Technical Validation

Enterprise-grade Browser Security and Governance with Seraphic

Browse Safely Everywhere and with Any Browser

By Justin Boyer, IT Validation Analyst; and Tony Palmer, Principal IT Validation Analyst

August 2022

Introduction

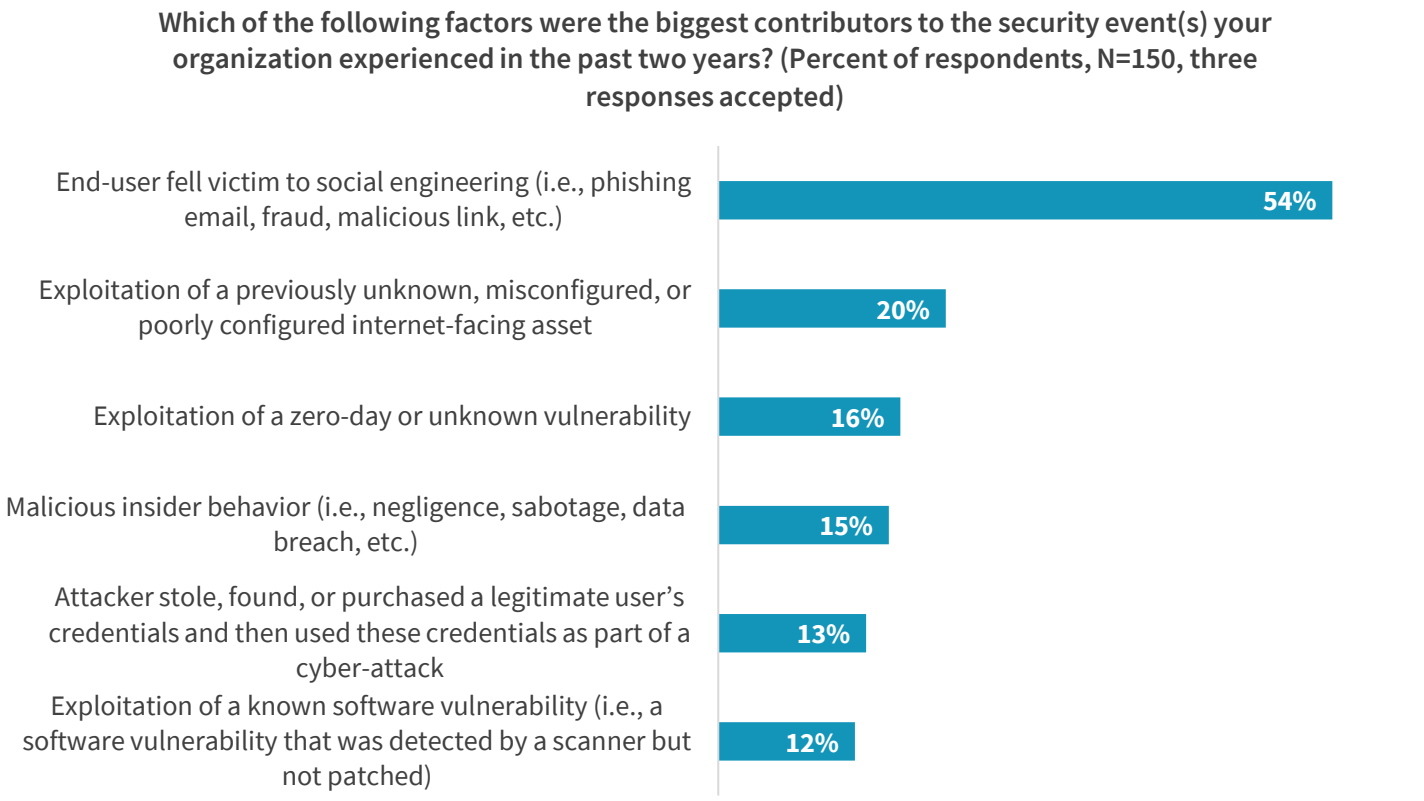
This ESG report details the evaluation of Seraphic. We validated Seraphic's ability to prevent cybersecurity attacks through the web browser, enforce company policy, and maintain compliance without affecting the end-user experience. Seraphic incorporates strong protection and governance into all browsers seamlessly.

Background

The web browser has become a main working and productivity tool for modern organizations. Employees use internally created web applications and software-as-a-service (SaaS) tools daily. In addition, public websites also play a critical role in workers' productivity, such as for research or news. The browser's importance to daily work has led it to become a common attack vector. The wrong link or visited page could lead to browser compromise, putting enterprise and user data at risk.

According to ESG research, more than half of organizations (54%) cite end-users falling victim to social engineering (phishing, malicious links, etc.) as one of the biggest contributing factors to security events they have experienced (see Figure 1). Other large contributing factors include zero-day as well as known vulnerabilities that were exploited.[1] Organizations must work harder than ever to protect their end-users. ESG research shows more than half of organizations see either fortifying cybersecurity or improving operational resiliency against cyber-attacks as a top business initiative driving technology spending.[2]

Figure 1. Top 6 Biggest Contributors to Security Events



Source: ESG, a division of TechTarget, Inc.

