eSENTIRE

SOLUTION BRIEF

Multi-Signal Managed Detection and Response for Financial Services

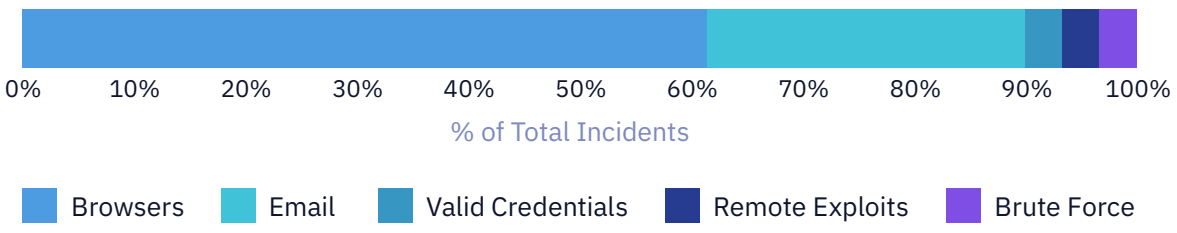
Whether for monetary gain or to disrupt business operations, cybercriminals have made financial organizations a top target. This can result in millions of dollars in fines and lost revenue, an incalculable amount of damage to your financial firm's reputation, and even general destabilization of the economy. While most financial organizations recognize this and have strong preventative security controls in place, clever social engineering and one wrong click by an employee can open the door to your company's network.

Over the last 12 months, eSentire's Threat Response Unit (TRU) detected and responded to more than 76 incidents across our financial services clients. **In about 32% of these incidents, the attack progressed to a "hands-on" phase and only timely threat detection and response prevented a business disrupting event.**

Top financial services security challenges

1. A clear understanding of risk-based best practices
2. Lack of visibility into personal devices (BYOD)
3. Lack of internal resources and expertise
4. Compliance with regulatory requirements
5. Lack of visibility into IT and OT assets
6. Technical capabilities to identify and contain threats
7. Zero-day risks, often associated with global mega attacks
8. Lack of response plan and/or slow response to past incidents

Most common initial access vectors in attacks targeting financial services



Understanding the Threat Landscape for Finance Services

Based on TRU's observations about threats conducted against the finance sector, cybercriminals are increasingly using browser-based and email-based vectors to gain Initial Access into your environment. Once they have gained access, the threat actors can progress to performing Intrusion Actions and then Actions on Objectives to deploy ransomware or other infostealer malware.

The most common initial access vectors we observed in these incidents are:

- **Browsers (63%):** These threats are encountered when employees browse the web. TRU observed multiple threats, such as SocGholish, GootLoader, and SolarMarker, used as intrusion vectors against financial firms. However, SocGholish, a browser-based threat, was by far the most common intrusion vector observed.
- **Email (29%):** These threats arrive in email inboxes disguised as typical business communications with subjects like “Invoice” and “Signature Required.” To bypass email filters, these malware strains often wrap malicious documents (e.g., Word or Excel files that use macros to execute malicious commands) and other files (e.g., LNK, ISO) in a password-protected .zip archive. To increase the chances of a user unwittingly aiding the attacker, several malware strains (e.g., Qakbot and IcedID) are known to hijack and replay older email threads, sometimes from known business partners.
- **Valid Credentials (3%):** Malware that rely on harvesting credentials were another top choice for threat actors to gain initial access into corporate environments. These malware included infostealers, built to find and exfiltrate credentials, banking information, browsing history, and more, as well as banking trojans, which are now augmented with functionality to collect information that can help threat actors to prioritize high-value.
- **Remote Exploits (3%):** These attacks are performed against vulnerable Internet-facing infrastructure, including web servers, email servers, VPN services, and even workstations exposed directly to the Internet. There is a constant onslaught of outdated attacks exploring most IP space at any given time, a malicious element of what’s known as Internet Background Radiation.
- **Brute Force (3%):** This is a type of sub-technique under the Credential Access tactic, as mapped by the MITRE ATT&CK Framework, in which threat actors may use a bot or a form of repetitive, iterative mechanism to guess the password.

