XMA

chrome enterprise

The Browser is Now the Security Perimeter

(Whether You Planned It or Not)

Why modern productivity depends on a unified control plane for SaaS, GenAI, and legacy applications.

A strategic guide for UK CIOs, CISOs, and IT Directors.

The Modern Productivity Paradox

The Problem: We have updated where people work, but not how we protect that work.

85% of the workday is now browser-based*, yet security still sits at the network edge.

Users already choose Chrome for its speed, but IT lacks visibility into the actions taken inside those tabs.

The "Legacy Anchor":

Most UK organisations are stuck. You want to adopt a browser-first strategy, but one or two "heritage" Windows applications force you to maintain costly VPNs and resource-heavy VDI. This creates a fragmented environment that is expensive to manage and difficult to secure.

The Data Gap:

Standard browsers offer zero protection against:

- **Shadow AI:** Employees pasting proprietary intellectual property into unapproved LLMs.
- **Visual Leaks:** Sensitive data displayed on-screen being captured via smartphone photos.

The Shift

- **Before:** Security = VPN + Device Management.
- **Now:** Security = Context-aware actions inside the browser tab.

*https://www.paloaltonetworks.com/sase/prisma-browser/omdia-state-of-workforce-security

REAL-WORLD SCENARIO

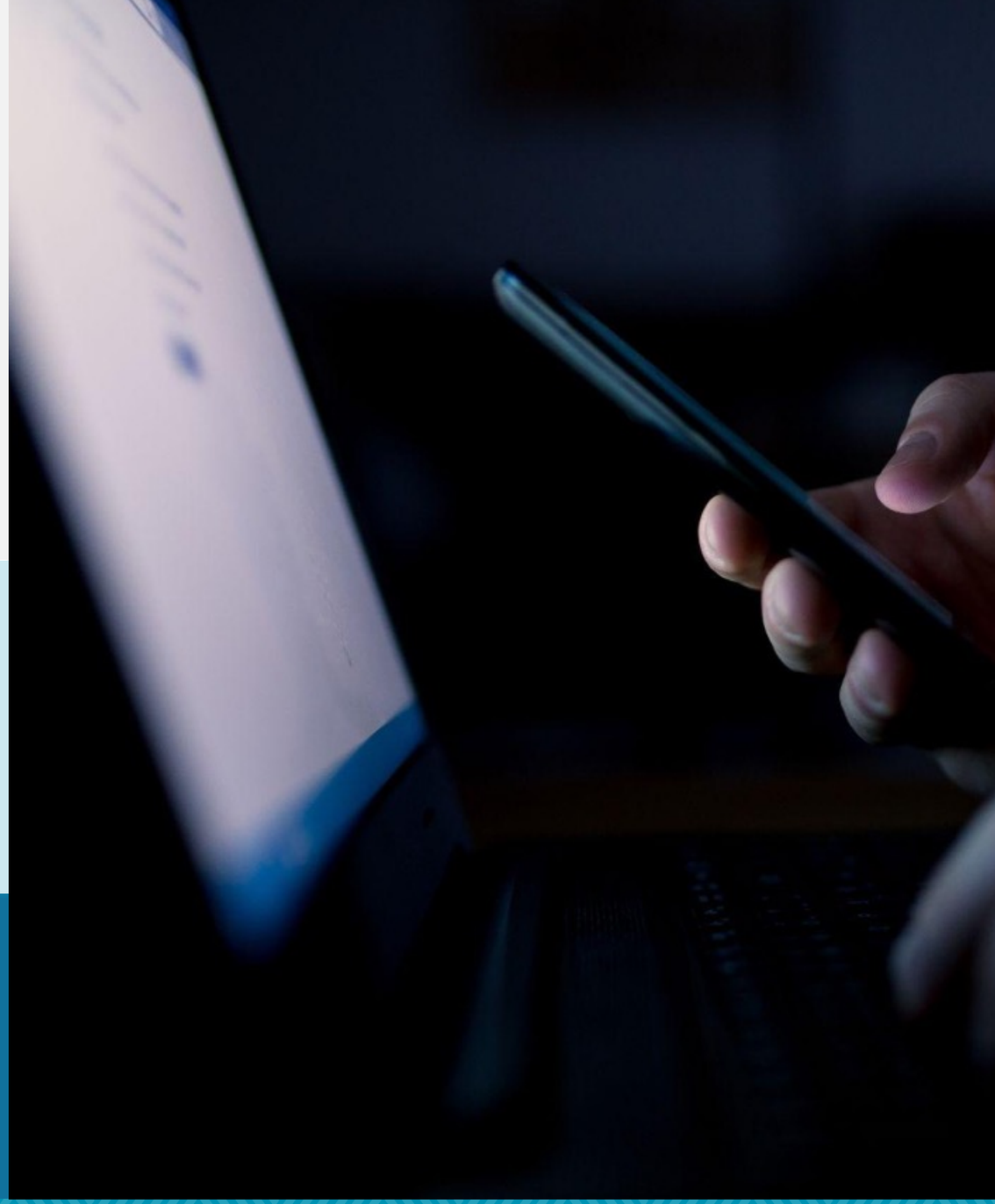
A disgruntled employee is attempting to steal sensitive company data

