ERICOM
Be Connected, Be Secure

Locking down the vault: Keep cyberthreats away from your business

Contents

Introduction

Small and medium-sized financial service organizations -- local banks and credit unions, brokerages, financial advisory firms, and accounting and insurance practices -- often earn high marks for customer service. When it comes to cybersecurity, however, it's a challenge for smaller firms with limited staffing and security budgets to keep pace with their larger peers.

Small and medium-sized financial services firms are especially vulnerable to cyberattacks

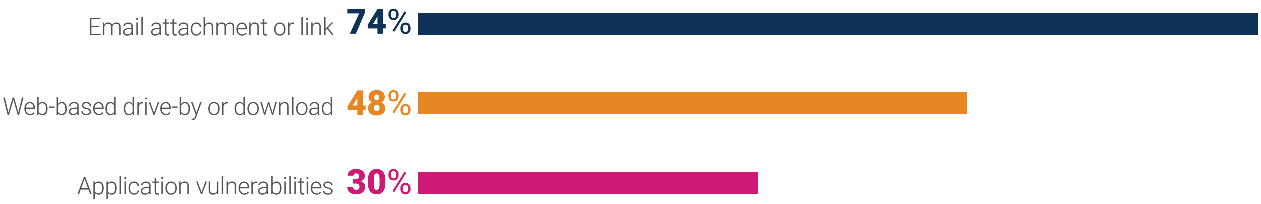
Financial services organizations, by definition, deal with money and personal data that are highly attractive for malicious actors. When seeking targets that are both rewarding and easy to breach, cybercriminals may assume that small and medium-sized financial service providers trail their larger counterparts in locking down security gaps – and too often, they are correct.

Cybercriminals assume that small and medium-sized financial service providers trail larger counterparts in locking down security gaps

Worldwide, banking is one of the most cyber-regulated industries. Regulations apply equally to local banks, credit unions and other small financial service organizations as they do to large banks, insurance companies and brokerages. For smaller organizations however, compliance may consume a larger proportion of security budgets, leaving fewer manpower and financial resources for non-mandated – but essential -- security coverage.

Today, spear-phishing, business email compromise (BEC) and users' erroneous clicks on malicious links are the most dangerous threat vectors, along with fileless malware, zero-day attacks and other web-based threats that penetrate systems via porous browsers.

Top vectors by which threats enter organizations



Sans 2017 Threat Landscape Survey: Users on the Front Line[1]

[1] https://www.sans.org/reading-room/whitepapers/threats/paper/37910

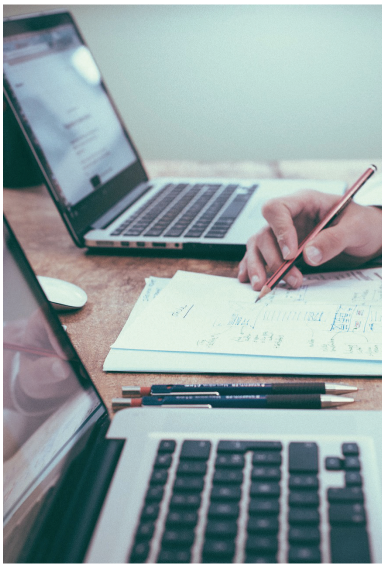
Financial services companies, like all businesses, in all fields, need to protect their data and systems. At the same time, however, internet use is non-negotiable: The web is an essential business resource for employees as well as third-party services. And like most businesses, financial service organizations conduct much of their operations, as well as customer interactions, via the web.

Traditional solutions aren't enough

Gartner recommends remote browser isolation (RBI) as a critical solution for securing web access

While traditional detection-based solutions are effective against known threats, they cannot keep up with the rapid evolution of malware variants. By the time they catch up, immense damage can be done. Phishing protections are similarly insufficient: The majority of phishing sites are taken down within six hours, way before even the best URL filtering solutions can mark them as malicious and block user access or warn users away.

Whitelisting websites offers some measure of protection but has serious downsides as well. Many users need access to a wide and unpredictable range of websites and having to request permission to access them reduces productivity, frustrates users, and increases demands on IT. Perhaps worse, even whitelisted sites can be hacked and infected with malware, putting site users at risk.



To address the risks presented by web-borne malware, Gartner has enumerated seven major security goals for services that secure web and internet traffic[2], including enforcing acceptable use policies via URL filtering, blocking bad URLs, protection from malicious file downloads, and detection and blocking of malicious content within a site. They also identified complementary solutions that should be integrated with secure web gateways (SWG) and other standard security architectures to achieve web security goals, naming remote browser isolation (RBI) as a "simple way to protect all users from malicious content" both on its own and in conjunction with DNS redirection and/or full proxy solutions.

