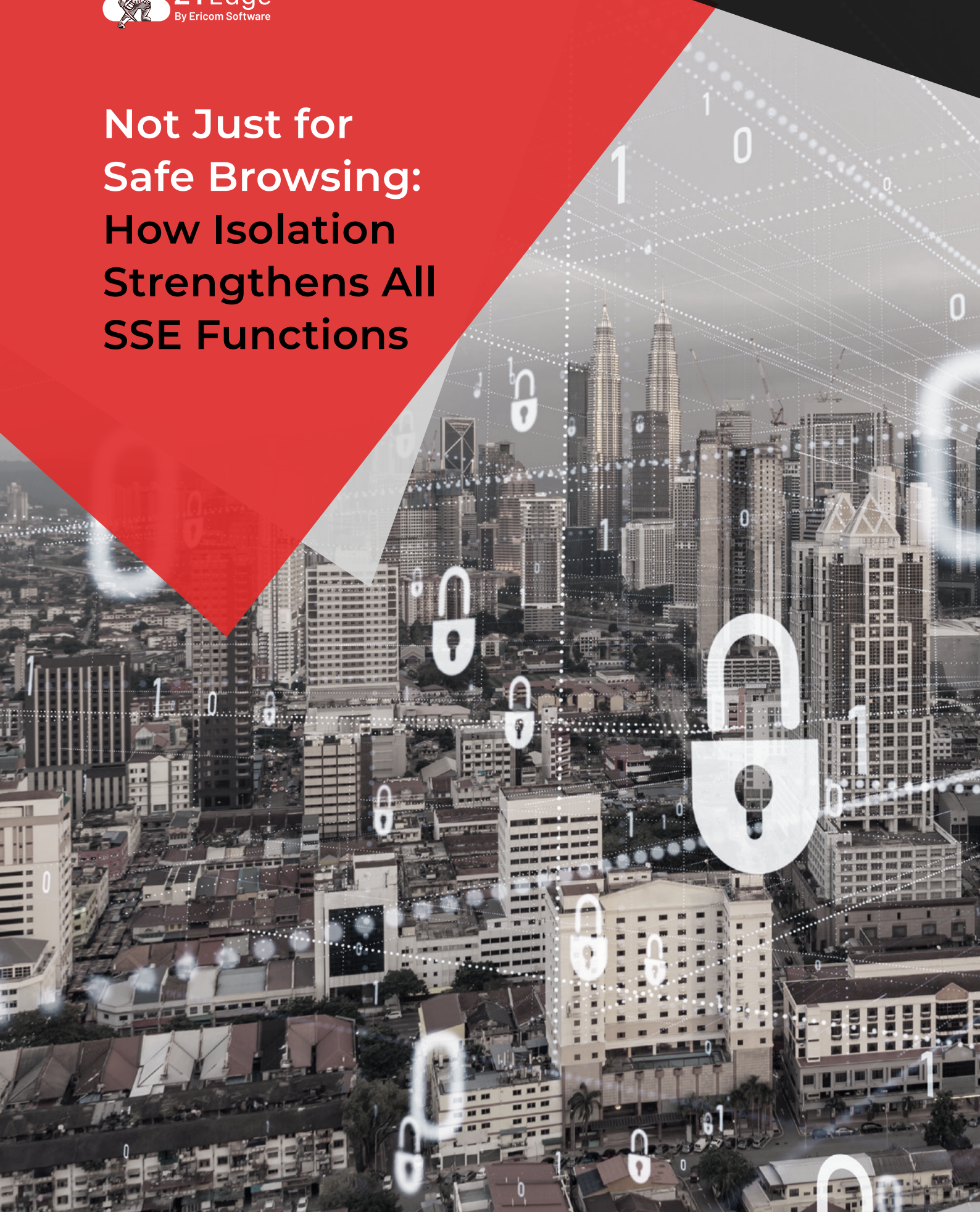
ZTEdge™
By Ericom Software

Not Just for Safe Browsing: How Isolation Strengthens All SSE Functions



Contents

ZTEdge™
By Ericom Software

Web Isolation at the SASE Core

In 2009, to protect thousands of desktops used by people doing sensitive nuclear research, the US federal government began to airgap them from the internet. “Remote managed hosted virtualization,” opened websites on a “remote” server, with only site images streamed to the desktops the researchers used.

