browser can block access to unsafe websites or applications.

Zero trust model via SASE ensures that every device, user and application is continuously authenticated and authorized before access is granted. All these measures vastly reduce the threat of shadow IT by enforcing strict access controls and preventing unauthorized access.

Seamless user experience

One of the main benefits of combining an AI-secure browser with a SASE network is maintaining a seamless user experience while ensuring high levels of security. AI can optimize performance and improve user experience with minimal lag, even when accessing secure, encrypted connections.

The integration of security functions directly into the browser means that users can browse without slowdowns while still being protected from online threats. Also, SASE supports Single sign-on (SSO) so users can access all the applications they need with one set of credentials.

Zero Trust model via SASE ensures that every device, user and application is continuously authenticated and authorized before access is granted. All these measures vastly reduce the threat of shadow IT by enforcing strict access controls and preventing unauthorized access.

Utilize AI and SASE to remain one step ahead of cyber threats and to modernize and secure your network while maintaining flexibility and performance for today's disparate workforce.

Future-proof security

Implementing an AI-secure browser and SASE network is a game-changing strategy in securing your network against increasing cybercrime and threats. It provides businesses with a future proof network ready for 5G and IoT. Offering total security for your corporate network, an improved and seamless user experience, and simplified network management in a scalable and cost-effective manner. So, utilize AI and SASE to remain one step ahead of cyber threats and to modernize and secure your network while maintaining flexibility and performance for today's disparate workforce.

Want to learn how Prisma Browser can enable your team to browse bravely?
Speak with our team and experience the secure browser.

Or schedule a demo today to see Prisma Browser in action.

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.