RBI protects organizations from web-borne threats by sending only a rendered website image to the user's browser, while actual browsing takes place in the cloud, a remote location, or on a virtual machine. Of course, the devil is in the details: a number of remote browser isolation solutions are available, and small to medium-sized financial service providers must find the solution that effectively secures their data and networks without disrupting user, customer, IT or infrastructure workflow.

[2] Select the Right Strategy for Securing Web Access

Finding the right browser isolation solution

Small and medium-sized financial services businesses face some unique challenges that should guide their decisions when choosing a browser isolation solution. Let's get specific:

Software solution vs hardware

For distributed organizations such as banks with several branches but limited information security staff, clientless software solutions that can be deployed and managed from a central location minimize the need for on-site support and enable efficient management.

Compatibility with small business security stacks

Security stacks of small and medium-sized businesses may include appliances and solutions ranging from entry-level to next generation. Additional solutions must be easily integrated with all grades of technologies that are – or may eventually be -- part of the security stack.

Flexible deployment on site, in the cloud or as a service

Many financial institutions prefer the control afforded by an on-premise solution, while others appreciate the ease of cloud or service-based solutions. Because no one flavor is appropriate for every financial service organization at every point, security solutions that offer a choice of deployment options are ideal.

User experience

No financial service business (or any business, for that matter) can tolerate poor browsing experience caused by security solutions: Brokerages need to execute orders within seconds and insurance agencies, banks and investment house must provide high-touch customer service, without delays or interference. Seamless performance is essential when securing browsing from web-borne threats.

Excellent support

Dedicated cybersecurity staff is in short supply in many small and medium-sized businesses. Despite their attractiveness as a target for cyberattack, this holds true for most financial service SMBs as well. As such, it is important to choose a solution that is backed by strong, hands-on support, especially during integration and on-boarding.

Ericom Shield: Remote Browser Isolation for financial service providers

Financial services organizations of all sizes are choosing Ericom Shield to secure their systems from web-borne threats and social engineering attacks that leverage the web. Banks, credit unions, brokerages and accountancy firms appreciate that it provides airtight protection, yet enables employees to access the web as they need, without in any way impeding productivity.

> **"Ericom Shield is seamless to end users, who don't even realize they're using it. Other products require a different application for browsing the web."**
>
> ***CIO, community bank***

In the words of one CIO, "After reviewing other remote browser solutions and how they function in the real world, Ericom Shield was the solution that best matched our needs."

Ericom Shield executes all web content in remote isolated containers that reside in either the DMZ or cloud. A safe content stream is sent to the browser, enabling full, natural user interaction with websites.

To protect against credential theft, security administrators can pre-select responses to suspected phishing and BEC attacks based on threat probability and organizational policies. For instance, a warning requiring user acknowledgement may be issued before a user can continue to a suspected phishing site or the website may open in 'Read-Only' mode, preventing information entry via keyboard or copy-paste functions.

Critically, Ericom Shield technology requires less processing overhead than other browser isolation solutions and is therefore less costly to operate as well as more secure.

> **"Ericom pre-sales and ongoing support is top tier. It is fantastic."**
>
> ***CIO, community bank***

To accommodate the unique needs of each organization, Ericom Shield is available as an on-premise or cloud solution, as well as isolation-as-a-service. The solution integrates seamlessly with both enterprise and entry-level solutions of leading security providers including Cisco, Check Point, McAfee, Fortinet, Palo Alto Networks and others.

As a clientless, centrally managed software solution, Ericom Shield is ideal for businesses that are strapped for cybersecurity staff. Seamless integration with Active Directory and Ericom Shield's intuitive management dashboard make it quick and easy to specify privilege and security levels for individual users and groups.

Finally, customers rave about Ericom's start-to-finish support, from POC and throughout integration and roll-out.

The bottom line

With Ericom Shield, banks and financial service businesses can allow employees to freely browse the internet as needed, without burdening tightly-stretched IT staff. Organizational networks and endpoints and customer data are protected from the most prevalent vectors for browser-borne malware, human error, malicious links, and harmful downloads.

Ericom Shield is an advanced remote browser isolation solution that adds a powerful layer to organizational defense-in-depth strategy by isolating malware, ransomware and other threats where they can't harm corporate network or user devices. It transparently secures Internet use, including file downloads and phishing sites, while reducing risk, costs and operational burden to IT staff responsible for browsing operations. Ericom Shield harnesses the power of isolation to deliver secure browsing and protect the corporate network and endpoints.

For more information about how Ericom Shield Remote Browser Isolation can protect your financial services organization from browser-borne malware, human error, and other threats

Contact us

ERICOM
Be Connected, Be Secure

www.ericom.com/solutions/browser-isolation

shield@ericom.com

US: (201)767-2210
Europe: +44 (0)1905 777970
ROW: +972-2-591-1700