EVERFOX

BROCHURE

Securing Financial Industries

Protecting Financial Services: A Critical Priority

Organizations that deliver the financial services on which we all depend are consistently under pressure to defend against cyberattacks while still maintaining the system availability and integrity on which the business depends.

Cyberattacks on financial industries are growing in frequency and sophistication, while becoming potentially more severe and destructive. For example, a Trojan attack such as SharkBot targeted Italian and UK banks in late 2021, granting itself admin rights, collecting keystrokes, intercepting F2A SMS messages, and accessing mobile banking and cryptocurrency apps to transfer funds. In another, a financially motivated cybercriminal gang, FIN8, breached the network of two U.S. financial organizations. Defending against cyberattacks is a persistent challenge.

Effective protection against these attacks requires flexible solutions that can adapt to their unique industrial contexts and challenges while being strong enough to keep out even the most persistent or advanced adversary.

As many organizations attempt to implement Zero Trust Architectures or align to a Zero Trust approach to cybersecurity, it is critical to look at segregating networks and enabling capabilities that provide advanced analytics and baselining user behaviors. Baselining and monitoring privileged users enables continuity to the cybersecurity architecture, and segregating networks adds additional protection against adversaries, whether they are nation state or non-nation state actors.

Challenges for Financial Services

Email Security

Email security is a critical challenge for financial services due to an increase in malware, ransomware, phishing attacks and insider threats. With over 91% of breaches starting with an email. These challenges necessitate robust and adaptive email security measures

System Vulnerabilities

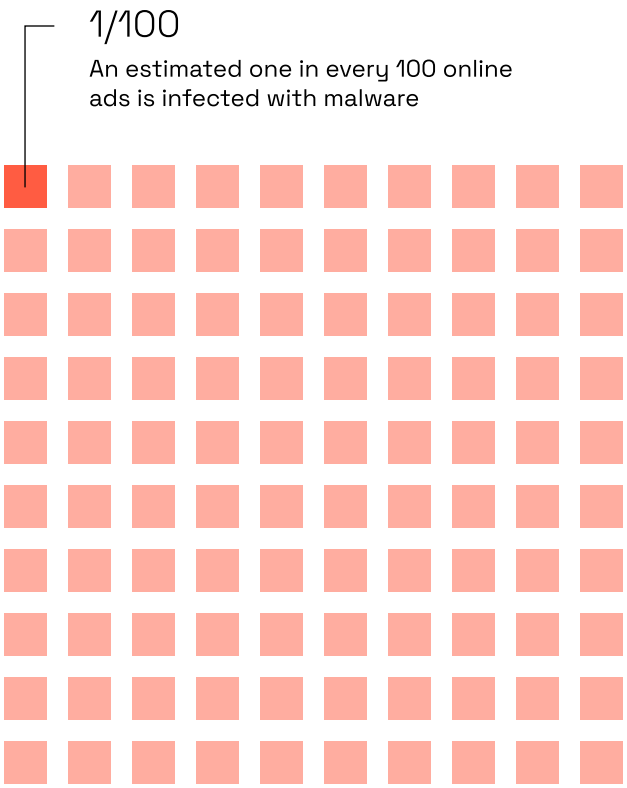
Most malware depends on software vulnerabilities. For example, malvertising aims to install malware without the user's knowledge. Malware can only be downloaded to a device if the software has a vulnerability that can be exploited, allowing it to install.

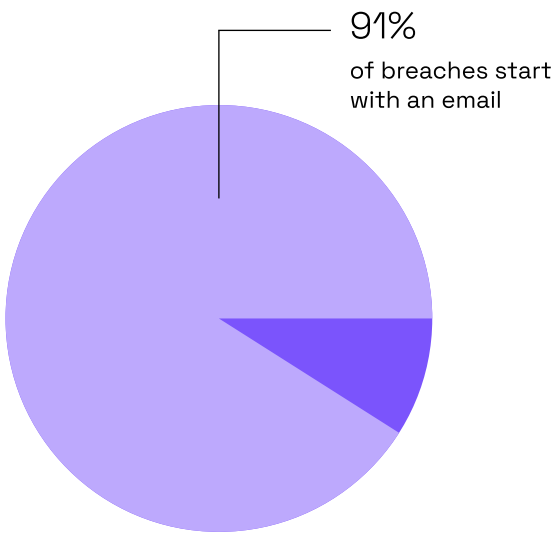
Ineffective Security Measures

A companies choice in security measures can often be the difference between data loss and data protection. Understanding that cyber security is not a one size fits all solution. Ensuring that the right measures are deployed for the security needs is crucial.