[1] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.
[2] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

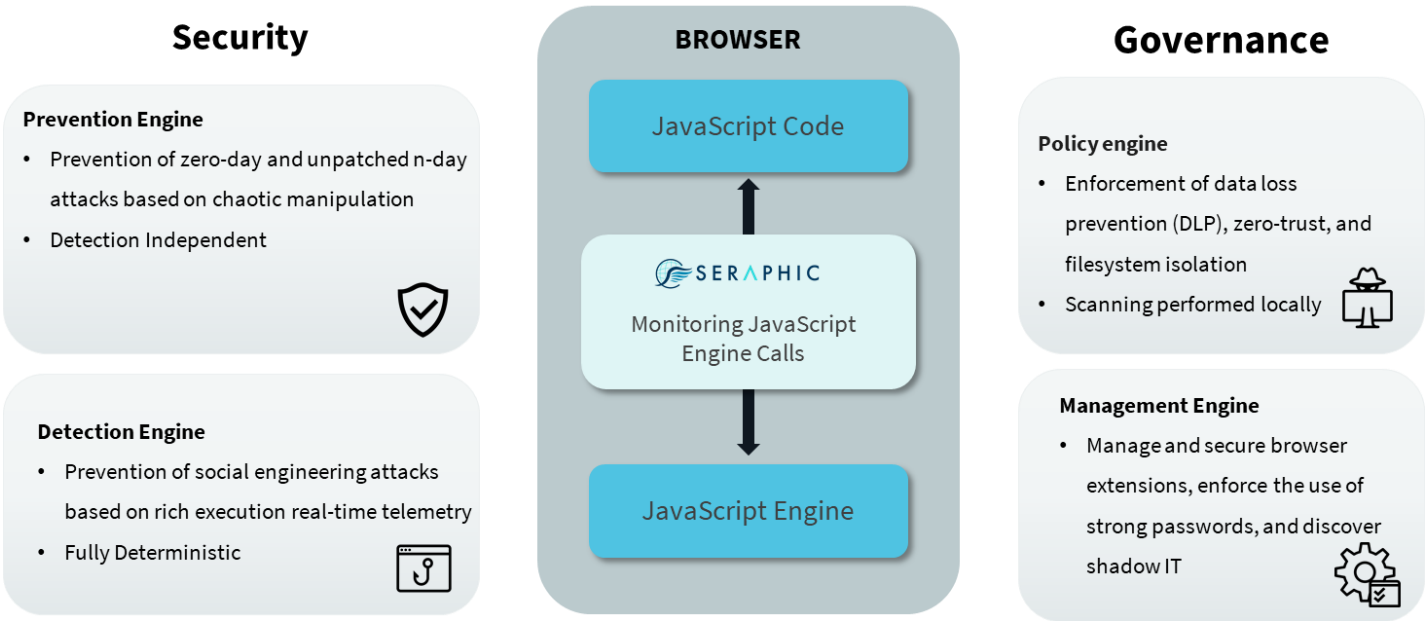
As the remote workforce grows, enforcing company policies across all devices, including mobile devices used in a bring-your-own-device (BYOD) environment, becomes a greater challenge. The goal of consistent policy enforcement and data loss prevention (DLP) across all end-user devices has led organizations to depend on multiple tools, increasing cost and complexity to manage them all. 35% of organizations surveyed by ESG buy security products and services from more than ten vendors.[3] Despite some feature overlap in vendor products, multiple vendors are needed since no one vendor covers all use cases an organization might need. Organizations require reliable browser security and compliance tools that won't degrade the user experience.

Seraphic Security

Seraphic provides robust exploit prevention, phishing and web attack protection, fine-grained DLP controls, and governance tools for browser and other JavaScript environments (i.e., Office 365 and Electron applications). Seraphic's JavaScript Browser Agent (JSA) is injected into every browser session, creating an abstraction layer between the running code and the JavaScript engine (JSE) that intercepts and controls all JSE calls. Seraphic's Browser Agent is comprised of four different engines: Seraphic's exploit prevention engine creates a non-deterministic environment without interfering with normal operations. Rather than relying on detection techniques, which can fail to recognize unknown patterns, the Seraphic exploit prevention engine focuses on making it impossible for any exploit to work. In parallel, Seraphic operates a detection engine independently of the exploit prevention engine, which provides detailed real-time execution telemetry, enabling the prevention of social engineering and other web-based attacks. In addition to the prevention and detection engines, Seraphic also provides policy and management engines covering browser visibility, control, and governance for all browsers across all devices.

Figure 2 illustrates the high-level architecture of the Seraphic Browser Agent. The Seraphic Browser Agent is injected into every session, creating an abstraction layer between the input JavaScript code and the JavaScript Engine that intercepts and control all JSE calls. Seraphic attests that the location and approach make their solution unique in the marketplace.

