



Next Generation

Enterprise Browser Security on any browser



The new security paradigm

In the modern business, users can be anywhere: working on-campus or remotely. Corporate resources and data are everywhere: on-premises data centers and in the cloud. Web browsers are the tool that connects these distributed users and resources, making it the most-used enterprise application. However, browsers also expand the endpoint attack surface and create a data leakage/loss vector.

➤ **Browsers are the main productivity tool and the most serious threat to businesses**

The key security concerns

Protecting the endpoints against compromise via the Internet due to exploitation, phishing and other web-based attacks.

Securing corporate data against leakage or loss as it is accessed by employees and 3rd parties on managed and unmanaged devices.

➤ **Organizations need to protect the EP from untrusted sites and to secure their data from untrusted devices**

Existing defenses are insufficient

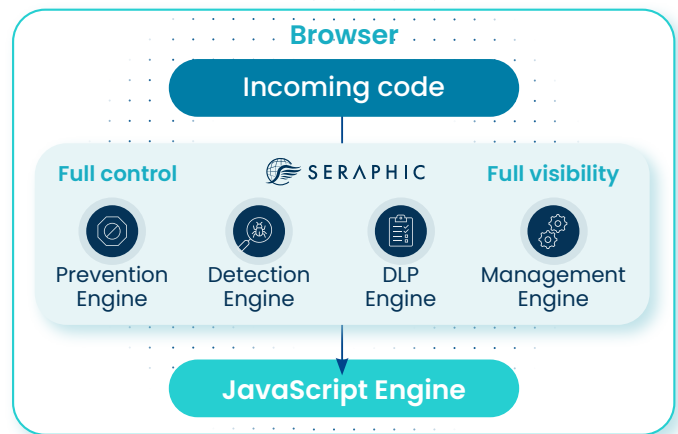
Existing solutions lack the necessary visibility into the browser and thus fail to protect the browser or to secure the corporate data as it is accessed via the browser.

➤ **Existing solutions are too complex, expensive and compromise user experience & productivity**

Introducing Seraphic Security

A light agent injected into the browser, any browser, converting it into an enterprise grade browser. The Seraphic agent creates an abstraction layer between the executing code and the browser JavaScript Engine (JSE).

➤ **The browser is the "New OS" and it requires its own solution. The Seraphic agent is the only solution working directly inside the JSE**



What makes us different?

- ✓ **Unique Prevention Engine** that stops 0-days and unpatched N-days without detection techniques
- ✓ **Unique Detection Engine** that stops web-based and phishing attacks without threat intel feeds
- ✓ **Unique DLP Engine** that performs content scanning, data masking, controls the flow of sensitive data
- ✓ **Unique Management Engine** for visibility and fine-grained policy enforcement

We stop attacks that others cannot

Seraphic provides an easy and light solution, with top detection and prevention capabilities for all web-based threats.”

Yaron Slutzky, CISO at Agoda Booking Holdings Group

With Seraphic you get

> Security features

- Exploit prevention
- Web-based attack protection
- Phishing protection
- Adversary-in-the-Middle protection
- Network scanning prevention
- Identity/Credential protection

> Governance features

- User action restrictions
- Data Leakage/Loss Prevention (DLP)
- Content filtering
- Extension management
- Privacy controls
- Audit logging

Easy and fast deployment to the whole organization within minutes

- **Extension based** - Seraphic agent is distributed by an extension installed as a corporate policy via tools like Jamf, BigFix, Intune, VMware Workspace ONE, GPO, etc.
- **Proxy based (without extension)**
Forward proxy - for corporate outbound traffic
Reverse proxy - for corporate inbound connections to internal web apps

Seraphic integrates with all leading IdP, SIEM, Malware analysis, Sandbox, and CDR platforms.

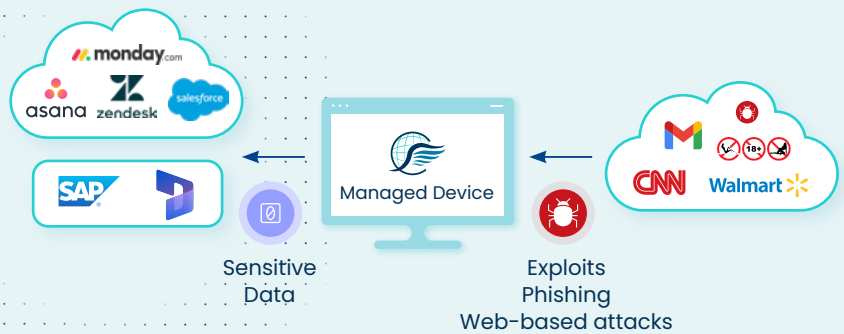


Complete coverage of hybrid work use cases

> Managed Devices

Employees on-premises and remote/WHF

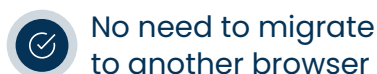
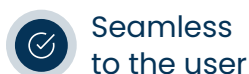
- Safe Browsing** Robust security
Full replacement of RBI
Reduce SWG
- DLP** Full control/monitoring of browser actions
Reduce CASB
- Remote work** Simple connectivity
No need for VDI/VPN



> Unmanaged Devices

BYOD, 3rd Parties, Contractors, Affiliates, M&A Employees

- DLP** Full control/monitoring of browser actions
Reduce CASB
- Remote work** Simple connectivity
No need for VDI/VPN
- Privacy** Full separation between private and corporate browsing



SERAPHIC

Protect the Browser | Secure Corporate Data

seraphicsecurity.com