Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published December 2018
Sponsored by **McAfee Enterprise**

Why You Should Seriously Consider Web Isolation Technology

Executive Summary

The web is an increasingly risky place and it can introduce and cause a wide range of threats in an organization, including ransomware, other types of malware, leaks of sensitive and confidential information, and catastrophic data breaches, among others. While these problems can occur when employees visit web properties that are well outside the bounds of corporate policy, they can also happen when employees visit valid web sites or access webmail only for work purposes. As a result, organizations need a cost-effective way to mitigate these risks that will balance employees' needs for productivity, while at the same time ensuring that the web does not create an avenue for threats to do damage on the corporate network.

KEY TAKEAWAYS

- Employees spend a significant amount of time accessing various web-based resources like web sites and webmail. Almost all organizations permit employees to use the web for work-related purposes and the vast majority permit personal use of the web from the corporate network.

- A number of serious consequences can result from unfettered use of the web. Employees who visit malicious web sites, mistakenly download various types of malicious software, click on "malvertising" links that can appear on a wide variety of web sites, or fall victim to search engine poisoning can introduce a variety of malicious content into the organization, sometimes with devastating consequences.

- Drive-by downloads are an even bigger threat than users mistakenly downloading malicious content or clicking on malicious links, since they can infect an endpoint without any action required on the part of the user.

- The problems that can result from even "safe" web use are real: the research conducted for this paper found that 60 percent of organizations have been infected with ransomware, other malware or some other threat directly as a result of employee web browsing and/or employee access of personal email on corporate platforms and devices.

- Thirty percent of organizations have suffered data loss directly as a result of employees browsing the web and/or accessing their personal webmail on company time.

- Organizations can mitigate virtually all of these risks by implementing web isolation technology – a technology that permits users to employ the web as they would normally, but that creates physical isolation between web browsing activities and the computers or devices on which the web is accessed.

A number of serious consequences can result from unfettered use of the web.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Light Point Security; information about the company is available at the end of the paper. The paper also presents some of the results from an in-depth, primary market research survey that was conducted specifically for this paper.

©2018-21 Osterman Research

The Dangers of Web Browsing

THE WEB IS COMMONLY USED

The web is an essential element of the workplace and it can make employees more productive by enabling them to access information, storage, social media, cloud services, and various other resources. However, employees also spend significant amounts of unproductive time on the web. For example, one study found that users spend two hours 15 minutes using the web each day for non-work-related activities, such as reading news web sites, checking social media and searching for new jobs[i]. Combined with work-related activities, Osterman Research conservatively estimates that users are spending at least three hours per day using various web properties. In an organization of 500 users, that means that users will spend a combined total of at least 375,000 hours using the web each year.

LOTS OF BAD THINGS CAN HAPPEN

There are a number of problems that can result from web browsing, even from "trusted" sites:

- Users can be directed to malicious web sites or malicious pages on valid sites, resulting in the installation of malware, client-side scripting and other dangerous content. One firm estimates that at any given time there are 18.5 million web sites infected with malware – about one percent of the total[ii]. A drive-by attack can occur in as little as half a second after the user visits a malicious page or site.

- Some users visit non-business-oriented web sites and can inadvertently download malicious content. As one example, in October 2018 the US Office of Inspector General reported that a single employee of the US Geological Survey had visited 9,000 pages of pornography web sites, many of which were routed through Russian web sites that contained malware. The result was that the employee's computer was infected with malware along with his Android mobile phone[iii].

- Users can inadvertently download malicious software, resulting in the installation of malware, client-side scripting and other dangerous content. For example, some malicious downloads can be disguised as trusted software, such as those purporting to be updates to Adobe Flash, but are not from trusted sources and can serve up malicious software. One such fake Adobe Flash update installed a valid update of the Flash player – and cryptocurrency mining malware[iv].

- A significant proportion of advertisements that appear on web sites can deliver malicious content – so-called "malvertising". One such campaign had compromised more than 10,000 WordPress sites and was generating about 40,000 attempted infections per week as of mid-2018[v].

- Search engine poisoning is a common technique for distributing malicious content, wherein cybercriminals will use search engine optimization (SEO) techniques to get malicious content to appear prominently in search results. One example of this threat was focused on keywords used in the US mid-term

There are a number of problems that can result from web browsing, even from "trusted" sites.

©2018-21 Osterman Research

elections – more than 10,000 web sites (most of which were WordPress sites) were hacked to promote more than 15,000 different keywords[vi].