A dissatisfied employee has been accessing sensitive customer information on their personal device

The employee is attempting to download the data so they can sell it to a third party

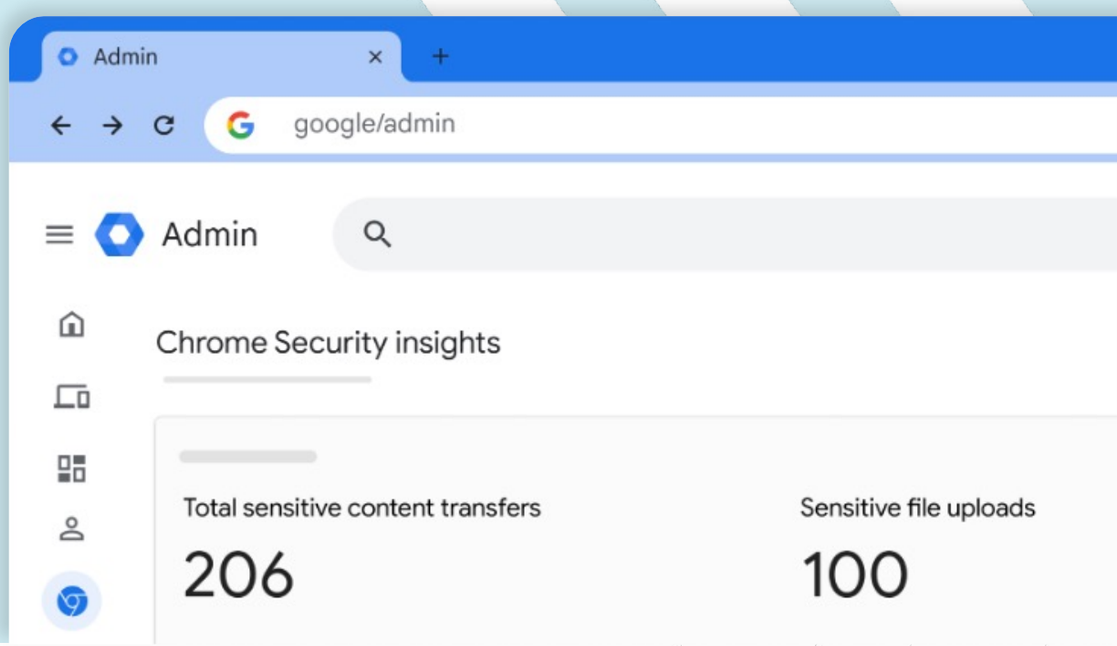
Let’s chat about your security:

How does your organisation handle keeping corporate data secure in scenarios like this?



SOLUTION

Get in-depth visibility into risky behavior and quickly take action



Suspend Chrome profiles or browsers in an unusable state or revoke access to critical apps

Get a granular view of your users' browsing activity with in-depth security insights and event reporting

Save a record of risky behavior to the Evidence Locker for further investigation

Use data loss prevention policies to add a watermark or mask to sensitive data and prevent users from downloading, screenshotting, printing, or pasting it.

