

What if your business could be as secure **outside your firewall...**

...as it is within?

You've wisely invested in a Palo Alto Firewall, building a robust security foundation for your operations.

But that can't protect you from the modern, browser-based threats evolving fast beyond your network perimeter.



New era, new threat

Modern enterprises run on browsers, and that's actively reshaping where security threats and risk live. Recent research shows¹ that browsers are now **where a massive 85%** of all work happens:

- Cloud-based collaboration tools
- Digital services
- New AI-powered apps
- Third-party access
- Remote working
- BYOD

¹ Source: Palo Alto Networks - The State of Workforce Security.

95%

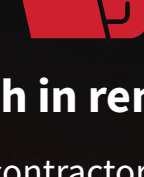
of organisations have experienced browser-based attacks outside their firewall.¹

Four reasons browser-based risk is evolving faster than your security strategy



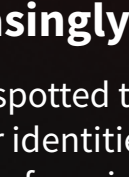
Web apps everywhere

From email and collaboration tools to HR and finance systems, we constantly move between web apps at work, often **choosing a convenient browser tab over installed software.**



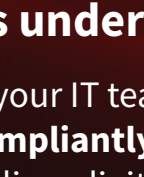
Rapid growth in remote working

With growing contractor numbers, more remote workers and **employees moving between personal and corporate devices**, our workforces have become more distributed.



Attackers increasingly target identities

Threat actors have spotted the security gaps and started targeting user identities, behaviour and web activity, rather than focusing on infrastructure.



IT teams under pressure

That all leaves your IT team **struggling to securely and compliantly support flexible working** and deliver digital services across locations, devices and cloud platforms.

Did you know?

The average organisation now runs **over 350 SaaS apps** operation wide?²

75% of knowledge workers use AI tools at work³.

Source: ² The 2024 State of SaaSops Report; ³ Microsoft - Work Trend Index

Browser risk is business risk

IT teams face spiraling security challenges:

Employees are using **multiple digital tools and AI services** to accelerate everyday tasks, often without the organisation's permission.

Partners and contractors need to securely collaborate on shared platforms with fast access to systems and data.

It's tough to monitor **how workers access sensitive cloud-based data.**

Sprawling security complexity and inconsistent policies deployed to try to manage it all **make life frustrating for IT and slow work down.**

The time for a new security approach is now

New browser-first workplaces are transforming how IT leaders think about security - **and CDW is leading the way.**

Our enterprise customers increasingly ask us how to secure their extended operations from **modern threats beyond the network perimeter.**

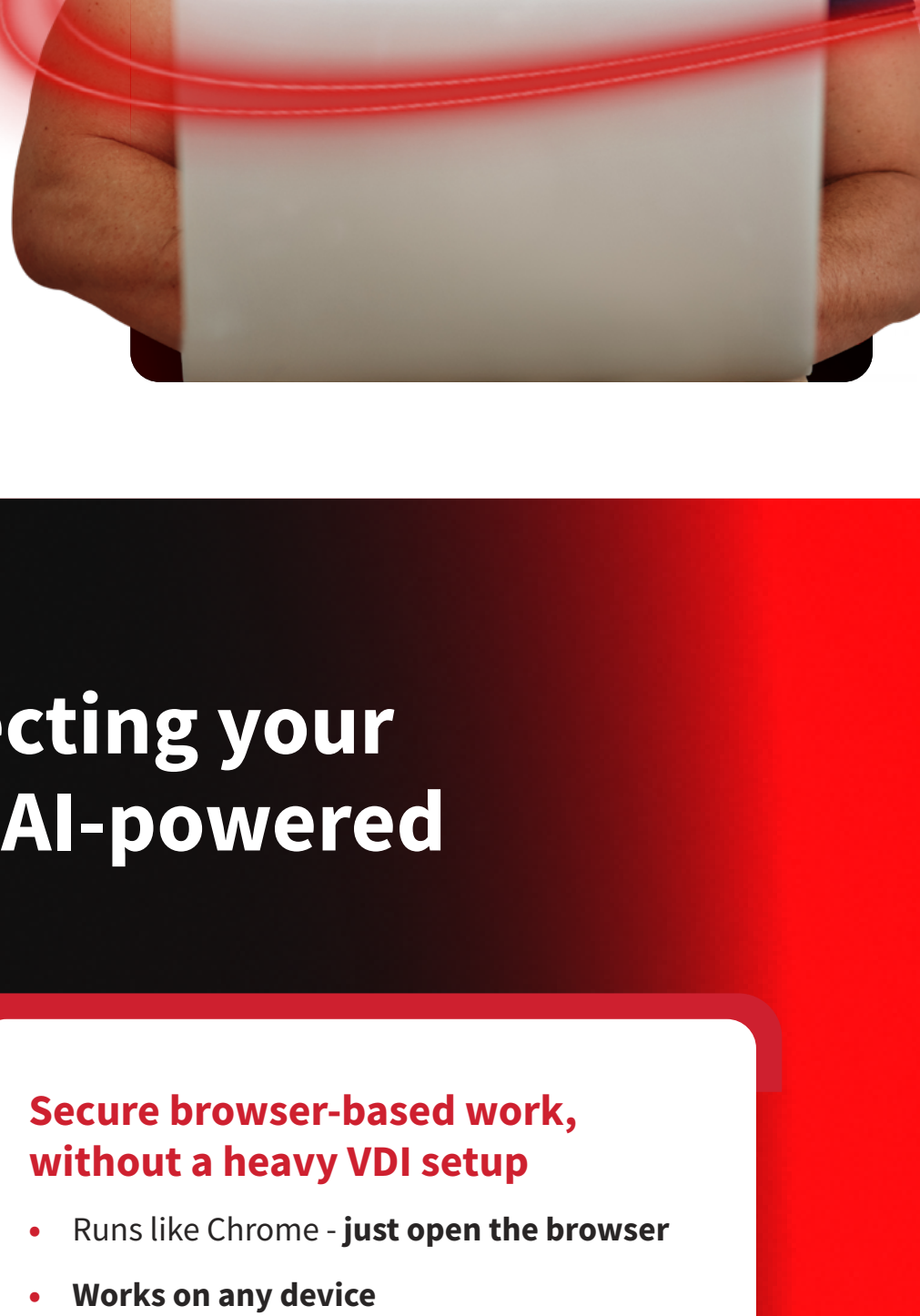
Our answer? A new security approach that's right for these times.

