seraphic Stopping attacks that other solutions cannot

Enable Safe Browsing On Any Browser

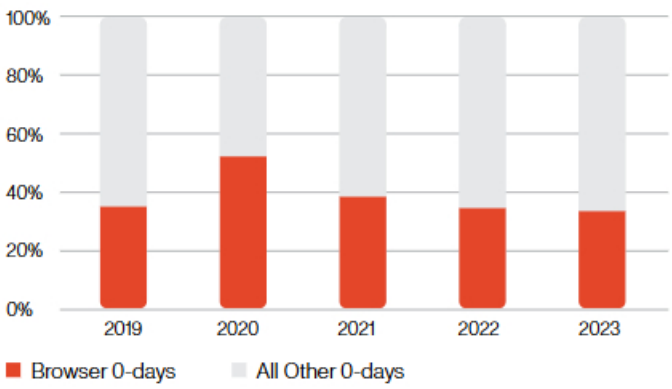
Attack prevention and detection

Web-borne threats are on the rise

Web browsers are vulnerable because they have large, complex codebases. All complex systems have bugs, some of which manifest as security vulnerabilities and browsers had over 700 vulnerabilities in 2022 alone. Browsers are also at risk because they are one of the few applications whose purpose is processing external code (such as scripts and extensions).

Web browsers are targeted because they are ubiquitous, but also because they are mixed-use. Browsers have access to both personal and business credentials and data, making them valuable to a wide variety of adversaries who have focused on exploiting them

Nearly 40% of the zero-day exploits in the wild over the past 5 years target browsers



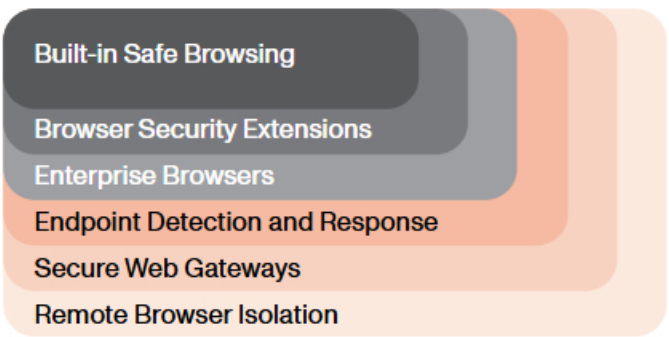
Web browsers are core to other attacks such as phishing where email may be the lure but the damage comes when users supply credentials to malicious sites. They are also the target of web-based malware.

76% of ransomware in 2022 was delivered via web browsing (up from 12% in 2021)

Existing solutions are insufficient

The diverse range of threats impacting browsers have spawned an equally diverse array of solutions:

- **Built-in Safe Browsing** is a consumer-focused feature that relies entirely on threat feeds of known malicious sites and known malware
- **Browser Security Extensions** have restricted functionality and are unable to provide comprehensive visibility and protection
- **Enterprise Browsers** inherit the vulnerabilities of Chromium, do not provide additional prevention and detection capabilities, and require users to adopt unfamiliar browsers
- **Endpoint Detection and Response (EDR)** monitors the OS for abnormal behavior but has no ability to monitor code execution within browsers
- **Secure Web Gateways (SWG)** depend on traffic steering and decryption which degrade user experience, as well as threat feeds resulting in a high rate of false negatives
- **Remote Browser Isolation (RBI)** can limit the impact of certain types of attacks but offers no protection against phishing or other forms of credential theft, and is costly, complex, and compromises user experience