Figure 2. Seraphic Browser Agent



Source: ESG, a division of TechTarget, Inc.

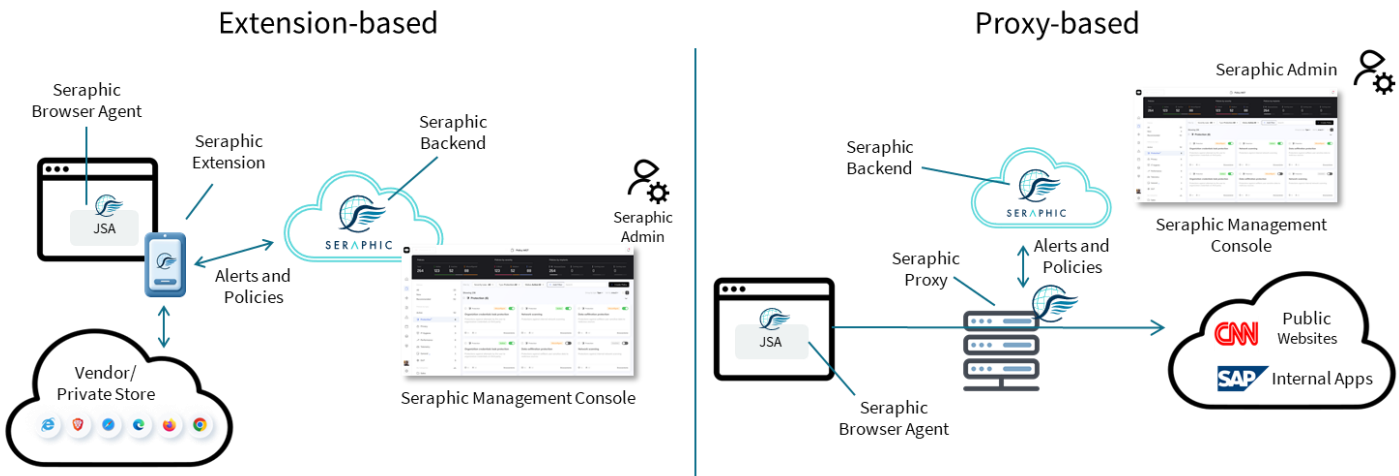
[3] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

Seraphic's architecture enables four main benefits:

- All processing happens on the local device. This enables maximum efficiency, no latency, and data security by preventing the exploit at the point of attack. It also prevents sensitive data from being sent to a separate server for processing.
- It provides protection and compliance enforcement while providing a seamless user experience. Users will use the web browser in the same way as before, without connecting to a remote or custom browser to perform their work.
- It's compatible with any device, including mobile devices. Seraphic can be deployed to all devices, managed or unmanaged, remote or on-prem, and even to third-party contractors.
- Deployment is frictionless and scalable. Administrators deploy Seraphic agents across the enterprise easily with no interruption to end-users.

Figure 3 illustrates Seraphic's deployment process. The security team defines the desired policies and security protections. Then, they use the Admin Console to deploy the Seraphic browser extension to end-user devices via vendor or private marketplaces. Deployment can be done automatically and silently by standard corporate distribution tools to managed devices and in one click via an emailed link in unmanaged devices. The extension injects Seraphic's lightweight JavaScript Browser Agent into the browser. The JSA then communicates through the Seraphic extension with the Seraphic backend to receive policies and settings and regularly check for updates. All of this happens in the background for employees with no interruption to their work. Alternatively, the same JavaScript Browser Agent can be injected into each session seamlessly by a proxy, without requiring the installation of the Seraphic Extension. It's important to note that in both cases, the Seraphic Browser Agent is JavaScript code injected into every session and exists only during the session.

Figure 3. Seraphic Deployment and Administration



- **Seraphic Extension** - Installed from a vendor or private store
- **Seraphic Browser Agent (JSA)** - Injected by Seraphic extension into each user session

- Seraphic Browser Agent (JSA) injected into user sessions by **smart proxy**
- **Forward proxy** – for traffic moving from on-premises endpoints to internal and external apps
- **Reverse proxy** – for traffic moving inward from off-premises endpoints to internal web apps

Source: ESG, a division of TechTarget, Inc.

ESG Technical Validation

ESG performed validation of Seraphic's capabilities via remote demonstration with the goal of assessing how Seraphic protects users and enterprise data from attackers. Specifically, ESG evaluated Seraphic's exploit prevention engine, its seamless user experience and easy deployment, and its compliance and policy enforcement tools.

Exploit Prevention Engine

Browser exploits rely on the predictable nature of certain low-level primitives within the JavaScript engine. These primitives can be manipulated by an attacker to perform unintended functions.

Imagine a cyber-criminal looking to steal a person's identity. They would need several pieces of information, such as the person's name, address, government ID, and bank account information, to name a few. An effective solution would be to prevent the criminal from obtaining any one of these necessary data points.

