

F R O S T & S U L L I V A N

2024 ENABLING TECHNOLOGY LEADER

*IN THE GLOBAL
ZERO TRUST BROWSER
SECURITY INDUSTRY*

F R O S T & S U L L I V A N

BEST
2024 PRACTICES
AWARD



Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Seraphic Security excels in many of the criteria in the global zero trust browser security market.

AWARD CRITERIA	
<i>Technology Leverage</i>	<i>Customer Impact</i>
Commitment to Innovation	Price/Performance Value
Commitment to Creativity	Customer Purchase Experience
Stage Gate Efficiency	Customer Ownership Experience
Commercialization Success	Customer Service Experience
Application Diversity	Brand Equity

The Need for a Browser-agnostic ZTBS Solution

Enterprises increasingly deal with a hybrid workforce, including employees working from home, cafes, or the airport. Thus, employees will inevitably connect to risky Wi-Fi networks or access corporate applications from unsecured devices. Enterprises find it challenging to restrict employees to operate within the virtual security perimeter.

The growing transition to software-as-a-service (SaaS) applications, easily accessible from a browser, drives employees to work primarily out of a browser. Thus, the browser provides a vast attack surface for an initial foothold for cyber adversaries. In fact, web browsing is the most common method for delivering ransomware.

At the same time, securing the browser is a challenging task. Traditional security tools that use isolation-based approaches, such as VDI, VPN, and DaaS, suffer from clunky user interfaces and inefficient workflows. While enterprises deploy many tools around the browser, the browser itself remains a weak spot.

Zero trust browser security (ZTBS) solutions focus on securing the browser without interrupting user workflow and productivity. ZTBS solutions leverage zero trust policies at the authentication layer to protect against malware and prevent data leakage.

Some ZTBS market approaches suffer compatibility limitations with existing browsers or operating systems. However, the most efficient approach to ZTBS must be a browser-agnostic tool that functions, irrespective of the browser type, version, OS, or the existing security architecture of the company.

Seraphic Security – A Unique Approach to ZTBS

Seraphic Security is a browser agnostic ZTBS solution that provides DLP, governance, security, and connectivity to turn any browser into a centrally secured and managed enterprise browser. The core technology of Seraphic security is a browser agent deployed by an extension, dedicated browser, or a proxy.

A management console brings together Seraphic Security's Agent (deployed through one of the methods noted above) for security analysts. Seraphic extension, dedicated browser, or a proxy all communicate with the Seraphic cloud backend. In addition, the architecture has an enforcement proxy to enforce usage policies and to the ability to connect to remote networks without VPN or VDI. The platform delivers robust security and governance to all browsers while preserving the native experience for the end users.

Typically, in a web browser, a JavaScript engine renders the incoming code from a website. The Seraphic Security browser extension injects its own lightweight JavaScript code into the browser by embedding it and creating an abstraction layer. This abstraction layer provides visibility into the rendering code and end-user activity, allowing security teams to control the security parameters of the browsing session.

Superior Prevention and Detection Architecture

Seraphic Security's prevention engine prevents zero-day and unpatched n-day vulnerabilities based on chaotic manipulation. The platform leverages a patented moving target defense approach, which breaks predictability for cyber adversaries exploiting vulnerabilities. Therefore, security teams can stop all exploits on all browsers, whether zero-day or known vulnerabilities.

Seraphic Security's browser extension includes a detection engine that detects many browser-based attacks, including social engineering and cross-site scripting attacks. Many solutions rely on threat intelligence feeds to detect phishing attacks. However, the lifespan of a phish is too short, making threat intelligence feeds outdated and irrelevant. Seraphic Security uses a real-time contextual engine to determine phishing attacks based on user telemetry and web page data. While the agent does not stop the user from browsing a potentially malicious web page, the platform prevents users from performing malicious or risky actions like typing their credentials on the site. This just-in-time protection reduces the false positives rate and preserves user productivity.

“Seraphic Security protects SaaS applications running on the web browser and as a native application on the endpoint. Existing as a JavaScript agent that can run on electron-based applications (also known as hidden browsers) allows Seraphic Security to extend the security capabilities from the browser to the application.”

***- Swetha Krishnamoorthi
Senior Industry Analyst, Cybersecurity***

Seraphic Security's policy engine allows security teams to define DLP policies at a granular level. Security teams can specify the exact scenarios of what is restricted or allowed for users. Lastly, the management engine of Seraphic Security's platform enables security teams to manage all browser aspects, including third-party extension management. Security teams can block, allow, or restrict the usage of third-party extensions based on enterprise risk appetite.

Comprehensive Use Case Coverage

Seraphic Security also offers zero trust private access (ZTPA) capabilities for internally hosted applications with its smart connector. Users logging in from remote networks can utilize Seraphic Cloud and connector to get access to internally hosted applications. The Seraphic ZTPA works in two ways:

1. Direct access, wherein Seraphic reroutes the traffic to the application after the user enters the address.
2. Application portal, wherein the platform allows secure application access after authentication based on the user profile, without any installation on the personal device.