- Web browsers will store login credentials from the web sites that users visit and these credentials can be harvested, enabling access to potentially sensitive web sites.
- Most web browsers use autofill to improve the user experience, but this information can be captured.
- Cookies can be captured and analyzed.
- Geolocation data can be captured and analyzed.
- Browser history can be captured and used to tailor phishing and/or spearphishing attacks.

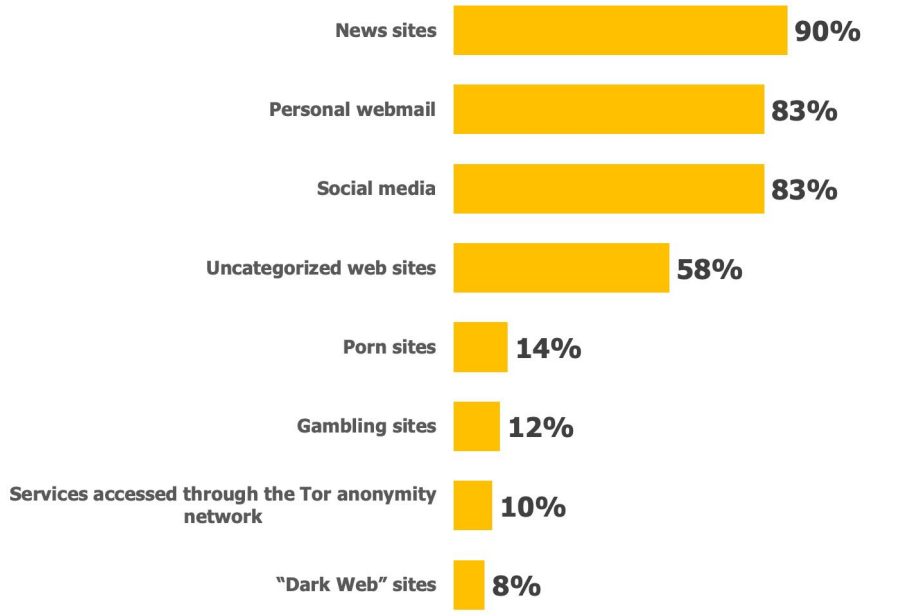
LOTS OF BAD THINGS DO HAPPEN

The survey that was conducted for this white paper found that the risks discussed above are not theoretical – they are commonly experienced by the vast majority of organizations. For example:

- The survey found that 99 percent of the organizations surveyed permit employees to access the public Internet from their work platforms and devices for work purposes.
- The survey also found that 86 percent of organizations permit employees to access the public Internet from their work platforms and devices for personal uses, as well.
- Employees visit various web sites and access a number of services, many of which are extremely risky and can result in serious problems. As shown in Figure 1, these include not only relatively innocuous resources like news sites and personal webmail, but much more risky content like porn sites and the Dark Web.

Sixty percent of organizations have at some point been infected with ransomware, other malware or some other threat directly as a result of employee web browsing and/or employee access of personal email on corporate platforms and devices.

Figure 1
Percentage of Employees Who Access Various Web Sites and Services



Source: Osterman Research, Inc.

- The survey also discovered that 60 percent of organizations have at some point been infected with ransomware, other malware or some other threat directly as a result of employee web browsing and/or employee access of personal email on corporate platforms and devices; eight percent are not sure whether this has happened or not.

- Thirty percent of organizations have suffered some type of data loss directly as a result of employee web browsing and/or employee access of personal webmail on corporate platforms and devices; 10 percent aren't really sure.

THE RESULTS CAN BE DEVASTATING

The consequences that can result from a web-based exploit can be enormous and can wreak havoc on an organization. These include:

- **Data breaches**
  Data breaches reported by the Identity Theft Resource Center in 2017 totaled 1,579, exposing nearly 180 million records. This translates to a breach every five hours 33 minutes, and an average of more than 113,000 records exposed per breach. The most common methods of data breach were related to phishing and malware – much of it delivered via the web – accounting for 60 percent of all breaches[vii].

  Data breaches can have debilitating effects. They can result in various compliance violations, such as those involving:

  - The data breach notification laws that exist in all 50 US states

The consequences that can result from a web-based exploit can be enormous and can wreak havoc on an organization.

- The European Union's General Data Protection Regulation (GDPR) or other privacy regulations like the upcoming California Consumer Privacy Act (CCPA)

- Violations of the Health Insurance Portability and Accountability Act (HIPAA)

- Violations of Securities and Exchange Commission (SEC) and Financial Industry Authority (FINRA) rules

Moreover, they can upset customers whose data has been stolen, resulting in lost future revenue, tarnishing an organization's reputation and requiring significant involvement by IT and security teams. Add to this the often significant expense to remediate these problems.