Similarly, Seraphic's exploit prevention engine eliminates the predictable nature of a JavaScript environment by "scrambling" those primitives in a way that doesn't affect the execution of legitimate code but prevents malicious code from finding what it needs to function. Chained attacks find no foothold within the environment.

The prevention engine doesn't rely on any detection techniques and treats code received from a highly trusted domain in the same way it treats code received from a less trusted or even suspicious site. This approach enables the Seraphic exploit prevention engine to prevent unknown patterns like zero-day exploits that detection-based solutions can fail to detect because signatures of the attack have not yet been captured to use for detection.

Protect Users from Malicious Attacks

ESG tested Seraphic's ability to prevent common web-based attacks that could lead to data or user credential compromise.

Seraphic uses a just-in-time intervention approach to protect end-users without interrupting their work. Even if a malicious payload has been detected, the user session will continue as usual while the malicious payload is terminated by Seraphic.

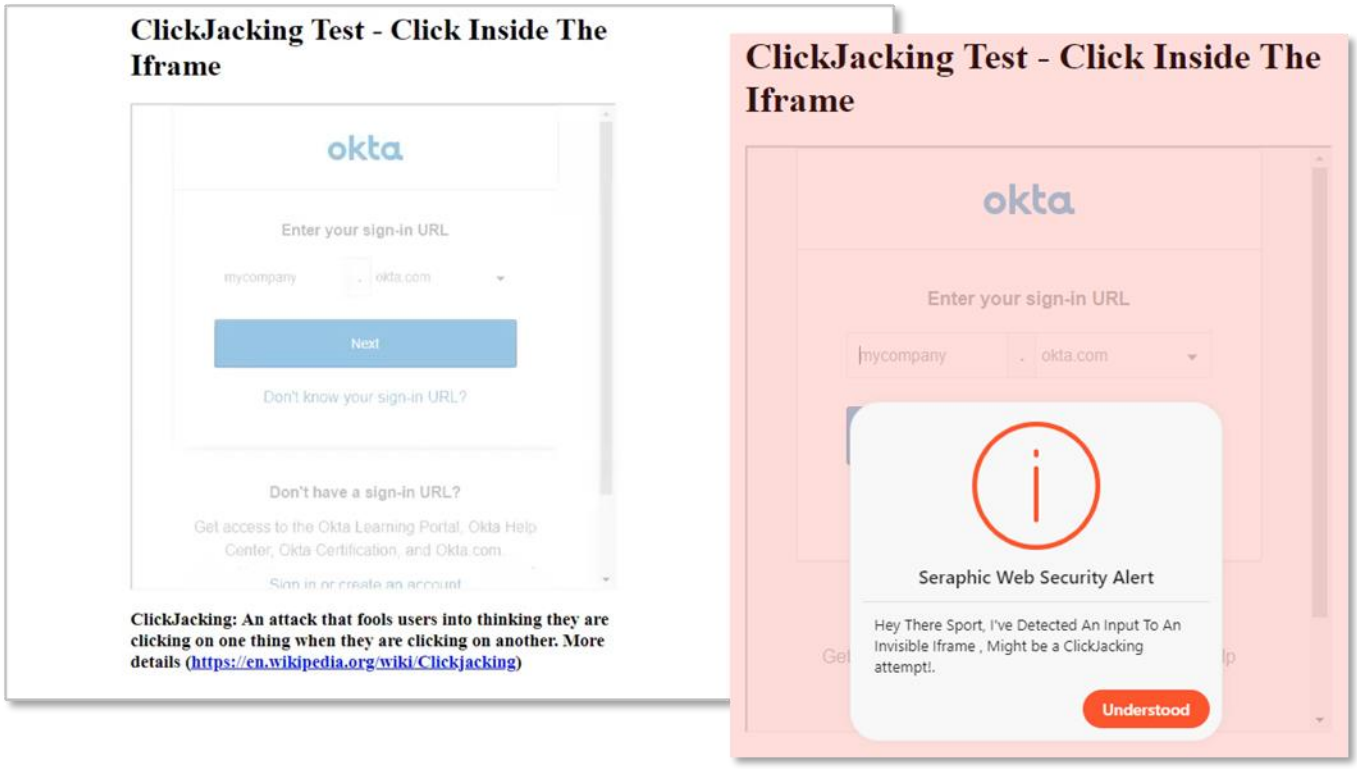
Two examples observed by ESG are clickjacking and browser-in-the-browser (BiTB) attacks.

Clickjacking occurs when an attacker fools a user into thinking they are clicking one thing when they are clicking something else. The UI is manipulated in a way that hides malicious intent behind legitimate UI controls. For example, showing a form or button to the user that in turn sends their information to a malicious site or authorizes an unwanted transaction.

ESG observed a clickjacking attack where a sign in form was shown to the user that they may see often in their daily work, such as for an identity provider. However, an invisible iframe is present so when they fill in the form, their credentials will be sent to a malicious site to be recorded and then used or sold on the dark web.