Browser exploitation

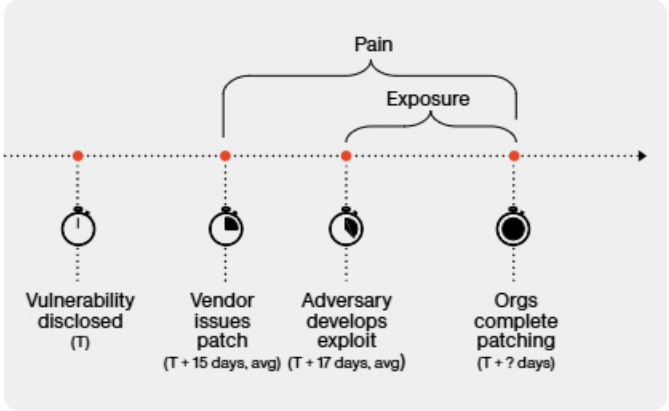
The term "patch gap" refers to the period between when a vulnerability is identified and when affected systems are fully patched. It can be further divided into 3 phases:

- Prior to disclosure to the vendor (zero-day)
- After disclosure, but prior to a remedial patch being released (N-day)
- After the release of a patch, but prior to 100% patch installation (N-day)

Although it takes vendors an average of 15 days to release a patch, adversaries are either ahead or not far behind, while organizations may struggle to achieve 100% coverage, even after weeks or months.

There is both significant operational overhead and considerable exposure during the patch gap as IT and security teams attempt to shore up their defenses.

In 2023, browser vendors issued 19 emergency patches addressing zero-days being exploited in the wild—Seraphic prevented exploitation of all of them



Source: Google Project Zero and RAND Corporation

Seraphic bridges the patch gap

Seraphic's patented technology stops 0-day and and unpatched N-day browser exploits without relying on any detection techniques.

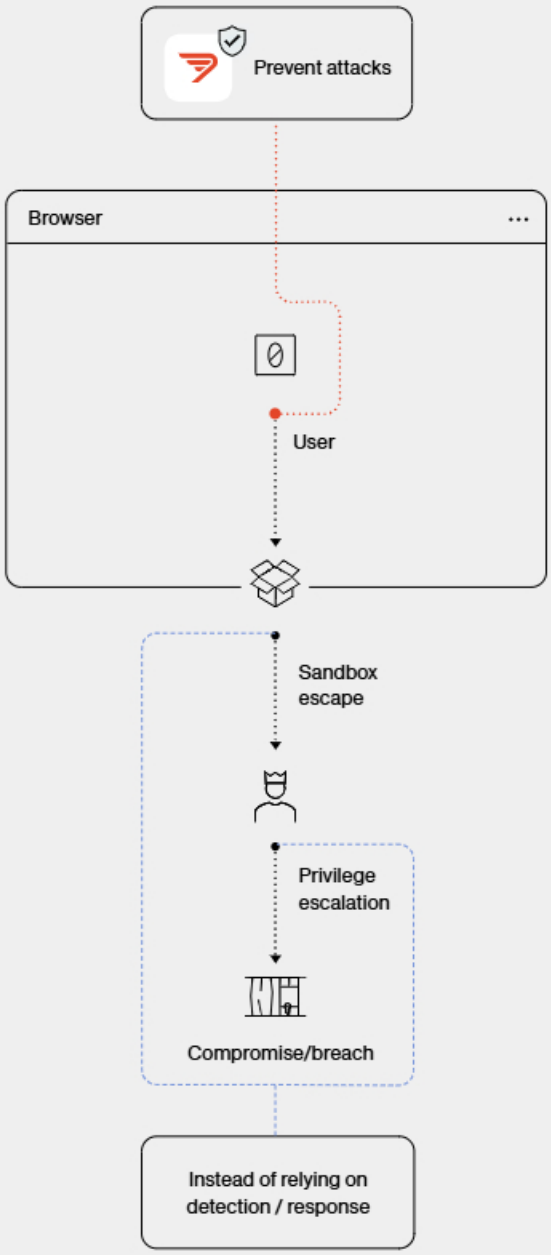
Seraphic unique Prevention Engine:

- Works in any browser
- Implements a form of **Moving Target Defense** (MTD) similar to Address Space Layout Randomization (ASLR) that disrupts exploits without any prior knowledge of them
- Immunizes the browser by stopping exploitation of memory corruption vulnerabilities
- Has a very low rate of false negatives

These capabilities help organizations stay safe throughout the entire **patch gap**, even if they don't know they're in it.

