DATA SHEET

Attack Surface Intelligence for Financial Services

Discover and defend your entire attack surface

Challenge

Financial institutions work with large amounts of sensitive information related to clients, partners, and employees – making them an ideal target for cybercriminals. To compound this threat, ongoing digital transformation projects, increased cloud reliance, and a growing remote workforce combine to significantly expand the attack service these organizations must secure.

Critical Exposures in the Attack Surface

Misconfigurations: Open ports and remote access parameters, for example, that might allow malicious parties to gain unauthorized access to networks and applications

Vulnerable Software: Digital assets susceptible to attacks, such as contact management systems (CMS), database servers, and JavaScript libraries

Exposed Administrator Panels: Exposed, public-facing admin panels for popular technologies and software can provide attacker's easy access into your network using stolen credentials

Solution

Proactive attack surface management is essential for keeping up with an expanding threat landscape and sophisticated attackers intent on targeting financial institutions. With digital assets scattered across the internet, often spun up without proper security oversight and hygiene, and left forgotten and unsecured, financial institutions must ensure they understand where soft spots in their perimeter could be.

Equipping security and compliance teams with a comprehensive toolset to understand and mitigate risk helps organizations see the blind spots that are visible to adversaries and move the advantage back to their teams. Access to an outside-in view of their external infrastructure helps organizations catalog and remediate their vulnerabilities, misconfigurations, and unknown assets that cybercriminals are looking to exploit.

How Attack Surface Intelligence Can Help:

- Discover previously unknown shadow IT and out-of-policy assets
- Accelerate vulnerability scanning and incident response
- Confidently prioritize assets that may be vulnerable to threats or exploits
- Disrupt adversaries, while minimizing disruption for your business

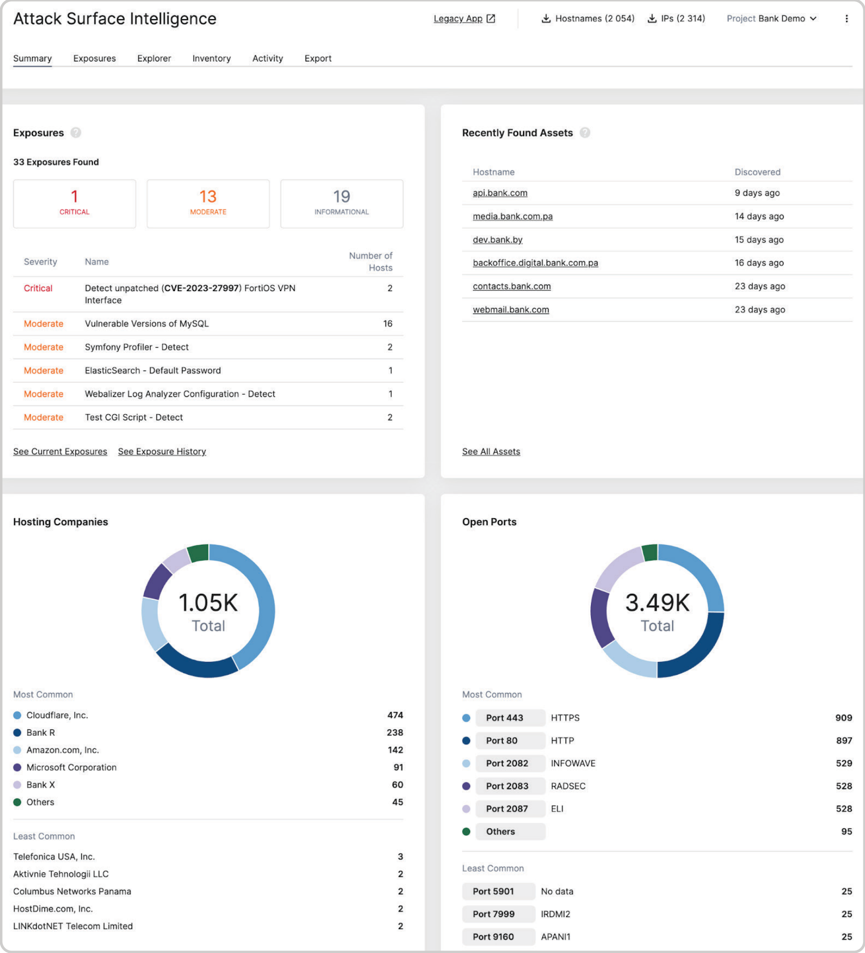
Client Use Case

A large financial services company has found Attack Surface Intelligence to be invaluable for detecting critical ports not meant to be open. While protections are often in place for the company to ensure outsiders can't access critical ports, some were temporarily opened but mistakenly not closed. Using Attack Surface Intelligence has helped them design new workflows to ensure these inadvertent mistakes do not repeat.

Attack Surface Intelligence provides defenders with a complete understanding of their attack surface via a real-time snapshot, as well as a historical view, of all on-premise and cloud based assets on the internet at any given time. Armed with real-time exposure scoring and comprehensive intelligence on vulnerability and misconfigurations helps security teams prioritize incident response investigations, supercharge vulnerability scanning, and confidently reduce risk.

Features

- **Asset discovery and inventory:** Discover and map your external-facing assets and systems. Ensure mergers and acquisitions don't leave shadow IT, marketing campaigns are spun down with proper care, and your infrastructure isn't tied to a vulnerability being exploited in the wild.
- **24-7 infrastructure monitoring:** Continuously manage your digital footprint with persistent scanning of the internet for domain-related environments (such as cloud services and external-facing on-premises infrastructures) and distributed ecosystems (such as IoT infrastructures).
- **Exposure Prioritization:** Identify critical risk to your business with actionable intelligence on vulnerable systems, misconfigured assets, and exposed infrastructure to quickly find and block off potential doors into your business before cybercriminals can exploit them.



Severity	Name	Number of Hosts
Critical	Detect unpatched (**CVE-2023-27997**) FortiOS VPN Interface	2
Moderate	Vulnerable Versions of MySQL	16
Moderate	Symfony Profiler - Detect	2
Moderate	ElasticSearch - Default Password	1
Moderate	Webalizer Log Analyzer Configuration - Detect	1
Moderate	Test CGI Script - Detect	2

Hostname	Discovered
api.bank.com	9 days ago
media.bank.com.pa	14 days ago
dev.bank.by	15 days ago
backoffice.digital.bank.com.pa	16 days ago
contacts.bank.com	23 days ago
webmail.bank.com	23 days ago

Most Common	
● Cloudflare, Inc.	474
● Bank R	238
● Amazon.com, Inc.	142
● Microsoft Corporation	91
● Bank X	60
● Others	45

Least Common	
Telefonica USA, Inc.	3
Aktivnie Tehnologii LLC	2
Columbus Networks Panama	2
HostDime.com, Inc.	2
LINKdotNET Telecom Limited	2

Most Common		
● Port 443	HTTPS	909
● Port 80	HTTP	897
● Port 2082	INFOWAVE	529
● Port 2083	RADSEC	528
● Port 2087	ELI	528
● Others		95

Least Common		
Port 5901	No data	25
Port 7999	IRDMI2	25
Port 9160	APANI1	25

Attack Surface Intelligence provides complete and persistent oversight of external assets to support exposure reduction across the business

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,700 businesses and government organizations across more than 75 countries.

www.recordedfuture.com @RecordedFuture