Built for resilience. Empowering governance. Unleashing productivity.

Simplifying complexity is the key

The goal isn't more security tools.

It's **safer and simpler** ways to work.



Two simple steps to protecting your network perimeter with AI-powered protection from CDW

1

Prevent browser-borne attacks

With Palo Alto Prisma® Browser (PB) AI-powered browser security.

Secure the place where 85% of work now happens.

- ✗ No VPN
- ✗ No VDI software install
- ✗ No hardware to ship or manage
- ✓ **Just** secure access controlled at the browser

Secure browser-based work, without a heavy VDI setup

- Runs like Chrome - **just open the browser**
- **Works on any device**
- Takes **minutes** to deploy
- Cloud-delivered - **no hardware, no patching**

Unleash responsible GenAI productivity

- **Block specific tools for some apps or users**
- **Block sensitive actions like copy/paste**
- Monitor use on personal devices
- Enforce **GenAI governance policies** - no endpoint agents

Empower contractors, partners and BYOD

- **Secure SaaS/ web app access** from personal devices
- Apply **access policies** based on user, app, or device
- **Block risky** downloads, copy/paste or screen capture
- Monitor and log browser activity for **compliance**
- **Automatically revoke access** when device posture changes
- **End permissions** as soon as the project is done

2

Extend security beyond the browser

With Palo Alto Cortex XDR: the world's most effective AI-powered endpoint security.

Get a unified picture of risk beyond the browser and extend protection across every device, network, user and the cloud with a solution proven in 5 years of exceptional MITRE ATT&CK evaluations.

STOP attacks at the endpoint

With AI-powered prevention protecting you against evolving adversary techniques and zero false positives.

SEE WITH 100% ACCURACY how attacks unfold

Across endpoints, networks and identity data proven by MITRE ATT&CK Evaluations using AI-driven detection & analytics.

CUT ALERTS BY 98% and identify root causes

Reducing alert fatigue for stretched IT teams and letting security analysts achieve a near real-time response using native ML-driven automation.