REAL-WORLD SCENARIO

Company apps and data are being accessed on unmanaged devices

Employees of an acquired company are still using their old, unsecured devices

A third-party supplier is using their own devices to access your corporate apps and data

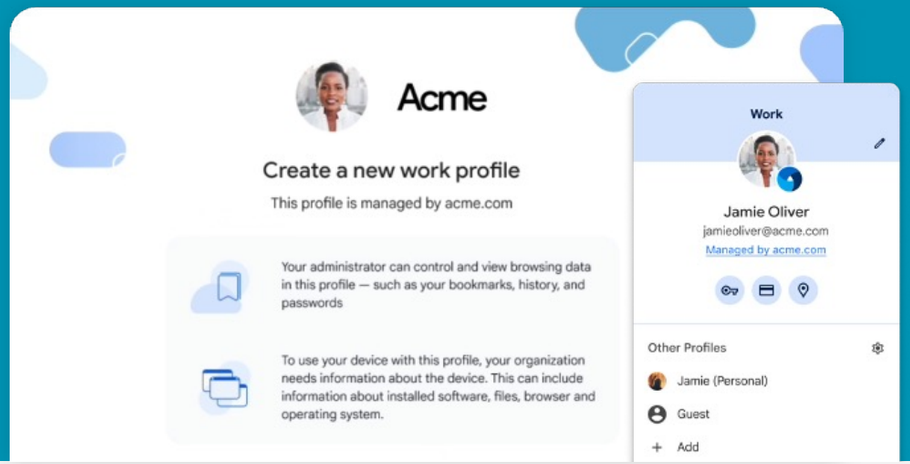
An important project requires collaboration with contractors who work on their personal devices

Let’s chat about your security:
What is your policy for unmanaged devices? Is it enforced?

SOLUTION

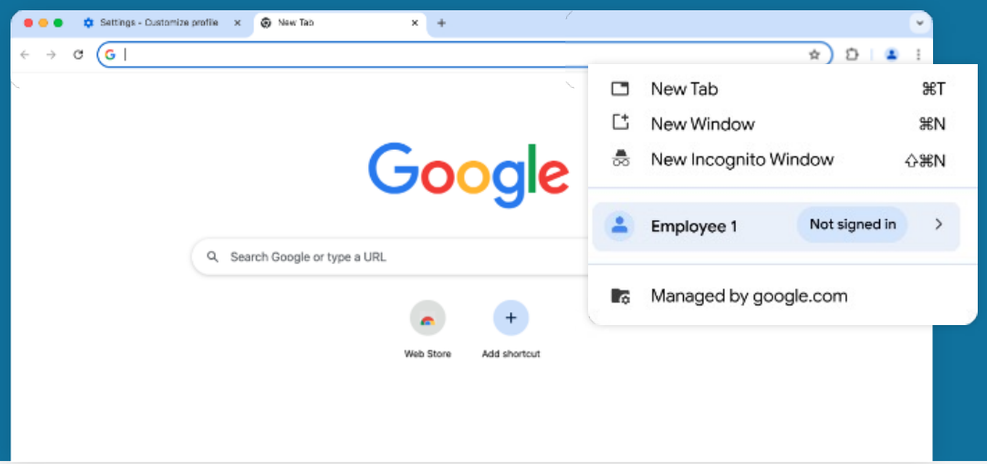
Multiple approaches to management

Manage via profiles



- Requires signing into Chrome with company credentials
- Typically used for devices that arent corporate-owned
- Other profiles (personal, guest, incognito) are unmanaged

Manage the browser



- Requires deployment of an Enrollment Token to set up, but profile is not required for management
- Typically used for corporate-owned devices
- All profiles (corporate, guest, incognito) are managed

A simplified approach to secure access

Browser based approach

- **Flexible** - Enable secure access to any app across all devices, operating systems, and locations.
- **Centralised** - Manage and secure your own browser, apps, extensions, and more, all in one place
- **Insightful** - Unlock powerful insights only possible through the scale of Google's global threat intelligence
- **Fast** - Built-in security and single browser agent enhance speed and user experience
- **Cost-effective** - Get a complete solution for just £6 per user per month

Network-level approach

- **Vulnerable** - SaaS protections can be bypassed on unmanaged devices and networks
- **Constrained** - Insights are limited by the data that's available to the selected solution
- **Fragmented** - Multiple management and security platforms adds complexity for IT and security teams
- **Latency risks** - Multiple agents create a slow user experience
- **Expensive** - Costs can quickly balloon as more tools are added

Cameyo

Chrome Enterprise Premium + Cameyo

Secure the browser you already use, bridge the apps you cannot leave behind.

Chrome Enterprise Premium (CEP):

This is an agentless security layer that provides:

- **GenAI Guardrails:** Contextual prompts appear before a user pastes data, allowing you to block transfers to unapproved AI tools.
- **Visual DLP (Data Loss Prevention):** Protect sensitive information with dynamic watermarking and screenshot blocking to prevent "photo-theft".