$228,589

Average daily cost of downtime for finance organizations with 500 employees

204 DAYS

Average mean time to identify (MTTI) a data breach

$5.9 MILLION

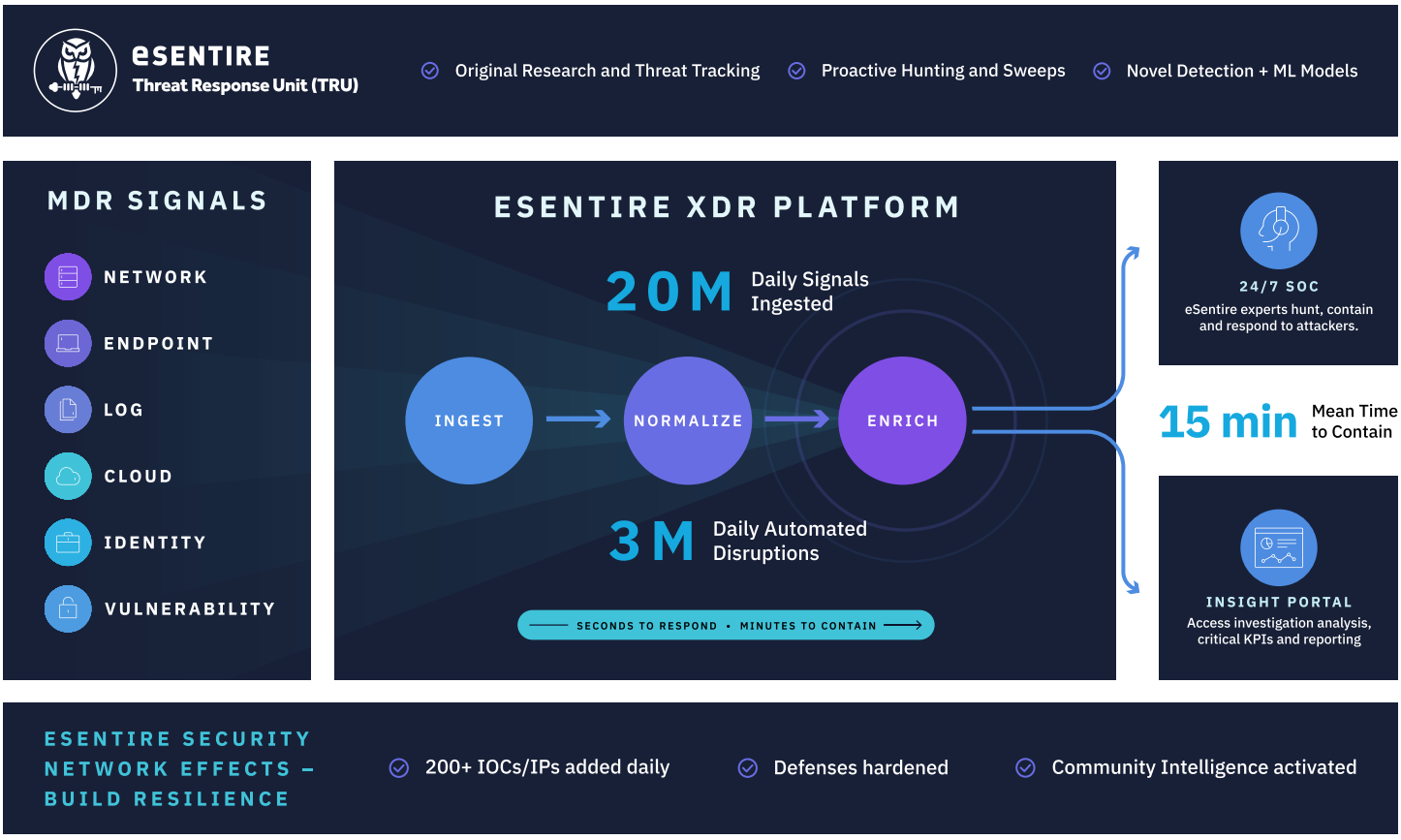
Average cost of a data breach for the global finance sector

eSentire Has Been Protecting Financial Services Companies for 20+ Years

We are recognized globally as The Authority in Managed Detection and Response (MDR) because we hunt, investigate, and stop cyber threats before they become business-disrupting events. In fact, eSentire was founded in 2001 to secure the environments of the world's most targeted industry - financial services. Now with 2000+ customers, across 80+ countries globally, we have scaled to deliver cybersecurity services across highly regulated industries, with a proven track record of success supporting credit unions, banks, mortgage brokerages, hedge funds, and private equity firms. We protect over 250,000 employees across over 400 financial customers.

Our team of 24/7 Cyber Analysts and Elite Threat Hunters don't drown you in alerts. We have a successful track record of identifying new threats, stopping nation state attacks, and preventing ransomware gangs from shutting down business operations & creating damaging public incidents.

At eSentire, we are proud to go beyond the response capabilities of other MDR providers to deliver results. We support your cyber program with a combination of cutting-edge machine learning XDR technology, 24/7 Threat Hunting expertise and security operations leadership to mitigate your business risk, enable security at scale, and drive your cyber program forward.