ESG validated that Seraphic detected this attack, and when the user clicked inside the form, the action was stopped and a pop-up message appeared,[4] warning the user that a clickjacking attack has been detected and preventing them from entering any data (see Figure 4).

Figure 4. Seraphic Blocks a Clickjacking Attempt



Source: ESG, a division of TechTarget, Inc.

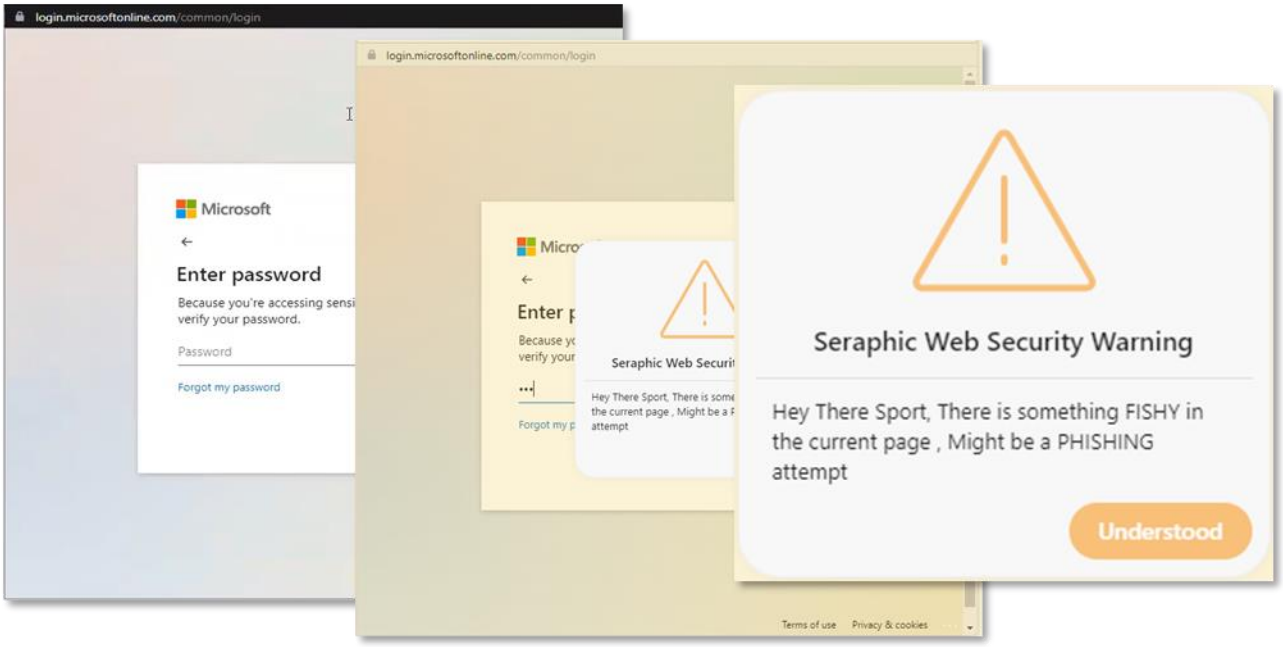
A BiTB attack consists of using JavaScript to simulate a browser window within the browser and spoofing a legitimate domain. It takes advantage of the commonly seen "Sign in with" buttons that allow users to use credentials from sites like Facebook or Google to sign into third-party services. However, if the user visits a malicious website, perhaps sent to them in a phishing email, they could be presented such a login form that looks real, including a legitimate URL, but is trying to steal their credentials.

ESG observed this type of attack being blocked by Seraphic (see Figure 5). The page presents what appears to be a Microsoft page asking for a password—something seen on an almost daily basis by many modern employees. However, this is a phishing attempt to steal user credentials. When the employee clicks into the password box and begins typing, a message appears warning the user that this is a phishing page. Seraphic won't allow the user to enter any text into this page, protecting them and the organization from a potential data breach.

This is again a Seraphic just-in-time intervention approach since the page isn't blocked completely; Only the input events are terminated so the user can still navigate through to the page but without the risk of data leak.

[4] Administrators can control the text for pop-up messages via the Seraphic Admin Console.

Figure 5. Seraphic Blocks a Browser-in-the-browser Attack



Source: ESG, a division of TechTarget, Inc.

Why This Matters

According to ESG research, social engineering attacks are the factor most cited by organizations as the biggest contributor to security events that they have experienced over the past two years.[5] Employees are under attack from skilled criminals who work day and night to find ways of tricking users into giving up their data.

Seraphic protects employees with its exploit prevention engine and powerful detection capabilities that block phishing attacks, browser exploitation attacks, and other common tools used by criminals to gain access to enterprise data. Employees can browse the web and perform their work free from the fear of becoming a cyber-criminal's next victim.