- **Ransomware attacks**
  Ransomware can be delivered in a number of ways, although the most common methods of delivery are through phishing emails (including when employees use their work or personal webmail on corporate networks) and through exploit kits. While ransomware infection rates have fallen in recent months, one source[viii] reported that 2.8 percent of users – or one in 36 users – had encountered ransomware at least once during the period April 2017 to March 2018.

  The cost of ransomware can be enormous. For example, the City of Atlanta was hit with a ransomware attack in March 2018 that demanded $52,000 to recover the City's files that had been encrypted. The attack impacted 8,000 City employees who were unable to use their computers. In the 11 days ended April 2, 2018, the City had spent $2.67 million on eight emergency contracts to recover from the attack[ix]. One source estimated that the City might end up spending $17 million to fully recover[x].

- **Banking malware**
  Banking malware is a particularly damaging threat because it can infect an endpoint and then monitor logins to bank or other financial accounts for the purpose of stealing login credentials to these accounts. The techniques that cybercriminals use can involve simple keystroke logging or it can use webinjects that are custom designed for specific banking institutions. As just one example, the Dridex banking Trojan stole in excess of $40 million in just 2015 and by mid-2017 had stolen many times that[xi].

- **Computers can become part of a botnet**
  Another consequence of a web infection is that computers can become part of a botnet – an army of "bots" that can be used for criminal activities like sending spam, committing click fraud, delivering malware, capturing login credentials, or participating in distributed denial-of-service (DDoS) attacks. A botnet can consist of a few thousand computers, but can be orders of magnitude larger, such as Conficker that compromised 10.5 million computers and BredoLab that consisted of more than 30 million computers.

Malware infections from web sites and other sources can "de-anonymize" anonymous data.

©2018-21 Osterman Research

- **De-anonymization**
  Malware infections from web sites and other sources can "de-anonymize" anonymous browsing sessions. Users may use advanced tools to hide their identities while browsing, but if a user's computer is infected with malware, those tools will be unable to guarantee the user remains anonymous.

Users are an Enormous Risk

BROWSERS ARE COMMONLY USED BY CORPORATE USERS

As noted above, browsers are commonplace in the context of how information workers remain productive. For example:

- As of mid-2018, 28 to 35 percent of all email opens were accounted for by webmail, nearly double that of thick clients like Outlook[xii].

- Google G Suite, which uses the browser for productivity applications and email, has more than four million paying organizations using the platform[xiii].

- While mobile accounts for the bulk of web access as of the end of September 2018, four of the top ten platforms accessing the web were on desktops and laptops (Windows 7, Windows 10, Mac OS X and Windows 8.1)[xiv].

- According to HTTP Archive, the median web page accessed from a desktop computer as of October 15, 2018 downloaded 1,534 kilobytes of data, made a total of 75 requests, transferred 420 kilobytes of external scripts, transferred 653 kilobytes of images, made 33 requests for images, and made 10 TCP connections[xv]. One estimate is that as web pages increase in size by an average of 16 percent per year, the average page size will be slightly larger than four megabytes by late 2019[xvi]. In short, visiting a single web page transfers a significant amount of data – some of it potentially malicious – to local storage on the desktop from where it can then spread to other endpoints.

- There is a significant number of other applications that users employ on the web during the course of their work, such as collaboration tools, CRM, HR applications, cloud storage applications, and the like. One source calculates that, as of early 2018, enterprises use an average of 1,181 cloud services[xvii]. Many, if not most of these services, use the browser as the primary access mechanism.

While users accessing the web in the course of their work are not exhibiting overtly risky behavior, the fact that they are downloading such an enormous quantity of data to the corporate network through their browsers, some of it malicious, poses a serious risk to an organization.

The use of web isolation technology... should be seriously considered by any organization looking to prevent web-borne threats from entering their corporate networks.

MANY USERS ARE NOT CAREFUL

Compounding the problem of users downloading such enormous quantities of content through the web browser during the normal course of their work are the truly risky behaviors that many users perform. For example, many users are not adequately trained about potentially damaging behavior, such as downloading non-IT approved content from the web or using non-business web sites like Facebook or gambling sites. Many users will click on links on various web sites, such as those

©2018-21 Osterman Research

that prompt them to download a software update, without thinking about the risks of doing so. Many users log into non-secure Wi-Fi networks using their work computers, such as those in airports, coffee shops or restaurants, potentially exposing the entire corporate network to damaging threats that can infiltrate through their web browser when they access corporate resources.

Why Web Isolation is Essential

Current approaches to protecting against web-based threats, such as SSL inspection and DLP, provide some level of security, but they are not completely effective and can provide a false sense of security. Making sites read-only or blacklisting them can also provide some level of security, but they can seriously impede user productivity.

