Brought to you by Informa Tech

Publication date:
15 Jun 2023

Author:
Rik Turner, Senior Principal Analyst

On the Radar: Red Access injects security into browsing

Summary

Catalyst

Protecting the browsing activities of enterprise users is a growing security challenge that has been addressed in a number of ways: filtering, isolation, extensions, and dedicated secure browsers, aka “enterprise” browsers. Red Access Agentless Browsing Security Platform takes a browser-independent, agentless approach that combines server and endpoint analysis using a proxy with what the vendor terms a “security environment” dynamically injected into each web session.

Omdia view

Remote and hybrid working has increased with the growth of the internet, and then burgeoned dramatically as a result of the changes to work patterns caused by the COVID-19 pandemic. The highly distributed enterprise IT environment must deal with securing data, access, and devices across cloud-based services, public networks, and personal as well as corporate devices.

This challenge is increased as enterprise software makes ever more use of the dynamic flexibility of web-based applications and services. Not only are web browsers themselves used by individuals to surf for information, but they are also the portals used to deliver dynamic enterprise content and services, and browsing capabilities are even added into other applications to facilitate information access.

While the user, device, and network may have security in place, threats can be delivered through web sessions into the browser itself in what are often termed “client-side” attacks, distinguishing them from attacks on the server side, where a more mature security stack is usually in place. The impact of such attacks can be offset or deflected by remotely or locally isolating malicious actions or defended against by securing the browser or its activities.

Why put Red Access on your radar?

Browsers are not only powerful flexible tools in their own right, but browsing technologies and protocols are incorporated into other software. Red Access addresses the security, not just in a browser application but in browsing generally, such as other applications that embed the use of HTTP/S. It does this through an agentless cloud-based service that combines analysis of web traffic with the injection of a security environment into each web session.

Market context

The enterprise browser market is an emerging segment that recognizes the browser as a key vehicle to protect an organization's resources within its applications, while also ensuring users can operate safely. The case for such an approach has grown as corporate employees spend so much of their time on software-as-a-service (SaaS) platforms, or in the private apps written by organizations for their staff to access in infrastructure- or platform-as-a-service (IaaS or PaaS) environments.

In this scenario, the browser can become a vehicle for protecting critical apps and the corporate data that traverses them. It can also underpin paradigms such as hybrid work, contractors, and business process outsourcing (BPO), not forgetting bring-your-own-device (BYOD). And, of course, it can serve as defense against a burgeoning threat landscape.

Since all SaaS and private apps are accessed via a browser, being able to compromise that line of communication is invaluable for threat actors. Traditional consumer browsers were not developed with a security mindset, so they can inadvertently facilitate the delivery of ransomware and phishing. If attackers can infect the browser with a trojan, for instance, they can learn about the user's destinations on the internet and use that knowledge for a wide range of attacks, from theft of intellectual property to raids on online bank accounts. Such exploits are known as man-in-the-browser (MitB) attacks or boy-in-the-browser (BitB) attacks, where the malware changes a target machine's routing (often by altering an operating system's host file) then deletes itself.

Browser isolation

To address such challenges, there have been a range of responses from the security industry. The first came in the form of browser isolation technology, which places each browser session in a separate virtual machine that isolates it from the underlying infrastructure, including the machine's BIOS and operating system. Two flavors of this technology emerged:

- One carried out the isolation on the endpoint (so-called local browser isolation or LBI). This approach was championed by a vendor called Bromium, which is now part of laptop manufacturer HP. It had significant limitations at the time, however, because: (a) it was quite compute-intensive, taking CPU cycles away from the enterprise apps the user was working in; (b) the technology could only be deployed on more recent generations of x86 processors, so if the company had a mixed estate with older endpoints, Bromium was only a partial solution to its security problem.
- The other approach, called remote browser isolation (RBI), performed the same function on a server and presented a sanitized version of the web page to the endpoint. This approach was more popular because of the shortcomings of LBI outlined above. Several RBI vendors emerged,

and many were acquired; the best-known dedicated RBI vendor still in existence is Menlo Security.

It is worth mentioning in this context that neither of these approaches was designed to protect critical application usage or the underlying data. Rather, they were developed to protect enterprise users from bad actors that had compromised websites.