Nearly a decade later in 2018, the Defense Information Security Agency (DISA) began promoting the concept of using cloud-based internet isolation to enable secure browsing for the many defense department users. By then, remote browser isolation (RBI) had progressed well beyond earlier techniques, leveraging purpose-built technologies that were lightyears ahead of virtualization. While cloud-based RBI was still not quite ready for prime time, a number of solutions were beginning to pull ahead of the pack in the race to the cloud.

That same year, Gartner released a report on browser isolation that warned enterprises to not assume that the traditional “detect and respond” approach to malware could keep them safe from all – or even most – threats. Neil MacDonald, the analyst who authored the report, named remote browser isolation as an ideal way to reduce the exposure of internet-facing attack surfaces — that is, endpoint browsers.

Early on, Ericom recognized RBI’s strength as a Zero Trust solution for securing endpoints from the impossible-to-verify-as-safe web. With prescient timing, we began developing an RBI solution well before 2018 and were among the first to provide a cloud-based solution. And as such, we were also among the first to grasp that cloud-based web isolation technologies, when properly designed, can be leveraged to protect "internet-facing attack surfaces" that extend well beyond isolating browsers that Neil MacDonald had in mind from web-borne malware.

First, the attack surfaces that isolation can protect include web applications, SaaS and collaboration sites, private apps and the data they all contain, as well as browsers. And second, combining isolation with a policy engine enables flexible, granular controls that are essential for securing user access and activity in today’s cloud-enabled work-from-anywhere-on-any-device work environment, and restricting them in accordance with Zero Trust least-privilege access principles.

As pioneering developers of the most sophisticated web isolation solutions on the market, we were pleased to see that in its 2022 Strategic Roadmap for SASE Convergence, Gartner revised its earlier characterization of RBI as a “recommended” component of Secure Access Service Edge (SASE) implementations, and now considers it a “core” capability. Quite frankly, we were surprised that it was not included from day one.

Cloud-based isolation technologies, when properly designed, can be leveraged for critical applications that extend well beyond isolating browsers from web-borne malware.

As the report notes, the re-positioning of isolation to a core SASE capability was because it “has become widespread for certain key use cases.” And while the report does not provide additional detail what those use cases are, our role in the industry gives us a unique view into where enterprises are using isolation-based approaches in their SASE deployments to improve security outcomes and enhance their users' experiences.

In this white paper, we present the core components of Security Services Edge (SSE)/SASE and discuss how, beyond traditional browser isolation being included in their ranks, web isolation adds important secure access capabilities to those components. We also recommend key features and capabilities to seek in an RBI/isolation implementation.

A Note About SASE vs SSE

SASE and SSE are related, but not identical, constructs. Security Services Edge (SSE) is a Gartner-developed concept that defines a set of network, cloud, and application access security controls that are based on a Zero Trust approach to network security. In place of the older perimeter-based approach to cybersecurity, SSE can be used to enforce security policies that treat not only every user but all network traffic as potentially hazardous.

The Secure Access Service Edge (SASE) concept was also developed by Gartner as a networking paradigm that converges the security controls of SSE with network connectivity, typically with software-defined wide area networks (SD-WANs) as part of the mix. SASE provides a cloud native service that combines security with the cloud-based network architecture.