Seraphic stops attacks at the beginning of the exploit chain

Seraphic prevents exploitation even if the techniques and patterns are unknown.



Other solutions depend on known patterns to detect and respond to exploitation at later stages of the exploit chain, increasing the likelihood of false negatives and compromise or breach.

Seraphic is an ideal replacement for Remote Browser Isolation (RBI), offering better protection without impacting productivity

Account compromise

Valid **user identities** and credentials are the easiest way for adversaries to access enterprise resources. **Phishing** is the easiest and most reliable method of harvesting credentials, but organizations typically have only two types of defense:

- **URL filters** built on lagging indicators in databases or threat feeds
- **User awareness training**, which has limited effectiveness against increasingly sophisticated campaigns.

Over 37% of phishing site visits occur after a site has been identified as malicious

Adversaries can access corporate data within 72 minutes of compromising an account.

Seraphic protects credentials

Seraphic's position in the browser gives it unique visibility and enables it to provide superior protection against phishing and other forms of credential compromise.

Seraphic unique Detection Engine:

- Measures and evaluates 200+ runtime parameters to identify **malicious sites** in real time, without site classification or threat feeds
- Detects and blocks UI redressing attacks such as **Browser-in-the-Browser** (BitB) and clickjacking that are commonly used on phishing sites
- Is not susceptible to evasion techniques (such as **malicious pages behind a CAPTCHA**) that circumvent automated phishing protection tools

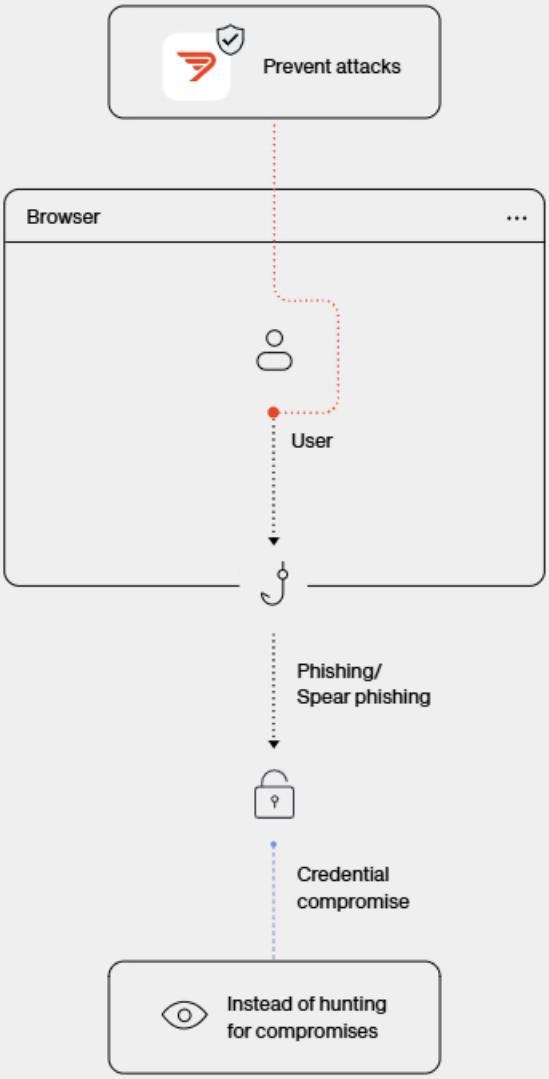
Seraphic also provides:

- **Password re-use prevention** to stop password sharing between sites or accounts
- **Encryption of session cookies** and tokens to prevent user impersonation
- **Credential leak notification** to alert organizations if their users' credentials have been exposed

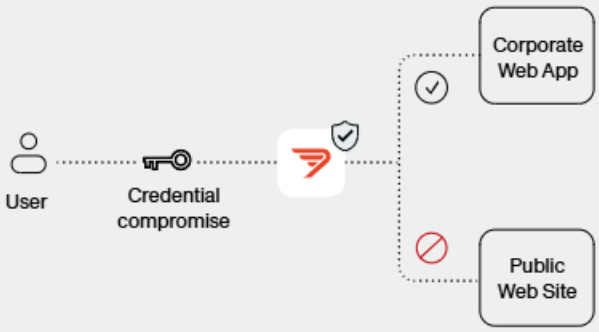
Seraphic is the only solution that protects users against 0-hour/ "golden hour" phishing attacks and guards authentication material inside the browser.