Instead, the use of web isolation technology effectively prevents almost all of the problems discussed above and should be seriously considered by any organization looking to prevent web-borne threats from entering their corporate networks. While server-side and client-side browser isolation technology can shield users from direct access to the web and thereby protect against the various threats associated with conventional web browsing, client-side solutions manage isolation on each local machine, not through a physically isolated "air gap" approach as with server-side solutions. Remote browsing solutions are another option for those that wish to implement true web isolation technology.

With web isolation technology even sites that are known to contain malware can be browsed with no potential for infection of the endpoint.

WEB ISOLATION SHIELDS USERS FROM THE INTERNET

The use of web isolation technology protects against the infiltration of web-based threats very effectively:

- **Performance and cost benefits**
  Web isolation offers performance and cost benefits over traditional methods of web security, since the need to download web code and execute it locally – in conjunction with inspecting, scanning and flagging potential problems – is straining IT resources. Moreover, isolating the web outside the network means fewer point solutions are required internally to monitor, control, and secure that content.

- **No local code execution**
  Code execution takes place remotely, thereby shielding users from potentially malicious code that, when downloaded through normal web browsing, could wreak havoc on their workstation and the corporate network, such as a ransomware infection or the installation of malware that could steal data. These threats could come from compromised web pages on valid web sites, web pages that were designed to be intentionally malicious, or malvertising, for example.

  As noted earlier, while conventional web browsing can be made safer by allowing users to visit only known safe web properties, there is the potential for impacting user productivity by blocking valid, safe sites that have not yet been classified as such. Our survey found that 46 percent of organizations have considered restricting use of the public web for all users because of security concerns, and another 34 percent have considered doing so for some users.

©2018-21 Osterman Research

- **Prevention of email-based threats**
  As a corollary to the point above, the large proportion of users who employ webmail to access the corporate email system, or that access personal webmail over the corporate network, will not expose the network to email-based threats. This is because malware delivered via webmail never reaches the endpoint and so cannot execute.

  Protection from malicious links
  Related to the previous bullet point, in addition to web-based email, remote browser isolation protects organizations from the malicious links that can be contained in emails received via thick email clients, such as Outlook. This is because links will automatically open harmlessly in the browser isolation solution, unlike what would happen using conventional web browsing.

- **Protection from malicious downloads**
  Browser isolation provides organizations with malware protection for file downloads because organizations can control which files users are permitted to download, and which ones they cannot. Moreover, for file downloads permitted by policy, the files are first scanned or sanitized before the download occurs.

- **User locations are not exposed**
  Corporate IP addresses are never exposed, resulting in enhanced security because users' locations are not exposed, malicious actors cannot track users' online activity, the content of searches is kept private, and geographic restrictions on accessing content are eliminated.

- **Data loss prevention**
  Browser isolation also enables data loss prevention capabilities to protect against insider threats and accidental data leaks. Similar to file downloads, organizations can control which files users are allowed to upload (and to what websites), and which ones they cannot.

- **A reduced number of alerts**
  Another benefit of web isolation technology is that by blocking malicious or suspect content from entering the corporate network, there are fewer alerts and false positives for security teams to analyze. In most organizations, security teams are already overworked dealing with the normal flow of alerts from a variety of sources, and so the ability to reduce at least one avenue of these alerts will be of benefit to the security function.

- The bottom line is that with web isolation technology even sites that are known to contain malware – as well as the millions that may or may not contain malware – can be browsed with no potential for infection of the endpoint.

Browser isolation provides organizations with malware protection for file downloads because organizations can control which files users are permitted to download.

THE BROWSING EXPERIENCE IS NOT COMPROMISED

There are a number of web isolation vendors and technologies available, and so we cannot make a blanket statement that there will never be a compromise of the user experience when using web isolation technology compared to conventional browsing. However, there are a number of vendors of web isolation technology that offer solutions that will not result in a degraded user experience. These solutions offer a browsing experience that is indistinguishable from conventional browsing in

©2018-21 Osterman Research

terms of page load times, the ability to play video, and the overall user experience. In short, users employing robust web isolation technology will not experience any change in the way they use the web or their ability to be productive.

