



Safely Enable 3rd parties and BYOD Using Any Browser

Secure workspaces for
personal / unmanaged devices



The makeup of modern business

Organizations need to enable access to corporate resources for users without corporate devices:

- **Contractors and/or External Service Provider (ESP)** with equipment from another entity
- **M&A/Subsidiary Employees** whose devices are not managed by a central IT department
- **Affiliates** accessing line-of-business apps
- **Bring-Your-Own-Device (BYOD) users** which may encompass all of the above and full-time employees using personal equipment to perform work-related tasks

➤ **Unmanaged devices are part of modern business but are untrusted by definition**

Personal device challenges

Unmanaged devices are an unavoidable reality, requiring organizations to balance:

- **Securing corporate apps and data** accessed by users and devices outside IT control
- **Preserving productivity and privacy** by supporting all browsers without monitoring personal activity
- **Managing cost and complexity** of the infrastructure for secure access to resources

Existing solutions are insufficient

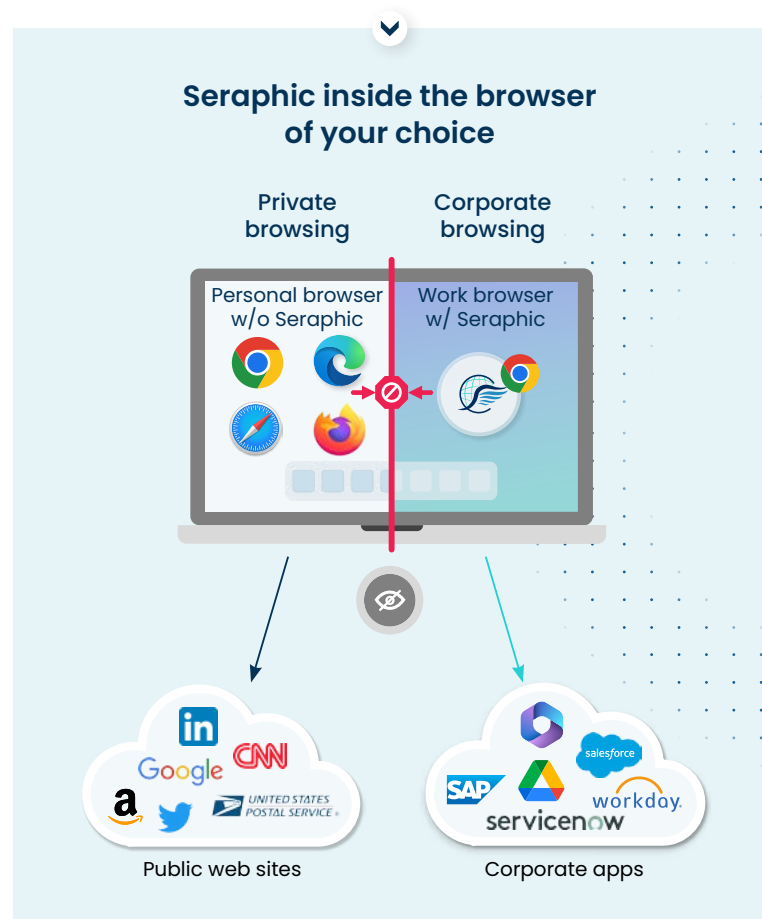
Most methods of enabling unmanaged devices compromise security, experience, or both:

- **CASBs** require traffic steering and may still lack visibility into user activity
- **VDI** requires extensive infrastructure and is subject to compute and network limitations
- **VPN/ZTNA** clients require installation, configuration, and backend infrastructure

Seraphic for personal devices

The Seraphic Agent can be injected into any browser, providing fine-grained visibility and control that enables the enforcement of DLP and governance policies across internal and SaaS web apps.

Seraphic Workspace allows users to choose their favorite browser and a dedicated instance of that browser with Seraphic embedded is created, enabling secure access to corporate resources while maintaining privacy for personal browsing.