ESENTIRE SECURITY NETWORK EFFECTS – BUILD RESILIENCE

- 200+ IOCs/IPs added daily
- Defenses hardened
- Community Intelligence activated

ULTIMATE FLEXIBILITY: ON PREMISES | CLOUD | HYBRID | BYOL | FULLY MANAGED SOLUTION

Network	Endpoint	Log	Cloud	Identity	Additional Visibility + Context Assets, MVS + Dark Web Monitoring
eSENTIRE Proprietary Technology	CROWDSTRIKE vmware Carbon Black Microsoft SentinelOne AGENT	sumo logic Microsoft	aws Microsoft Google Cloud LACEWORK	eSENTIRE Proprietary Technology Microsoft	eSENTIRE Proprietary Technology tenable cybersixgill

How eSentire Protects Financial Firms

Key Challenges	eSentire MDR	eSentire Exposure Management + Incident Response Services

A clear understanding of risk-based best practices	N/A	• CISO and Advisory Services
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management

Lack of visibility into personal devices (BYOD)	• eSentire MDR for Log	• eSentire Managed Vulnerability Service • CISO and Advisory Services • Vendor Risk Management

Lack of internal resources and expertise	• eSentire MDR for Network
	• eSentire MDR for Endpoint
	• eSentire MDR for Log
	• eSentire MDR for Cloud
		• eSentire Managed Vulnerability Service
		• CISO and Advisory Services
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management

Compliance with regulatory requirements	• eSentire MDR for Network
	• eSentire MDR for Endpoint
	• eSentire MDR for Log
	• eSentire MDR for Cloud
		• eSentire Managed Vulnerability Service
		• CISO and Advisory Services
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management

Lack of visibility into IT and OT assets	• eSentire MDR for Log	• eSentire Managed Vulnerability Service • CISO and Advisory Services • Vendor Risk Management
Technical capabilities to identify and contain threats	• eSentire MDR for Network • eSentire MDR for Endpoint • eSentire MDR for Log • eSentire MDR for Cloud	N/A
Zero-day risks, often associated with global mega attacks	• eSentire MDR for Network • eSentire MDR for Endpoint • eSentire MDR for Log • eSentire MDR for Cloud	• eSentire Managed Vulnerability Service • CISO and Advisory Services • Vendor Risk Management

Lack of response plan and/or slow response to past incidents	N/A	• Digital Forensics and Incident Response Services
		  • On-Demand 24/7 Retainer
		  • Incident Response Plan Development
		  • Incident Plan Assessment

Helping your organization meet regulatory requirements

The federal government imposes stiff penalties for non-compliance with regulatory rules regarding cybersecurity. Oversight is expected to increase, putting additional pressures on constrained security teams. Our MDR and Exposure Management Services are designed to help you navigate the complexity of GLBA, SOX, NYCRR, and PCI DSS standards and put in place corrective controls.

Experience the eSentire difference

At eSentire, we go beyond the market's capability in threat response. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, identity, and vulnerability data that enables complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. With two 24/7 Security Operations Centers staffed with cyber experts and Elite Threat Hunters, an industry-leading XDR Cloud Platform, and refined security operations processes, eSentire can detect and respond with a Mean Time to Contain of 15 minutes.

23+
Years in operation

2000+
Customers in 80+ Countries

Protecting
250,000
employees across 400+ financial customers

100%
Deployment Satisfaction

$6.5T+
Total AUM

	Support	eSentire	The Other Guys
Multi-Signal Visibility	MDR - Detection	✓	Not always multi-signal
Rapid Human-Led Investigations	MDR - Detection	✓	✓
Containment in 15 Minutes	MDR - Response	✓	Inconsistent MTTC
Automated Response Driven by XDR Platform	MDR - Response	✓	✓
Endpoint Threat Containment	MDR - Response	✓	✓
Quarantine Files	MDR - Response	✓	You're Responsible
Hash Blocking	MDR - Response	✓	You're Responsible
Account and Access Suspension	MDR - Response	✓	You're Responsible
Network Isolation	MDR - Response	✓	You're Responsible
Blocking Compromised Email Accounts	MDR - Response	✓	You're Responsible
Terminate Malicious Processes	MDR - Remediation	✓	You're Responsible
Facilitated Retroactive Email Purges	MDR - Remediation	✓	You're Responsible
System Reboot	MDR - Remediation	✓	You're Responsible
Removal of Registry Keys/Values	MDR - Remediation	✓	You're Responsible
Threat Eradication	MDR - Remediation	✓	You're Responsible
Root Cause Analysis	eSentire MDR and DFIR	✓	Limited
Digital Forensics Analysis	DFIR	✓	Limited
Crime Scene Reconstruction	DFIR	✓	Limited
E-Discovery	DFIR	✓	Limited

Ready to Get Started?

Reach out to connect with an eSentire security specialist and build a more resilient security operation today.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH, CONTACT US 1-866-579-2200

eSENTIRE