Solutions for unmanaged devices

Safely enable 3rd parties and BYOD on any browser

The makeup of modern business

Today businesses need to enable access to corporate assets, for different stakeholders that don't use a corporate device:

- **Contractors** whose equipment may be supplied by another entity
- **M&A/Subsidiary Employees** whose devices may not be managed by a central IT department
- **Affiliates** that require access to corporate resources
- **Bring-Your-Own-Device (BYOD) users** which may encompass all of the above—as well as some full-time employees—using personal equipment to perform work-related tasks

> **Unmanaged devices are part of the modern business, yet they are untrusted by definition**

Unmanaged device challenges

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

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

Existing solutions are insufficient

Most methods of supporting unmanaged compromise security, productivity, or both

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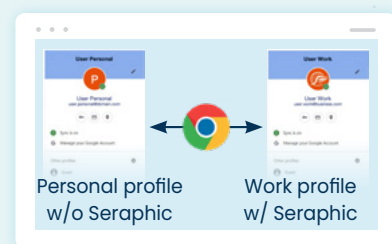
Seraphic for Unmanaged Devices

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. Multiple deployment options allow organizations to choose the best method for their needs:

- **An enterprise browser profile** – A separate Seraphic-protected profile exclusively for work-related activity
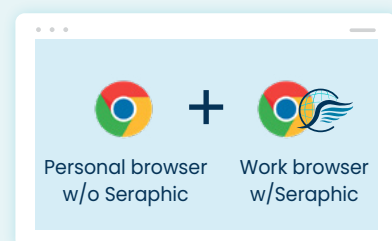- **An enterprise standalone browser** – A Separate commercial browser with Seraphic embedded

Seraphic inside the browser of your choice

Alternative A
Separate enterprise profile

Personal profile w/o Seraphic   Work profile w/ Seraphic

Alternative B
Separate enterprise browser

Personal browser w/o Seraphic   Work browser w/Seraphic

Why Seraphic?

Seraphic enables productivity and secures enterprise apps and data on unmanaged devices with:
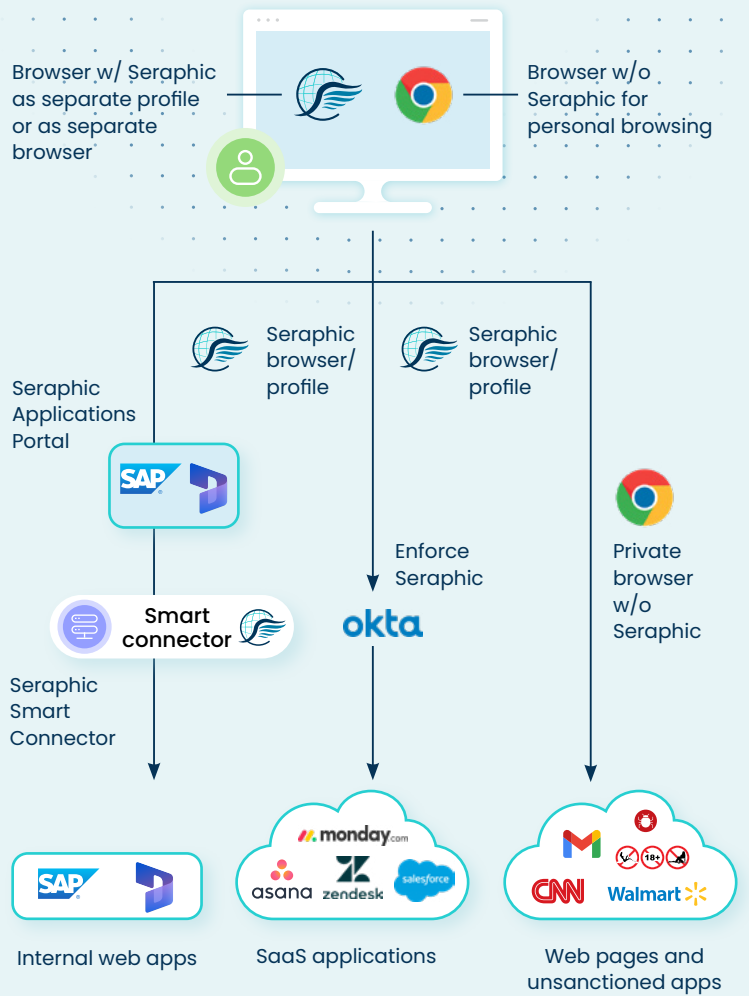
- **Granular governance and DLP policies** that enable scanning, masking, and controlling the flow of sensitive to/from unmanaged endpoints

- **Minimally invasive installation** that does not require installation of an OS agent or an unfamiliar browser

- **Clear separation** between work and personal activities, maintaining privacy so users can continue using their preferred browser

- **Simple connectivity and access** control that doesn't require installation and configuration of VPN/ZTNA clients, VDI/DaaS, or substantial on-premises infrastructure

> **Reduce cost and complexity, replace CASB, VDI/DaaS, and VPN/ZTNA**

With Seraphic, you get...

- Copy/paste/print/screen capture controls
- Credential leak notification
- Credential reuse protection
- Data leak notification
- Data masking
- Device posture checking
- Extension management
- File download/ upload/ encryption controls
- Real-time session control
- Session encryption and protection
- Watermarking
- Web API/URL scheme blocking
- Web app (internal and SaaS) activity logging
- Web app (internal) vulnerability protection

Seraphic for Unmanaged Devices

Browser w/ Seraphic as separate profile or as separate browser

Browser w/o Seraphic for personal browsing

Seraphic Applications Portal

Seraphic browser/ profile

Seraphic browser/ profile

Enforce Seraphic

Private browser w/o Seraphic

Smart connector

Seraphic Smart Connector

okta

Internal web apps

SaaS applications

Web pages and unsanctioned apps

A **separate enterprise profile** is created in an existing browser and Seraphic is installed **OR** a **standalone browser** with Seraphic embedded is installed.

Access to **internal web applications** is granted with a combination of the Seraphic Application Portal and the Seraphic Smart Connector.

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 is done under full privacy with the browser w/o Seraphic

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

SERAPHIC   Secure Corporate Data | Enable Simple Connectivity ——— seraphicsecurity.com