A simple and effective solution for BYOD and secure access to corporate apps from unmanaged devices"

Amit Bar On, Former Managing Director, Head of Cyber Services, EY

Why Seraphic?

Seraphic enables productivity and secures enterprise apps and data on unmanaged devices with:

- **Granular governance and DLP policies** that enable scanning, masking, and controlling the flow of sensitive to/from unmanaged endpoints
- **Minimally invasive installation** that does not require installation of an OS agent or an unfamiliar browser
- **Clear separation** between work and personal activities, so users can continue using their preferred browser and maintain their privacy
- **Simple connectivity and access control** that doesn't require installation and configuration of VPN/ZTNA clients, or DaaS/VDI

➤ **Reduce cost and complexity, by replacing CASB, VDI/DaaS, and VPN/ZTNA**

With Seraphic, you get...

Seraphic enables productivity and secures enterprise apps and data on unmanaged devices with:

- Copy/paste/print/screen capture controls
- Corporate branding for browser/workspace
- Data leak notification
- Data masking
- Extension management
- File download/ upload/ encryption controls
- Page watermarking
- Secure controlled access to internal web apps, Citrix and VMware VDI, RDP, SSH/Telnet, VNC
- Session cookie/token encryption
- Web API/URL scheme blocking
- Web app (internal and SaaS) access control
- Web app (internal and SaaS) activity logging

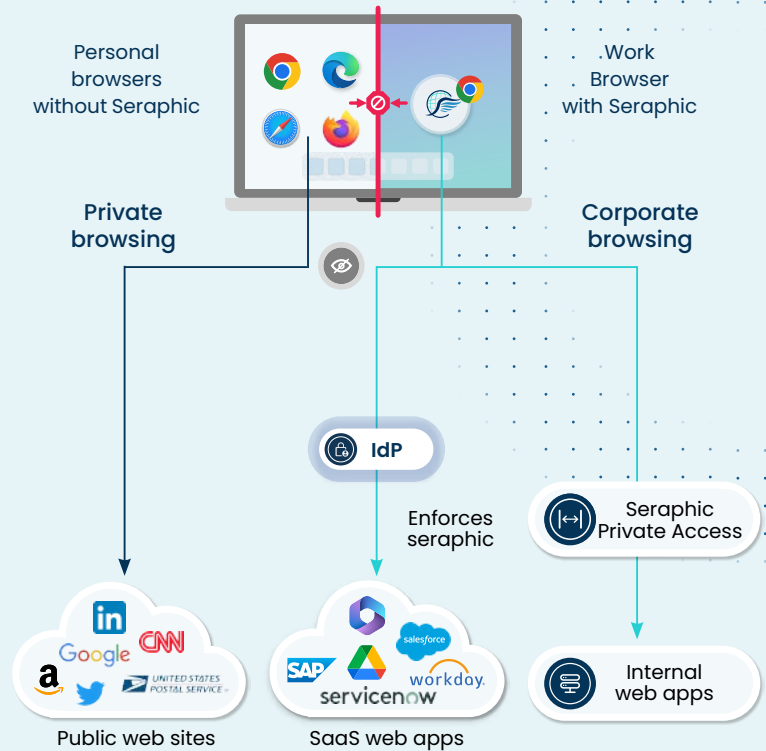


SERAPHIC

Secure Corporate Data | Enable Remote Work

seraphicsecurity.com

Seraphic Workspace for Unmanaged Devices



A standalone instance of an existing browser with Seraphic embedded is created.

Access to **internal applications** including web, Citrix and VMware VDI, RDP, SSH, and VNC is provided by Seraphic Private Access components.

Access to **SaaS apps** is controlled by the IdP which authenticates users and enforces Seraphic.

As users access **corporate resources**, Seraphic controls which data is visible in the browser and where the data can flow.

Personal browsing to the Internet remains completely private using the browser without Seraphic.

Browsers without Seraphic are unable to access internal or SaaS web applications.

Complete coverage of key use-cases

- Employee BYOD
- Corporate App Access
- 3rd-party and contractor access
- VDI alternative
- Distributed Workforce
- Zero Trust