The organization benefits by preventing zero-day exploits, data theft, ransomware attacks, phishing, and other common browser-based attacks that can cost the company millions of dollars. In addition, Seraphic can do the work of several individual tools, providing savings in cost and complexity.

Seamless User Experience

Browser isolation, a common technique used to protect employees as they browse the web, comes at a high price. It executes webpage code away from the user and then delivers the result to the employee's browser. This solution is expensive and resource-intensive. Cloud providers charge for processing time used to render pages and protect users. Also, companies must make sure that enough bandwidth is available to support the connections of all employees. In addition, the end-user experience is diminished due to the extra time it takes to process webpage code on a distant server before getting to the user.

[5] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

Some organizations use dedicated enterprise browsers or custom browsers designed to be more secure. However, this approach forces user migration to an unfamiliar browser, obliging them to learn new ways of working and potentially damaging productivity.

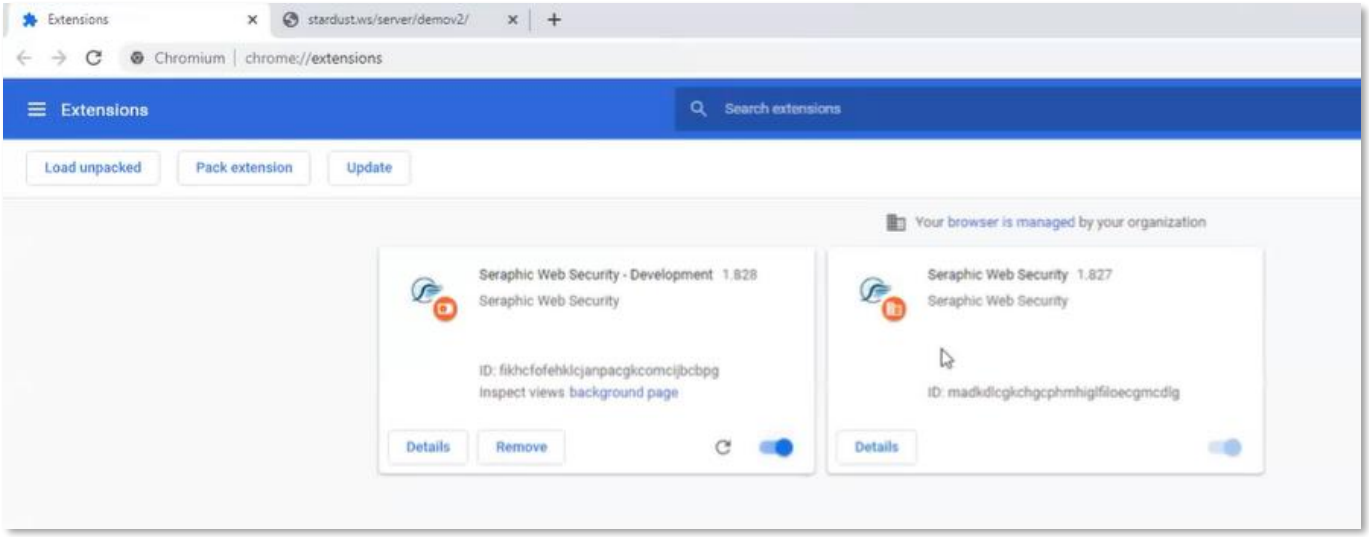
Seraphic's User Experience

ESG validated Seraphic's approach to protecting end-users and its effect on user experience. Seraphic's agent doesn't send data to a distant server. Instead, its detection engine uses real time execution telemetry to monitor page behavior in real time and reacts accordingly to accurately block common browser-based attacks. The exploit prevention engine isn't based on any detection techniques and prevents malicious code from successfully exploiting the browser.

From the user's perspective, nothing's changed. The organization deploys Seraphic agents to employee devices, along with a browser extension (such as the one depicted in Figure 6). The employee uses the same browser tomorrow that they did today, only with Seraphic running in the background to protect them from attack. There are no performance lags or external services required, even for DLP.

Seraphic's deployment is frictionless and scalable. Deploying to ten devices or 10,000 devices doesn't drastically change deployment times. Organizations of all sizes can deploy Seraphic quickly to all employee devices.

Figure 6. Seraphic Chrome Extension



Source: ESG, a division of TechTarget, Inc.

Why This Matters

Cybersecurity is a critical part of doing business online today. However, the increasing cost and complexity of security solutions drains companies of valuable resources that would otherwise be used to generate revenue. Techniques such as browser isolation are extreme and degrade performance and user experience.

Seraphic does its work without interfering with the end-user experience. The same browser used today will be used tomorrow. Seraphic allows organizations to protect their users and data without depending on custom browsers, proxies, remote browser isolation (RBI), external feeds, signatures, or patches. Employees will browse the web with confidence and speed while still protected by Seraphic.

Compliance and Policy Enforcement

ESG observed the strong compliance and policy enforcement Seraphic enables. Seraphic scales compliance to all users, enforcing rules set by system administrators to protect company data. It features a robust administration console used to define fine-grained policies and data loss prevention (DLP).