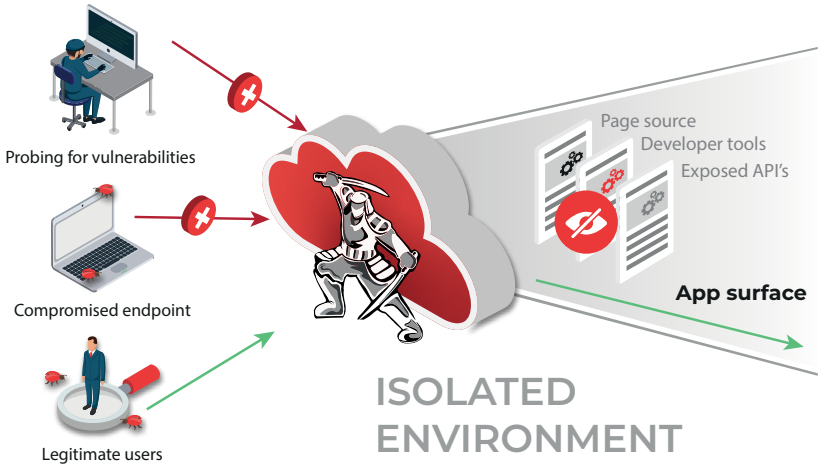
The migration to SASE/SSE is driven by the convergence of a number of trends: Adoption of a Zero Trust approach to network security, Covid-accelerated growth in remote work, increasing outsourcing, and especially, the move to the cloud. Together, these trends have buried perimeter-based approaches and left organizations more vulnerable to internet-delivered attacks. For instance, in cloud-based perimeter-less architectures, no SWG can verify that a website is threat-free since a zero-day exploit or unknown software vulnerability might enable malware infection.

Core Components of SSE – and Why Web Isolation Makes Them Better

As developers of ZTEdge, a comprehensive isolation-based SASE platform, we understood early on that web isolation enables uniquely rigorous application of Zero Trust security principles such as "least privilege access" and "assume breach." As a result, web isolation adds vital protection against threats that other SASE elements simply cannot. That's why we chose to implement web isolation as a central technology of our SASE platform long before Gartner added RBI protections to its list of "core" SASE components.

Web isolation enables rigorous cloud-based enforcement of Zero Trust security principles such as "least privilege access," "never trust, always verify" and "assume breach." As a result, it adds vital capabilities that strengthen other SASE functions.

In the context of web and email security, RBI protects against malware by isolating browsing in evanescent cloud-based containers. If a user clicks on a bad link in an email or website, malware remains in the isolated container and never reaches the endpoint. In addition, policy-based controls limit which sites users can access as well as what actions they can take on a site. For instance, new or uncatalogued sites may be opened in read-only mode to protect against credential theft.



Web isolation also provides robust protections for corporate web applications, and SaaS applications and private apps, as well as data that can be accessed via theses apps. By routing application access via cloud-based isolation, app surfaces are protected from malware on users' unmanaged devices and cloaked from view of threat actors seeking vulnerabilities to exploit. In addition, policy-based restrictions can be enforced to restrict access and prevent breaches, data exposure and compliance risk.

According to Gartner, the following components are "core" to SASE/SSE implementations. Integrating isolation strengthens every one of them.

SWG (Secure Web Gateway)

Located between the user and the internet, SWGs enforce web access policies and include antivirus as well as malware and ransomware detection/prevention. Initially delivered as on-premises devices, SWGs are increasingly deployed as cloud-based software solutions.

How Web Isolation Makes SWGs Better: SWGs operate on a detect-to-protect model. As a result, zero-day exploits, malware with unknown signatures, and phishing sites that have not yet been categorized as malicious can easily slip past.

Since RBI keeps all web content off endpoints, adding RBI to the SWG stops new malware and exploits from reaching users' browsers. And with policy-based controls, as-yet uncategorized sites can be opened in read-only mode to prevent credential theft. Finally, unlike SWGs which cannot "see" into end-to-end encrypted content like instant messenger chats (such as WhatsApp Web), RBI can scan that traffic to block malware and stop data exfiltration with Data Loss Prevention tools.

CASB (Cloud Access Security Broker)

CASB enables organizations to enforce security policies for users accessing cloud-based resources in much the same way they do for local, on-premises data, by mediating between users and cloud service providers. CASBs typically comprise filters, a firewall, and a proxy/reverse proxy.

How Web Isolation Makes CASB Better: Web isolation enables granular, policy-based control of user activity and interactions with SaaS apps and the data they contain, including web meeting solutions like Zoom and Microsoft Teams and collaboration platforms such as O365. It protects apps from malware that might be present on employees' BYOD or 3rd party users' unmanaged devices and delivers key data sharing controls and data loss prevention capabilities.

