seraphic Protect the Endpoint | Secure Corporate Data | Enable Remote Work

Enable Your Hybrid Workforce with Any Browser

Protection, visibility & control for corporate / managed devices

The modern office isn't a "place"

The idea that work is something people do, not somewhere they go is not a new one. Today's workplaces are digital, starting with a company-issued device and a combination of:

- **Multiple browsers** that allow access to the public Internet and corporate web apps
- **Modern** desktop **apps** for SaaS like Asana, Microsoft Teams, Notion, and Slack for collaboration and sharing data between co-workers and 3rd-parties.

These tools support employee productivity but they also expose organizations' users, endpoints, and data to a wide range of threats.

Users can be anywhere, corporate resources are everywhere

Introducing Seraphic Security

Seraphic is a light browser agent operating directly in the JavaScript Engine that transforms any browser into an enterprise browser by creating a defensive layer of security and governance that controls both the code the browser renders and the actions users take.

Seraphic protects the digital workplace and new perimeter: browsers and apps

Seraphic provides...

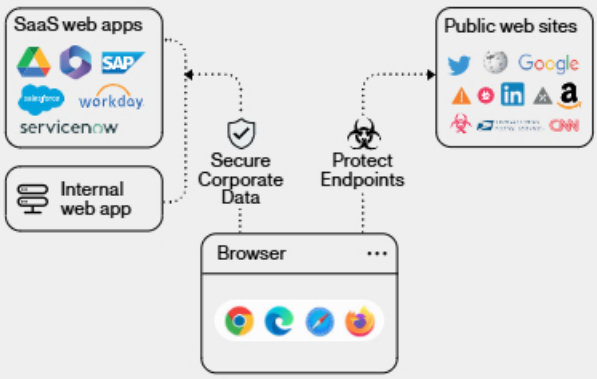
Security	Robust security without browser isolation (LBI/RBI) or proxy (SWG)
Governance and DLP Controls	Monitoring/ control of all browser activity
Connectivity and Access Control	Provide and control access to enterprise resources without CASB, VDI/ DaaS, or VPN/ ZTNA

The main security concerns

Even though the places and ways employees work have changed, organizations must accommodate familiar requirements:

- **Protecting user identities and endpoints** from compromise via the Internet due to exploitation, phishing, and other web-based attacks
- **Preventing corporate data leakage or loss** as it is handled in locations where traditional enterprise security controls are not deployed
- **Providing, controlling, and auditing access** to internal and SaaS-based web applications
- **Enforcing Acceptable Use Policies** (AUPs) by restricting access to web content
- **Mitigating risk from shadow IT** by identifying unsanctioned services
- **Supporting multiple browsers** for application compatibility and user productivity

Consistent security and policy enforcement on-and off-premises is critical



> **Seraphic enabled us to improve security and user experience, increase visibility of external threats, while reducing our infrastructure and costs"**
>
> ***Haim Inger, CTO & VP of Infrastructure & operations at Clal Insurance & Finance***

Why Seraphic?

Seraphic Security reduces the complexity and cost of protecting your managed devices and securely enabling a hybrid workforce by:

- **Protecting against** sophisticated **phishing** such as spear phishing and reverse proxy phishing (e.g., EvilProxy)
- **Stopping** JavaScript **malware** like GootLoader and SocGholish
- **Preventing exploitation** of browser vulnerabilities
- **Managing** browser **extension risk** by identifying and disabling risky extensions
- **Securing** sensitive **data** from leakage or loss with data masking, file upload/download controls, and user action (copy/paste, print, screenshot, etc.) controls.
- **Controlling** SaaS and web-based **application access** without proxies, DaaS/VDI, or VPN

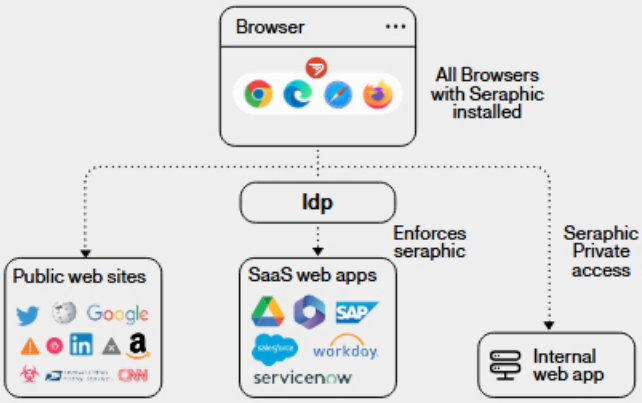
Existing solutions lack visibility and control

Other browser security solutions do not offer the breadth and depth necessary to defend the digital workplace:

- **Browser Isolation** only protects against small subset of threats and severely compromises user experience
- **Enterprise Browsers** emphasize DLP for personal / unmanaged devices and don't protect endpoints
- **Security Extensions** are constrained by the APIs and capabilities exposed by mainstream browser vendors
- **Security Service Edge (SSE)** relies on complex traffic steering and analysis that does not prevent unidentified attacks and does not any offer in-browser control

Seraphic provides the broadest protection and best user experience

Seraphic for corporate devices



- Seraphic Agent is distributed to all browsers by vendor extension installed as a corporate policy via tools like Jamf, BigFix, Intune, VMware Workspace ONE, GPO, etc. Thus ensuring that the device is protected when user is browsing to public sites by any browser installed on the device.
- Remote users can access internal web applications without VPN/VDI through the Seraphic Application Portal and Seraphic Smart Connector.
- IdP enforces Seraphic installation to ensure secure access to SaaS apps, devices w/o Seraphic cannot access internal or SaaS apps.

Why Customers Choose Seraphic

Superior Security

We created the first and only ASLR in the browser

We stop attacks that other cannot!

Full Productivity

User maintains their favorite browser

No need to change the browser!

Reduced Cost

Consolidate many existing tools with one browser client

Simplify your security architecture!

Complete coverage of hybrid work use-cases

- Safe browsing
- RBI Replacement
- Extension Management
- Corporate App Access
- GenAI Enablement
- Zero Trust

Replace RBI | **Replace CASB** | **Replace SWG** | **Replace VPN / ZTNA** | **Replace VDI/DaaS**