Seraphic detects phishing attacks that bypass other security tools in customer environments at a rate of 2–3 per month

Seraphic creates an additional layer of phishing protection



Seraphic blocks corporate credential re-use between sites



> **Top-Notch Security, Seamless Integration: A Game-Changer in Enterprise Browser Security"**
>
> *VP, IT & Security in the Media Industry*

Web-based attacks

Adversaries rely on web-based attacks because many security tools are unable to distinguish between benign and malicious activities. Web browsers are a reliable channel for them deliver malicious code, intercept and manipulate data, trigger unauthorized actions in web sites, and even "steal" compute resources or conduct network reconnaissance.

Seraphic protects credentials

By performing analysis locally on session information and external code passing into the browser runtime, Seraphic identifies and blocks attacks in real time.

These capabilities create robust defenses against:

- **Adversary-in-the-Middle (AitM)** attacks that can compromise sensitive data
- Attacks used for **malware delivery,** such as Cross-Site Scripting (XSS) and drive-by downloads/HTML smuggling
- JavaScript malware such as **GootLoader** and **SocGholish**
- Downloading infected files
- **Network scanning** that aids attackers in identification of additional targets
- **Cryptojacking** that consumes compute resources and provides financial resources to threat actors

In 2023, Seraphic blocked JavaScript malware an average 100 times per month

Additional capabilities

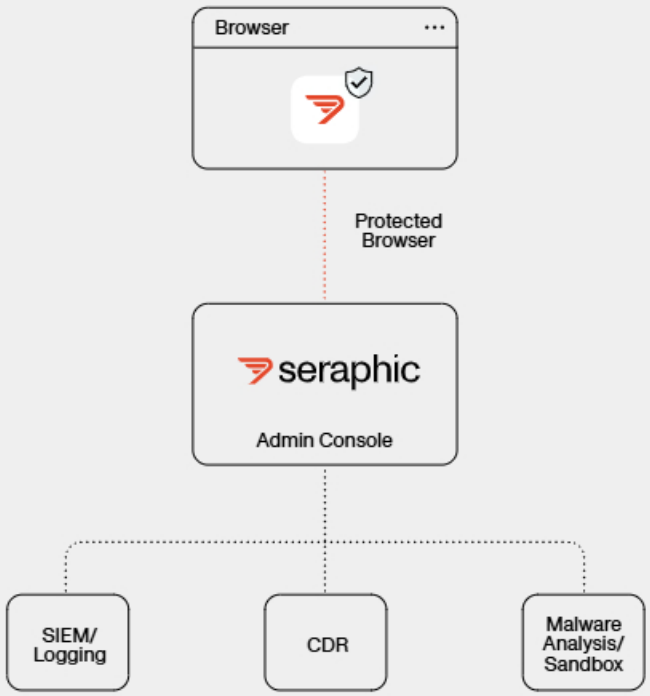
Seraphic also provides:

- **Extension management** to evaluate extension risk, allow/block specific extensions, and control permissions
- **Content filtering** for Acceptable Use Policy (AUP) enforcement without proxies

Seraphic Vs Other Solutions

	Seraphic	Browser Extensions	Enterprise browsers
Zero-day prevention	✓	✗	
Malicious JavaScript Protection	✓	✗	
Clickjacking Protection	✓	✗	
HTML Smuggling Protection	✓	✗	
XSS Protection	✓	✗	
Extension Control	Full control of all extensions	Limited control of other extensions	Only controls extensions in enterprise browser

Seraphic integrates with the enterprise security stack



Seraphic can send its unique telemetry to any SIEM or log aggregation system and can send downloaded files to CDR systems or sandboxes for additional processing