



Small and Medium-Sized Financial Service Businesses Choose Ericom Shield to Protect Against Web-borne Attacks

Customer profile

Community Bank & Credit Union

Product

Ericom Shield®

Industry

Financial Services



Challenge

- Protect systems of financial services companies from web-borne malware and social engineering attacks involving malware and credential theft
- Enable employees to freely utilize internet resources they need
- Reduce IT exception handling for unlisted sites, as well as overhead for breach detection and remediation securely access the websites they need for their work

Customer -- and Hackers -- Love Small and Medium-sized Financial Services Firms

Small and medium-sized financial service organizations -- community banks and credit unions, brokerages, advisory firms, and accounting and insurance practices -- often earn great marks for customer service. When it comes to cybersecurity, however, it's a challenge for smaller firms with limited IT staffing and even more limited budgets to keep pace.

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.

Detection-based Security Solutions Aren't Enough

While traditional detection-based solutions are effective against many known threats, they cannot defend against the constant stream of new malware and emerging threats. For instance, the average phishing site is already offline within six hours of publication, well before it can be identified and blacklisted.

Whitelisting websites offers some protection but has serious drawbacks. Bankers, loan officers and financial advisors need quick access to a wide and unpredictable range of websites. Moreover, even whitelisted sites can be hacked and infected with malware, putting site users at risk.

Remote browser isolation, which Gartner considers a critical solution for securing web access, protects organizations from web-borne threats by rendered websites elsewhere, with locations varying for different solutions. Only a clean content stream reaches the user's browser.

A number of browser isolation solutions are available, and small to medium-sized financial service providers must find the right solution for their business -- one that thoroughly secures their data and networks without disrupting users, customers, IT infrastructure or workflow.

Finding the Right Browser Isolation Solution

When choosing a browser isolation solution, the decisions of small and medium-sized financial services businesses should be guided by the following considerations:

Software vs hardware

Distributed organizations with several branches but limited information security staff need clientless software-based solutions that can be centrally deployed and managed from a remote location. Unlike hardware-based solutions, they minimize the need for on-site support and can be managed efficiently from afar.



Solution

- Ericom Shield provides airtight protection from phishing sites, fileless malware, zero-day threats and other browser-borne attacks, while enabling a seamless, natural browsing experience for users

Compatibility with small business security stacks



"The ability to host onsite was pretty important since, as a bank, we like to control everything."

CIO,
community bank



Security stacks of small and medium-sized businesses may include appliances and solutions ranging from entry to enterprise-level. Additional solutions must be easily integrated with all current and future technologies.

Flexible deployment options

Today, many financial institutions prefer the control afforded by an on-premise solution. Others appreciate the ease of cloud or service-based solutions, and it is likely that more organizations will ultimately move to the cloud. Security solutions that offer a choice of deployment options are the best way to go.

User experience

Users today will not tolerate browsing delays due to security considerations. Regardless of whether they work for a brokerage and must execute orders right now, or for an insurance agency that provides high-touch customer service, seamless performance is essential.

"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

Excellent support

With dedicated cybersecurity staff in short supply in many small and medium-sized financial service organizations, 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

Numerous financial services organizations have chosen Ericom Shield to secure their systems from web-borne threats and social engineering attacks. They appreciate the airtight protection it provides, while enabling employees to access the web as they need, without in any way impeding productivity.

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 may be issued that the user must acknowledge before continuing to a suspected phishing site. Alternatively, suspicious website may open in 'Read-Only' mode, preventing information entry via keyboard or copy-paste functions.



Results

- Safeguard organizational networks and endpoints from malicious web content and social engineering attacks while allowing users to browse freely
- Users can access unlisted sites without waiting for IT approval – and without risk
- Integration, deployment and permissions for all users, across all branches, are easily managed from a central location
- Financial institutions can choose on-site deployment, cloud-based deployment, or isolation-as-a-service models in accordance with security policies

Critically, Ericom Shield technology requires less processing overhead versus alternative solutions and is therefore less costly to operate – a key advantage that several financial services CIOs have cited.

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. It integrates seamlessly with both enterprise and entry-level solutions of leading security providers including Forcepoint, Cisco, Check Point, McAfee, Fortinet, Palo Alto Networks and others.

As a clientless, centrally managed software solution, Ericom Shield is well suited to 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.

Virtually all customers rave about Ericom’s start-to-finish support from POC through integration and to roll-out.



“Ericom pre-sales and ongoing support is top tier. It is fantastic.”

CIO,
community bank



The Bottom Line

Ericom Shield enables banks and financial service businesses to 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 attachments.

About Ericom Software www.ericom.com

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom’s solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access. © 2020 Ericom Software. Ericom and the Ericom logo are trademarks of Ericom Software. All other trademarks used in this document are the property of their respective owners.

Americas:
T +1 (201)767-2210
E-mail: info@ericom.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: ukinfo@ericom.com

Worldwide:
T +972-2-591-1700
E-mail: info@ericom.com

Follow us