Changes to the browser

More recently, the focus has shifted to making changes to the actual browser and, here again, two distinct approaches have emerged:

- First, there are vendors that propose an extension to the existing browser, injecting extra intelligence in the form of lightweight JavaScript that enables the security and manageability that is missing from standard browser technology.
- The second approach is the development of a completely new browser. This “enterprise browser” can either live alongside the standard one on the endpoint and be used for all corporate activity, leaving the other one for the user’s personal browsing, or it can completely replace the standard browser and be used for all the browser activity from that machine.

Red Access takes a slightly different approach, which has a little in common with both browser isolation and extension, although, rather than the browser, the code or content is extended, and only for the duration of that session.

Product/service overview

The Red Access product is called Agentless Browsing Security Platform, and protects any desktop web app or SaaS app, as well as any browser on any device. It does not make use of an agent, browser isolation or extension, or a new browser, but instead uses a cloud-based proxy to do two things:

- Provide Secured Service Edge (SSE) capabilities: static analysis and filtering of any HTTP/S application or web session activities, including browser exploits, URL filtering, file scanning, data loss prevention (DLP), CASB, extension management, and phishing protection
- Inject JavaScript security into the incoming web application content to protect the session as it operates and to enforce advanced in-browser policy capabilities. It then disappears when the session is finished. Secure Web Session injects this security element into each session. This is not a browser extension but could be considered as dynamically extending the web application or content to protect itself, in a manner similar in concept to Runtime Application Self Protection (RASP). Red Access itself prefers to refer to this additional code as an “injected security environment.”

Secure Web Session’s protection is not limited to traditional standalone browsers, but also protects other HTTP/S sessions such as in-app browsing, or links clicked within a desktop application.

Company information

Background

Red Access was founded in 2021 by CEO Dor Zvi and CTO Tal Dery. Both founders served many years in the Israel Defense Forces' technology units and worked for several years at secure email gateway startup Solebit, before it was acquired by Mimecast, and then afterwards at Mimecast until they co-founded Red Access.

The company raised $6m in seed funding in January 2022, in a round led jointly by Elron Ventures and Ten Eleven Ventures. Red Access emerged from stealth in May 2022.

Current position

Red Access offers its Agentless Browsing Security Platform on a per-user, per-year subscription basis, with discounted tiers for volume and multi-year licensing options. The per-user subscription allows each user to have multiple devices.

In addition, the vendor offers a free trial of its technology, which can be accessed through its website.

Future plans

The cloud-based proxy has been developed internally to be compatible with the latest encryption protocols such as WebSocket, and the next step is to offer a reverse proxy, which Red Access indicates will be in the latter half of 2023. This release will improve performance, reliability, and user experience.

Key facts

Table 1: Data sheet: Red Access

Product/service name	Red Access Agentless Browsing Security Platform	**Product classification**	Browsing Security, Hybrid Work Security
Version number	1.4	**Release date**	May 24, 2022
Industries covered	All	**Geographies covered**	North America, Europe, and Middle East
Relevant company sizes	SMB, midsize, and enterprise	**Licensing options**	Subscription base (yearly per seat, multi-year licensing option)
URL	https://redaccess.io/	**Routes to market**	Direct sales and channel partners (MSPs/MSSPs, VARs, and technology partners)
Company	Tel Aviv, Israel	**Number of**	25

headquarters		employees	

Source: Omdia

Analyst comment

Red Access has taken a novel approach with the combination of static and dynamic inspection, protecting “browsing” not just “browser” activities, without requiring an agent or extension to the browser, or even a new browser. This means that security is added to any aspect of web browsing activity without the need to replace or extend existing software, benefiting users, IT management, and security teams alike.

While Omdia applauds the innovative approach, the challenge for Red Access will be in getting the message out in the face of a sector increasingly being termed as “enterprise browser” technology. In other words, with full enterprise browsers and browser extensions already competing for audience attention and corporate budgets, a third approach may struggle to gain comprehension and mindshare. The company already has some channel partners, and more work in this area may be fruitful in championing the approach, as well as making sales.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Developments in Browser Security: From Isolation to Enterprise Browsers (March 2023)

Authors

Rik Turner, Senior Principal Analyst, Cybersecurity

Rob Bamforth, Associate Analyst

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com