Cameyo (Virtual App Delivery):

The bridge for your heritage applications:

- **Native Experience:** Legacy Windows apps appear as individual tabs in Chrome. There is no need for a full virtual desktop.
- **Zero-Provisioning:** Eliminate the need for VPNs or client-side agents on the endpoint.

Better Together:

CEP’s data protection policies extend to the legacy applications you stream via Cameyo. You manage one policy framework for your entire application estate, whether modern SaaS or legacy Windows.

Practical Outcomes Whether Public or Private

Corporate: Agility & IP Protection

Reduce "Citrix Tax":
Ditch the high licensing and hardware costs of traditional VDI. Cameyo streams only the necessary apps, reducing compute requirements and improving the user experience.

Secure Contractors:
Provide secure access to internal tools on unmanaged devices without the friction of installing local security agents.

UK Public Sector: Resilience & Compliance

Audit-Ready:
Meet Cyber Essentials Plus and DSPT requirements using the Evidence Locker and SIEM integration (Splunk/Chronicle) for a clear "paper trail".

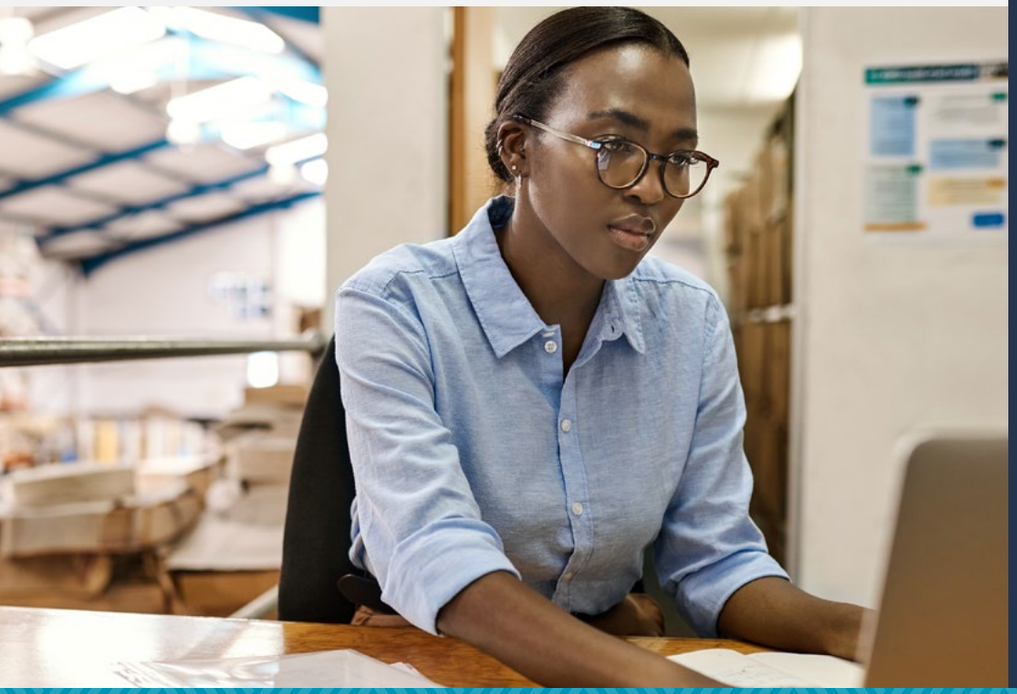
Sustainability & Net Zero:
Extend the life of existing hardware by moving compute tasks to the cloud. This directly supports Greener NHS targets and government e-waste reduction goals.

Heritage App Life Support:
Keep critical "heritage" apps running in a locked-down, modern Chrome environment without requiring an insecure, outdated OS on the device.

The Roadmap

Understand your exposure before you commit.

Modernising your security posture does not require a "big bang" migration. We recommend a data-driven, phased approach to identify risk without disrupting your current workflows.



Chrome Security Insights:

Start with a reporting-only phase. Collect data on existing insider risks, Shadow AI usage, and potential data loss events.

Legacy App Risk Assessment:

We help you identify which client-based apps are acting as "security anchors" and prioritise them for Virtual App Delivery.

The 60-Day Proof of Value:

Test premium features (including deep malware scanning and URL filtering) for up to 5,000 users at zero cost.

XMA

chrome enterprise

Take the First Step

The browser is already your primary workspace. It’s time to treat it like one. XMA can help you build a practical plan to reduce VDI spend and secure your GenAI roadmap.

Contact XMA today to schedule your Chrome Security Insights session or to begin your 60-day trial.

CONTACT US

xma.co.uk @xma @WeareXMA