Seraphic Security's ZTPA empowers enterprises to address security risks from BYOD use cases and third-party contractors to overcome user experience (UX) issues that are common with VPN or VDI applications.

Seraphic Security protects SaaS applications running on the web browser and as a native application on the endpoint. Existing as a JavaScript agent that can run on electron-based applications (also known as

"In 2023, the company released a Seraphic-embedded browser for unmanaged devices, a Seraphic electron agent for collaboration and productivity tools, Seraphic Mobile for Android and iPhone, and a Seraphic transparent proxy for preventing access to the browser without Seraphic. Seraphic Security has secured four patents covering the unique technologies underlying its architecture."

- Swetha Krishnamoorthi
Senior Industry Analyst, Cybersecurity

hidden browsers) allows Seraphic Security to extend the security, DLP, and governance capabilities from the browser to the application.

With unmanaged devices, Seraphic separates the personal and corporate profiles of the end user. Any user profile activity on an unmanaged device does not come under Seraphic's monitoring and security controls, thereby protecting user privacy. However, when the user logs into the corporate profile or accesses corporate applications from the unmanaged endpoint, the security team can enforce policies to use a designated browser (which can be any mainstream browser the user would like to use) with

Seraphic embedded in it. Thus, the enterprise can prevent data leakage to personal devices or applications.

An Agile, Customer-aligned Innovation Process

Seraphic Security has a robust innovation process that aligns with market trends and customer pain points. The company uses an agile development framework to measure R&D progress against the product roadmap. Seraphic Security uses an advanced analytics tool, a product analytics and error-tracking platform, to measure the effectiveness of new features.

Seraphic utilizes a gradual development process in which the company initially explores the value of a feature with design partners, moves to beta customers, and then finally deploys innovative solutions on a large scale. This gradual process allows the company to bring new technology to the market at scale while maintaining high customer satisfaction.

In 2023, the company released a Seraphic-embedded browser for unmanaged devices, a Seraphic electron agent for collaboration and productivity tools, Seraphic Mobile for Android and iPhone, and a Seraphic transparent proxy for preventing access to the browser without Seraphic. Seraphic Security has secured four patents covering the unique technologies underlying its architecture. The company has an additional 17 patents under different stages of the application process.

Strategic Marketing & Customer Acquisition Powers Growth

California-based Seraphic Security provides enterprise class security capabilities that replace SSE core capabilities and complement “adjacent” security technologies such as EDR. Seraphic has segmented its customer persona into three types.

1. **Large enterprises that have deployed SSE / SASE:** Seraphic complements the capability of SSE via their defense-in-depth security architecture.
2. **Enterprises with EDR but no SSE / SASE:** Seraphic provides DLP, governance, and security without the need to implement SSE.
3. **Enterprises looking for RBI alternatives:** Seraphic provides a lower-cost solution and a simpler architecture that provides a better user experience.

Seraphic Security has partnered with channel partners in the European Union and the United States to strengthen its footprint. Moreover, the company plans to partner with MSPs to release the “Super Admin Console” in 2024.

Such targeted marketing and customer acquisition efforts have helped the company acquire over 60 customers within two years of its launch, translating to a triple-digit YoY growth rate. Seraphic Security holds a growing market share in the secure browser extension market in 2023, according to Frost & Sullivan research.

Conclusion

The growing volume of hybrid workforce, transition to SaaS applications, and increasing frequency of web-based attacks call for a modern approach to browser security. Traditional solutions primarily use an isolation-based approach, which can negatively impact employee productivity by disrupting workflow. ZTBS solutions leverage the zero trust framework to extend security to the browser while ensuring a smooth user experience.

Seraphic Security’s browser-agnostic agent allows security teams to granularly enforce DLP policies and prevent users from inputting data on malicious web pages. In addition, the company extends the browser security capabilities to native SaaS applications on the endpoint, leveraging JavaScript code. Moreover, the Seraphic Security browser extension allows enterprises to replace VDI or VPN with its zero-trust private access use case. The platform can also provide secure access to corporate applications from unmanaged devices without impacting user privacy.

Seraphic Security earns Frost & Sullivan’s 2024 Global Enabling Technology Leadership Award for its strong overall performance in the ZTBS market.

What You Need to Know about the Enabling Technology Leadership Recognition

Frost & Sullivan's Enabling Technology Leadership Award recognizes the company that applies its technology in new ways to improve existing products and services and elevate the customer experience.

Best Practices Award Analysis

For the Enabling Technology Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at <http://www.frost.com>.

The Growth Pipeline Engine™

Frost & Sullivan’s proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

[Learn more.](#)

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- **Mega Trend (MT)**
- **Business Model (BM)**
- **Technology (TE)**
- **Industries (IN)**
- **Customer (CU)**
- **Geographies (GE)**

