Forcepoint Securing Financial Industries

Forcepoint

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

Phishing

Phishing attacks remains a favorite among cyber criminals, targeting employees and privileged users. Phishing emails are a severe threat, with Verizon stating that 22% of data breaches involve phishing (2020 DBIR Summary of Findings | Verizon Enterprise Solutions)

22%

of data breaches
involve phishing

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)
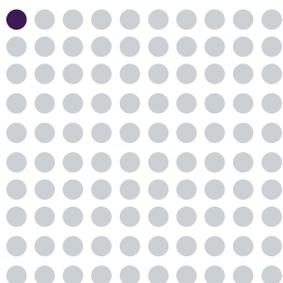
1/100

An estimated one in every 100 online ads is infected with malware
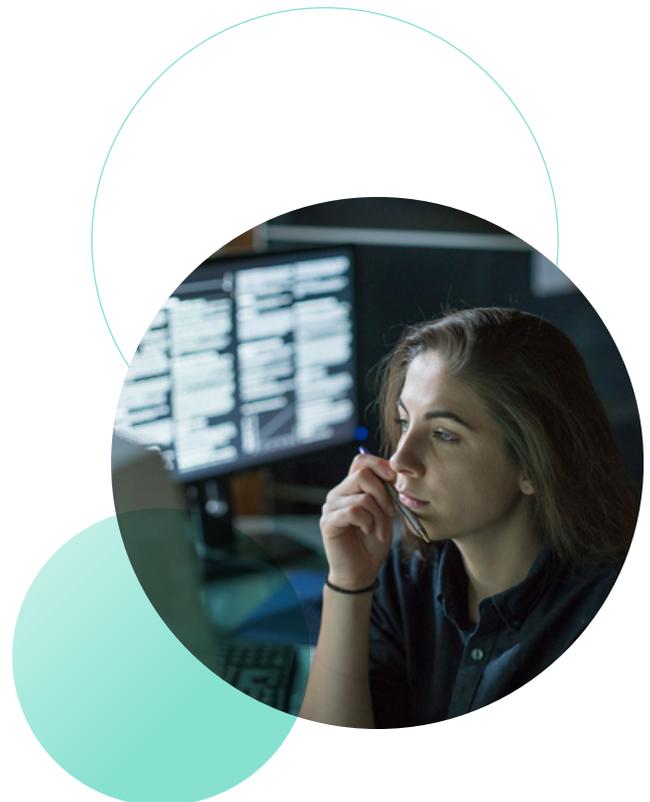
Forcepoint Financial Services Product Portfolio

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

Zero Trust Content Disarm and Reconstruction (CDR)

Forcepoint Zero Trust CDR works with the High Speed Verifier (HSV) 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 and can also be applied to the web application traffic.

Forcepoint One

Forcepoint ONE is an all-in-one cloud-native security platform that makes it easy to adopt Security Service Edge (SSE) by unifying crucial security services.

With Forcepoint ONE, security teams can now manage a single set of policies across all apps, from one cloud-based console, through one endpoint agent, with agentless support for unmanaged devices.

High Speed Verifier (HSV)

The Forcepoint iX Appliance with High Speed Verifier (HSV) deployed as a physical on-premise appliance constrains the interface to the HSM using verification in hardware logic to ensure the HSM only receives safe, valid data, preventing a malware attack

Data Guard

Forcepoint 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.

Next-Gen Firewall

Forcepoint Next-Gen Firewall (NGFW), combines fast, flexible networking (SD-WAN and LAN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Forcepoint NGFW provides consistent security, performance, and operations across physical, virtual, and cloud systems. It's designed from the ground up for high availability and scalability, as well as centralized management with full 360° visibility.

Unidirectional Gateway (Data Diodes)

Forcepoint Data Diode ensures secure one-way transfer with optical isolation, enabling organisations to create boundaries between trusted and untrusted networks by creating a physically secure one-way communication channel. Ideally suited to unidirectional protocols, Data Diodes enable you to send data from one secure network to another; data is transferred using light instead of electrical signals, ensuring that data can enter but never exit.

Forcepoint Insider Threat (FIT)

Forcepoint Insider Threat has been identifying and stopping threats from within for government and Fortune 100 customers for more than 15 years. With more than 1 million endpoints deployed, Forcepoint Insider Threat's proven solution protects some of the most sensitive organizations on the planet. One Fortune 100 retail client realized 60% ROI in the first year of deployment. Insider Threat empowers your organization, saving your team time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts. This frees your team to focus on high-priority tasks and improves efficiencies. Forcepoint Insider Threat also provides the context and forensic evidence needed for undeniable attribution and chain of custody–simplifying investigations, prosecution, and compliance.

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	• High Speed Verifier with Zero Trust CDR • NGFW • Forcepoint ONE • Forcepoint Insider Threat • Behavioural Analytics
Monitoring networks from the cloud	Secure and reliable data transfer with no data loss	• High Speed Verifier with Zero Trust CDR • NGFW
Combatting phishing attacks, ransomware and zero-day exploits		• Zero Trust CDR • Forcepoint ONE • Forcepoint Insider Threat • Behavioural Analytics
Web browsing upload and download		• Zero Trust CDR • Forcepoint ONE • Data Loss Prevention (DLP) • Remote Browser Isolation
Email and file transfer		• Zero Trust CDR • Forcepoint ONE • Data Loss Prevention (DLP)
Assured instant messaging		• Zero Trust CDR • Zero Trust CDR with iX Appliance • Forcepoint ONE

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on **www.forcepoint.com**, **Twitter** and **LinkedIn**.