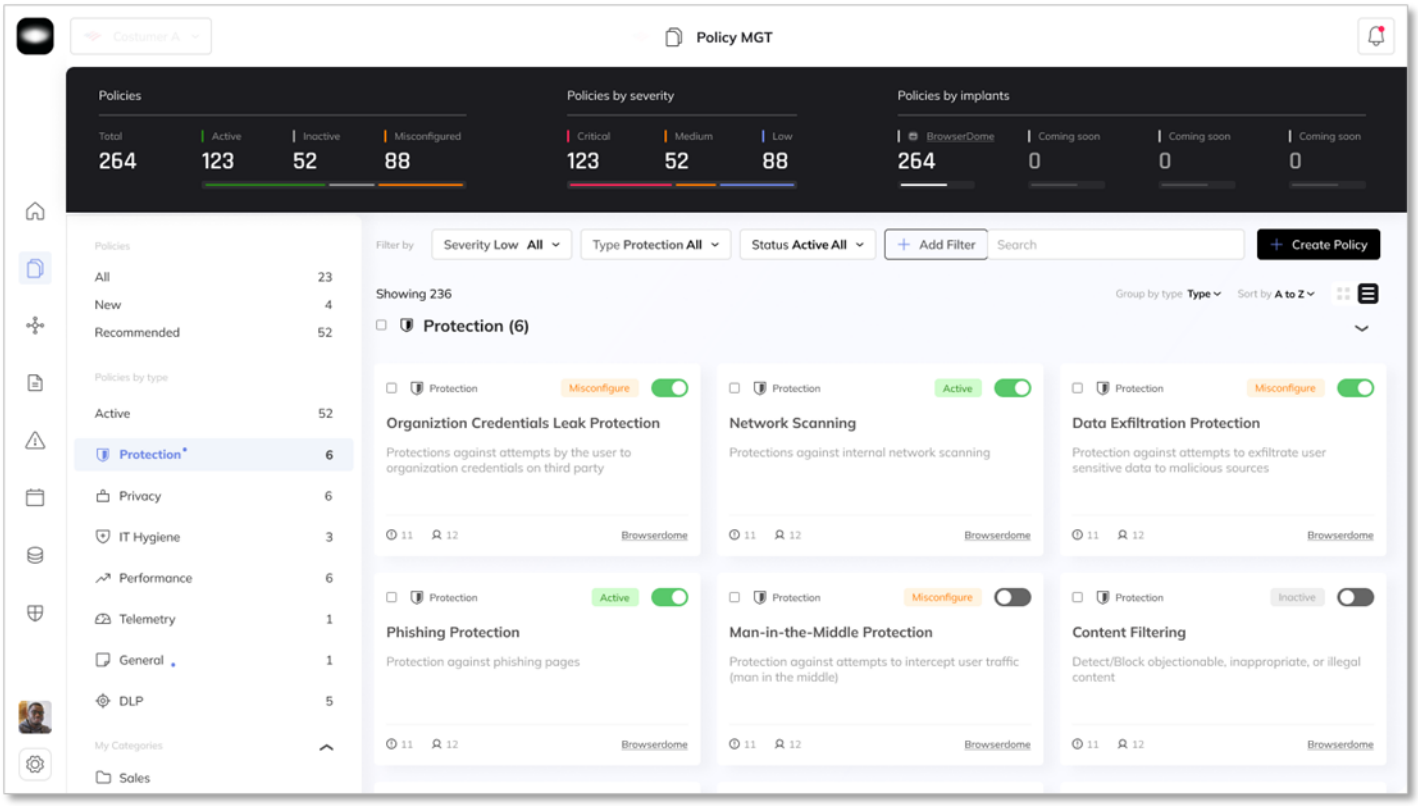
Seraphic Admin Console

The Seraphic Admin Console gives administrators the ability to define fine-grained policies for end-users. As shown in Figure 7, many options exist, including:

- Data Exfiltration Protection.
- Credential re-use Protection.
- Man in the Middle Protection.
- Phishing Protection.
- Content Filtering.

Seraphic's Admin Console provides a host of options based on the main categories of Protection, Privacy, IT Hygiene, Performance, and DLP.