Web-borne Threats and Malvertising

Hackers using spoof sites or even legitimate websites to carry exploits and malware. One form of this is malvertising, where usual legitimate ads on well-known websites are infected with malware. When a user navigates to an infected site, the may end up infecting their device. Malvertising is a serious issue, with an estimated one in every 100 online ads being infected (Security Gladiators)





Everfox Financial Services Product Portfolio

Everfox provides a comprehensive portfolio of products designed to help providers of financial services to meet these challenges.

High Speed Verifier (HSV)

Everfox HSV combines the best of data transfer solutions with the added benefits of dual one-way data transfer and builtin threat removal. As a bi-directional data verifier, the way the HSV conveys information and hides the attack surface of the destination server makes it suitable for protecting your sensitive data.

Data Guard

Everfox Data Guard enables the bidirectional, automated transfer of highly complex data-including real-time streaming video across segregated networks. With deep content inspection and highly granular policy based control over source, destination, and content, Data Guard is ideally suited to cross-domain data transfer and targets specific high assurance security requirements.

Everfox Data Diode

The Everfox Data Diode enables rapid data transfers from one network to another, while ensuring that no information passes in the opposite direction. The Data Diode can be used to get information out of a critical network without introducing any means by which that network can be attacked.

High Speed Guard (HSG)

Deliver secure, automated, high-performance data transfer for every environment and mission with Everfox High Speed Guard.

Everfox High Speed Guard streamlines and secures data distribution between separated networks to protect data where it resides.

Information eXchange (IX)

iX operates inline at the network perimeter to eliminate potential malware in business content, including unstructured formats like Office, PDF and structured data like XML, JSON.

Everfox Insider Risk

Everfox Insider Risk Solutions is a User Activity Monitoring (UAM) and Analytics platform which drive improvements in your insider risk program. Giving analysts and investigators the right tools needed to collect, explore, and gain insight into risky behavior.

Everfox Financial Services Product Portfolio

Everfox provides a comprehensive portfolio of products designed to help providers of financial services to meet these challenges.

Content Disarm and Reconstruction (CDR)

Everfox CDR works to deliver malware-free data without using detection. It works by extracting the valid business information from files, verifying the extracted information is well-structured and then building brand new files to carry the information to its destination. This unique zero trust approach is applied to all data, irrespective of whether it contains a threat or not. It renders IT files such as Office and PDF documents and images threat-free

CDR for Mail: Microsoft 365

Email is the most common attack vector for cyber threats such as phishing, malware and ransomware. Resulting in organizational disruption, financial damage, and data loss. Get comprehensive protection for your most critical business investment. Everfox CDR for Mail: Microsoft 365 stops advanced malware, zero-days and unknown attacks that can lead to ransomware and other devastating impacts.

Application eXchange (AX)

Everfox Application eXchange (AX) is a set of APIs developers can use to access our Content Disarm and Reconstruction-as-a-Service (CDRaaS) and integrate it into workflows and applications. The CDR engine transforms Office, PDF, image files and more, removing evasive, zero-day malware, known and unknown threats. Eliminating even steganography threats often concealed in images.

Gateway eXtension (GX)

Extend the capability of your perimeter web defense with the Everfox Gateway eXtension (GX). Ensure complete protection from the ever-increasing onslaught of known, zero-day, and unknown content threats.

Solution Summary

Scenario	Requirements	Consider these solutions
Ring-fencing the enterprise	A zero-trust security posture for all inbound content arriving at the enterprise network	• HSV with CDR • Insider Risk • Behavioural Analytics
Monitoring networks from the cloud	Secure and reliable data transfer with no data loss	• HSV with CDR
Combatting phishing attacks, ransomware and zero-day exploits		• CDR • Insider Risk • Behavioural Analytics • CDR for Mail: M365, AX & GX
Web browsing upload and download		• CDR • GX
Email and file transfer		• CDR • CDR for Mail: M365 • Data Guard • Data Diode • High Speed Guard
Assured instant messaging		• CDR • CDR with iX Appliance

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com

EverfoxTM is a trademark of Forcepoint Federal Holdings LLC. All other trademarks used in this document are the property of their respective owners.