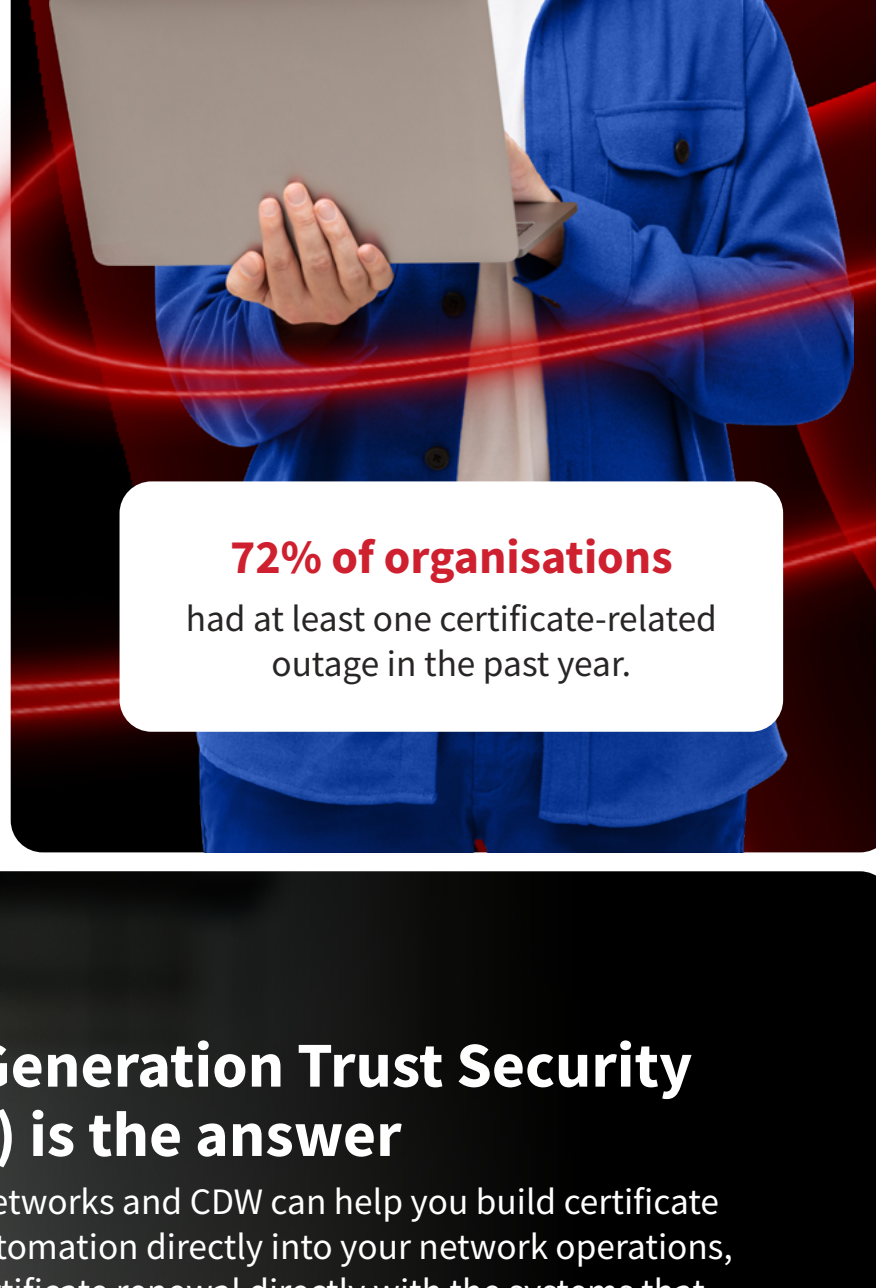
Protect against security outages on your firewall and VPN too

When a certificate expires on a firewall or VPN gateway, **the impact is immediate** - and you often won't realise it until the system breaks.

Shortening certificate lifespans are driving a projected **8-12x increase in renewal volumes by 2029.**

That means **more danger of missing deadlines** leading to:

- ✗ Remote access **fails**
- ✗ **Halted** security inspections
- ✗ Users **losing connectivity**



72% of organisations

had at least one certificate-related outage in the past year.

Next-Generation Trust Security (NGTS) is the answer

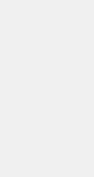
Palo Alto Networks and CDW can help you build certificate lifecycle automation directly into your network operations, aligning certificate renewal directly with the systems that enforce trust to keep critical services running:

- ✓ Renewals, deployment, and enforcement stay in sync
- ✓ Across firewalls, VPNs, and inspection services
- ✓ Preventing outages
- ✓ Maintaining operational stability

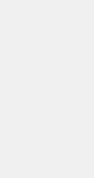
Secure the browser-first workplace beyond your firewall

Take the vital next step

with CDW and Palo Alto Networks.



You've already invested in a **robust Palo Alto Firewall**



Now protect yourself from threats beyond your network perimeter with **Palo Alto Prisma® Browser and Cortex XDR**



Add Next-Generation Trust Security to **keep your firewall & VPN performing**

The Palo Alto experts at CDW can help you seamlessly level-up your security maturity and **make security a competitive advantage with:**



Absolute visibility everywhere

See where browser-based work and AI interactions are happening and how applications, users and data interact across your digital environment.



End-to-end simplification

Integrate leading standards-based security technologies across user devices and applications, aligned with governance requirements and automatically synced for always-on certification.



Friction free access

Design policies and security architectures that balance protection with productivity protecting access to sensitive information without adding user friction.

Make your business as secure outside your firewall as it is within

Set up a meeting with CDW now