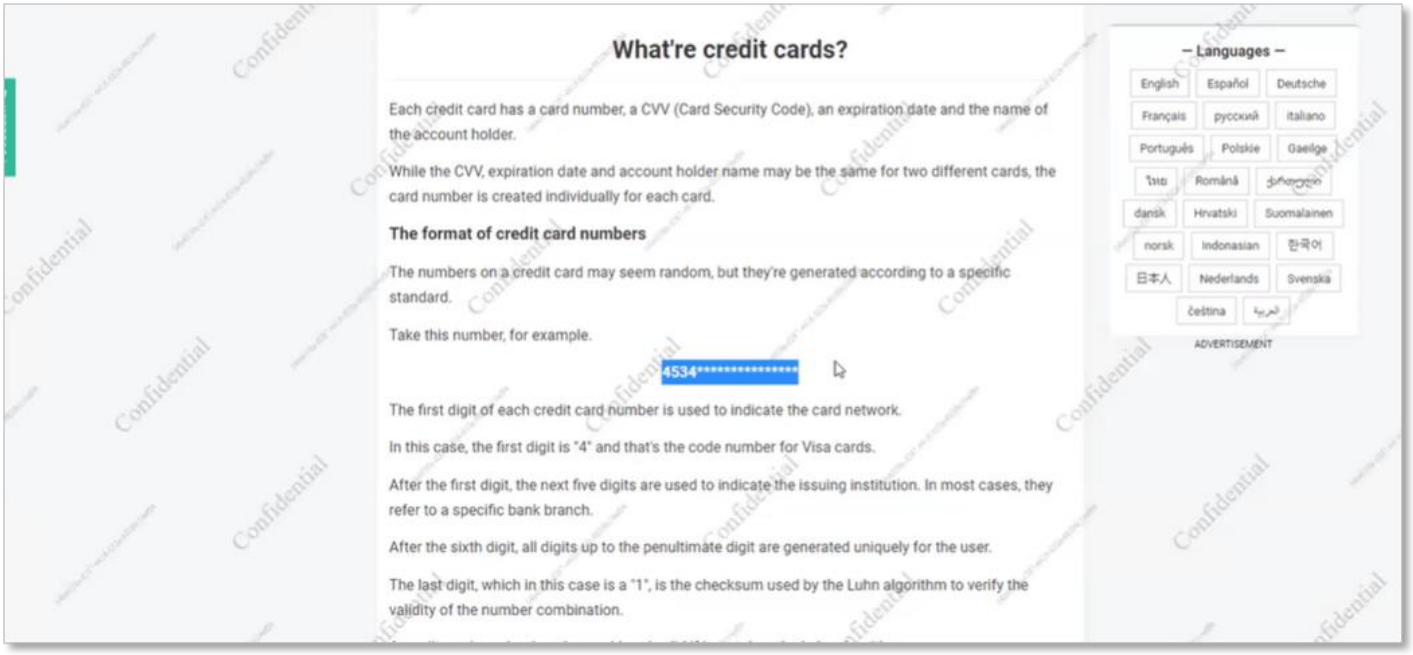
Figure 7. Seraphic Admin Console



Source: ESG, a division of TechTarget, Inc.

ESG validated Seraphic's DLP features. Figure 8 shows a sensitive page as viewed through a browser with Seraphic enabled. The watermark has the agent's unique ID within it. Therefore, if this page or an image of it were to appear on the internet or in discovery for a legal action, organizations will know exactly which employee may have leaked the information. Also, the credit card data on this page is masked automatically by Seraphic. This technique protects sensitive data from over-the-shoulder leakage or screenshots used to leak information.

Figure 8. Seraphic Data Loss Prevention



Source: ESG, a division of TechTarget, Inc.

Why This Matters

35% of organizations use tools from more than ten security vendors,[6] such as those used to protect browsers from cyber-attacks and those used to enforce policies and compliance. Every new tool increases complexity and cost.

ESG validated that Seraphic's technology used to protect against cyber-attacks provides policy enforcement, controlling how users interact with the web on company devices. The admin console is straightforward and powerful, making it possible to prevent cyber-attacks and enforce compliance at the same time. Multiple tools can now be rolled into one—Seraphic.

[6] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

The Bigger Truth

The web browser is a common attack vector, and the wrong link or visited page can compromise a browser and the entire machine. More than half of organizations say end-users falling victim to social engineering (phishing, malicious links, etc.) is one of the biggest contributing factors to security events.[7] Employees are under attack from skilled criminals who work day and night to find ways of tricking users into giving up their data.

ESG validated that Seraphic protects employees with its exploit prevention engine and powerful detection capabilities that block phishing attacks, browser exploitation attacks, and other common tools used by criminals to gain access to enterprise data. Seraphic deploys an abstraction layer to create a non-deterministic (i.e., unpredictable) environment inside any browser. Malicious code can execute, but it just doesn't work. Meanwhile, Seraphic doesn't interfere with normal operations in any way, and there is no performance impact.

Seraphic also demonstrated strong policy enforcement, enabling compliance and data loss prevention. Administrators have fine-grained control over what users can and can't do while navigating the web, protecting both the user and the company's data. Administrators can deploy Seraphic to all devices. Seraphic supports mobile users today in Safari on iOS and Firefox on Android. ESG believes that adding native application support on mobile devices would be a welcome enhancement.

If your organization is looking to stop browser-based cyber-attacks across the enterprise while maintaining compliance, all without impacting performance or employee experience, then ESG believes that you should consider the benefits of protecting your browsers with Seraphic.

 www.esg-global.com  contact@esg-global.com  508.482.0188

[7] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.