At Ericom Software, we call this use of web isolation "Web Application Isolation" (WAI). Unlike CASBs that require the use of complicated and brittle reverse proxies to support application access for BYOD and unmanaged devices, WAI is clientless and uses cloud-based controls to secure unmanaged device access to all web and cloud apps.

ZTNA (Zero Trust Network Access)

ZTNA is a secure way for remote users to access internal networks, without the risks associated with VPNs. ZTNA applies least privilege policies, in conjunction with microsegmentation, to limit user access to only the resources required for their work.

How Web Isolation Makes ZTNA Better: Connecting users to private corporate apps is another case in which Web Application Isolation simplifies and secures user access, even from unmanaged devices. Similar to the way that WAI enhances CASB with more granular control and secure access from unmanaged devices to SaaS apps, ZTNA that leverages WAI enables granular policy-based control of user activity and interactions with internal apps, data and other resources, **without any on-device agents or software required.**

Resources are cloaked from view, restricting the reach of threat actors should a breach occur. Robust data sharing controls, as well as the use of DLP and CDR for traffic scanning, are also part of the solution.

CDR (Content Disarm and Reconstruct)

CDR protects endpoints and networks from malware embedded in documents, images and other files, enabling users to safely download email attachments and files from websites..

How Web Isolation Makes CDR Better: Leveraging CDR within the isolated cloud-based container protects endpoints and networks from zero-day threats and other new malware that may not yet be identified by detection-based solutions. Critically, with web isolation, CDR can be applied to content within end-to-end encrypted traffic to, for instance, protect users from weaponized files sent via WhatsApp. In a similar manner, web isolation enables DLP to be applied to end-to-end encrypted interactions, ensuring that no PII or other confidential or regulated data is exposed.

Is “RBI Inside” Enough?

RBI is now considered to be a core component of SSE, but important questions remain about which RBI offering organizations should choose. It is important, as well, to investigate whether web isolation supports platform services beyond RBI. The degree to which isolation is integrated across services varies widely among SSE platforms.

Ericom Software RBI, which is deployed as a core component of the company’s ZTEdge platform, integrates several key capabilities that are essential in today’s hybrid workplace but which other RBI products lack, such as the ability to isolate virtual meetings to prevent data exposure and malware attacks. Ericom RBI's ZTEdge also blocks malware hidden in encrypted traffic such as instant messaging apps like WhatsApp and Telegram.

Through tight integration of cloud-based web isolation with ZTNA, ZTEdge clientless Web Application Isolation can protect web and cloud applications from malware on unmanaged devices in ways that other ZTNA, CASB, and web application firewall (WAF) solutions simply cannot. WAI prevents over-privileged access from 3rd party and users’ BYOD devices without installing any dedicated clients or software on the devices and without requiring use of special browsers or tools.

ZTEdge RBI

- Protects endpoints from phishing, ransomware and other web-based threats
- Isolates virtual meetings to prevent data exposure and malware attacks
- Blocks malware hidden in encrypted traffic like WhatsApp and Telegram

ZTEdge Clientless ZTNA (Web Application Isolation)

- Protects web applications and SaaS apps from malware on unmanaged devices
- Cloaks app surfaces against reconnaissance and port scanning
- Prevents data loss and exposure
- Blocks credential theft

Conclusion

With Gartner estimating that 80% of enterprises will have adopted cloud-based SASE/SSE by 2025, SASE/SSE architecture is clearly the wave of the future. Due to the delay in including RBI as a core component of SASE/SSE implementations, however, many platforms fail to fully leverage the protections it offers, often because their platform's web isolation technologies are not performant and robust enough, or sufficiently well-integrated, to handle the multiple key use cases discussed above.

As pioneers in the web isolation space, Ericom Software built its SSE platform around one of the most scalable, efficient, and performant cloud web isolation technologies in the world. The market is now validating the wisdom of that approach. For more details about how to choose the right RBI for your organization, see "Critical Questions to Ask RBI Vendors."

Contact us for a demo to see how it works!

Request a demo

www.zerotrustedge.com
info@zerotrustedge.com
US: (201) 767-2210
Europe: +44 (0) 1905 777970
ROW: +972-2-591-1700