COMPLIANCE IS AN IMPORTANT CONSIDERATION

As alluded to above, new data protection regulations, such as the GDPR and the California Consumer Privacy Act (CCPA), lay out various legal rights held by consumers over their personal and sensitive personal data. Entities that collect and/or process this type of data must extend these rights to consumers, or else face harsh penalties. Specific rights vary by regulation and region, although the GDPR is the most far-reaching of any current data protection regulation. While the GDPR has applicability for data subjects in Europe, the extra-territorial scope of the regulation means that a large proportion of organizations around the world are potentially subject to it. GDPR is indeed having global effects, with more than 100 countries around the world implementing laws that draw on its principles. Few are as extensive as GDPR, but many share similarities.

What this means for organizations that permit their employees to use the web is that it creates a number of compliance risks. For example, malware that enters an organization via the web could result in a data breach that could cost an organization tens or hundreds of millions of dollars in fines and other losses. The use of web isolation technology is one means to reduce the potential for data breaches from occurring.

Conclusion

Web browsing is dangerous and the problem is getting worse. Cybercriminals use a growing variety of techniques to infect endpoints, use valid web sites to distribute malicious content, direct users to various sources where their endpoints can become infected, steal credentials, and otherwise make even simple browsing a dangerous practice. To make web browsing dramatically safer, organizations should deploy remote browser isolation technology. Using this technology will preserve the integrity of the end user experience, while at the same time preventing malicious content from reaching the endpoint.

Sponsor of this White Paper

McAfee Enterprise has set the pace and standard within the cybersecurity industry for more than 30 years and has become a recognized leader for device-to-cloud cybersecurity solutions. As a trusted partner for 86% of the Fortune 100 firms around the world, we have helped simplify security, accelerate digital transformation, and better defend against advanced attacks, no matter where or how teams are working.

McAfee® Remote Browser Isolation provides the most powerful form of web threat protection available, eliminating the opportunity for malicious code to even touch the end user's device. McAfee Remote Browser Isolation features some of the most advanced security capabilities on the market, including advanced pixel mapping technology, integrated data loss prevention (DLP) and user entity behavior analytics (UEBA). In addition, McAfee Enterprise has changed the game when it comes to making Remote Browser Isolation accessible for any organization or any budget by making it a seamlessly converged component of MVISION Unified Cloud Edge.

McAfee Enterprise

www.mcafee.com/RBI

©2018-21 Osterman Research

Some of the key capabilities that set McAfee Remote Browser Isolation apart include:

Comprehensive Data Loss Prevention
Enhanced visibility and protection over how data is being accessed or shared.

Part of a Complete Threat Protection Stack
Works directly in-line with MVISION Unified Cloud Edge threat protection, ensuring consistent policies, data protection, and visibility across isolated and non-isolated traffic.

RBI at No Extra Cost
Remote Browser Isolation for risky web traffic is included as part of MVISION Unified Cloud Edge at no additional cost. McAfee Enterprise is the only vendor to offer RBI for free as part of its broader SASE security solution.

Simple to Use
Clientless technology seamlessly integrates with standard web browsers so users require no training or changes in behavior.

Fast and Responsive
Websites load quickly and are immediately responsive to typing, clicking and scrolling – no more slow web browsing!

Powerful Management
Robust policy and reporting engines provide the optimal flexibility and granularity to secure users' browsing activities.

©2018-21 Osterman Research

© 2021 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] https://www.inc.com/melanie-curtin/in-an-8-hour-day-the-average-worker-is-productive-for-this-many-hours.html

[ii] https://www.securityweek.com/185-million-websites-infected-malware-any-time

[iii] https://www.oversight.gov/sites/default/files/oig-reports/ManagementAdvisory%20_USGSITSecurityVulnerabilities_101718_0.pdf

[iv] https://researchcenter.paloaltonetworks.com/2018/10/unit42-fake-flash-updaters-push-cryptocurrency-miners/

[v] https://www.bleepingcomputer.com/news/security/massive-malvertising-campaign-discovered-attempting-40-000-infections-per-week/

[vi] https://www.bleepingcomputer.com/news/security/seo-poisoning-campaign-targeting-us-midterm-election-keywords/

[vii] https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

[viii] https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf

[ix] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[x] https://www.bankinfosecurity.com/atlantas-reported-ransomware-bill-up-to-17-million-a-11281

[xi] http://www.csoonline.in/media-releases/unstoppable-dridex-banking-trojan-causes-damages-Millions

[xii] https://www.emailmonday.com/mobile-email-usage-statistics/

[xiii] https://www.reuters.com/article/us-alphabet-gsuite/googles-g-suite-is-no-microsoft-killer-but-still-winning-converts-idUSKBN1FL3ZX

[xiv] https://www.w3counter.com/globalstats.php

[xv] https://httparchive.org/

[xvi] https://speedcurve.com/blog/web-performance-page-bloat/

[xvii] Source: Netskope Cloud Report, Winter 2018