SOLUTION BRIEF

Focus on Cybersecurity: Financial Services

Whether for monetary gain or to disrupt business operations, cybercriminals have made financial organisations a top target. A cyberattack can compromise systems that drive operations and can expose clients' personal financial data. This can result in millions of dollars in fines and lost revenue, an incalculable amount of damage to a financial firm's reputation and even general destabilisation of the economy. While most financial organisations 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 a company's network.

Financial services firms are 300 times more likely to be attacked than other companies, according to a report by the Boston Consulting Group.[1] Finance and insurance companies tend to experience a higher volume of attacks relative to other industries and have been the most attacked industry for four consecutive years, according to the IBM X-Force Threat Intelligence Index, accounting for 17 percent of all attacks.[2]

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

Types of cyberattacks experienced by financial services[3]

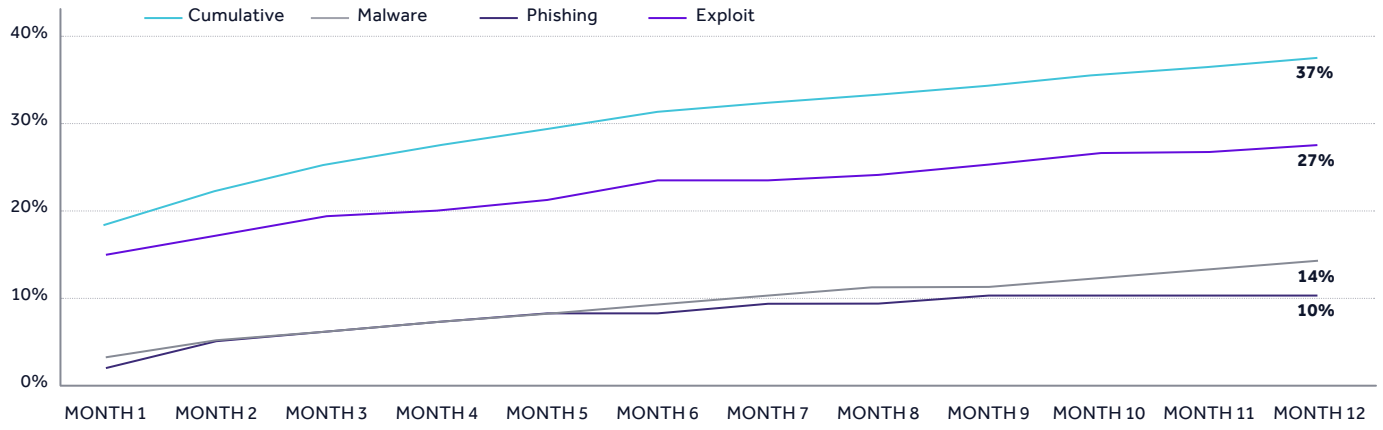
Malware	97%
Phishing and social engineering	76%
Web-based attacks	82%
Botnets	64%
Malicious code	60%
Denial of service	52%
Stolen devices	40%
Ransomware	45%
Malicious insider	34%

[1] *Global Wealth 2019: Reigniting Radical Growth, Boston Consulting Group (BCG)*
[2] *The annual IBM X-Force® Threat Intelligence Index, 2020*
[3] *Ninth Annual Cost of Cybercrime Study, Ponemon*

eSentire: Observing risks to the financial industry for two decades

We understand the unique challenges your cybersecurity team faces. For two decades, we've seen the dynamic nature of threats that specifically target financial organisations and their partners. For example, in 2019 our Security Operation Centres (SOCs) detected an alarming number of threat actors that were able to bypass financial service providers' existing security controls. Based on eSentire SOC data, the below chart shows that for every additional location, the risk of an incident getting past your traditional security controls significantly increases.

Observed probability of one or more security events due to a bypass of existing security controls per location



Financial services firms are hit by security incidents 300 times more frequently than businesses in other industries, as attackers focus on targets that will give them the biggest return on their investment.[4] And since financial organisations regularly handle highly sensitive personal financial information (such as home addresses and banking information), failing to maintain compliance and protect customer data can be disastrous for a company. The financial industry has experienced a 3x increase in the number of breaches since 2016.[5]

Data breach costs are the second highest amongst observed industries[6], due to the complicated nature of the way financial companies conduct business and their high value as a target to sophisticated cyberattackers. Meanwhile, cybersecurity teams continue to see rising timeframes to identify and contain security incidents, further underscoring the need for a tight security program.

3 to 1
ratio of attacks vs. other industries

3X
increase in number of breaches since 2016

$5.86M
average cost of a data breach

$210
average cost per record lost

177 DAYS
mean time to identify

56 DAYS
mean time to contain

Top three financial industry breaches in 2018

SunTrust Banks
↓
1.5M
records exposed

Guaranteed Rate
↓
188,000
records exposed

RBC Royal Bank
↓
66,000
records exposed

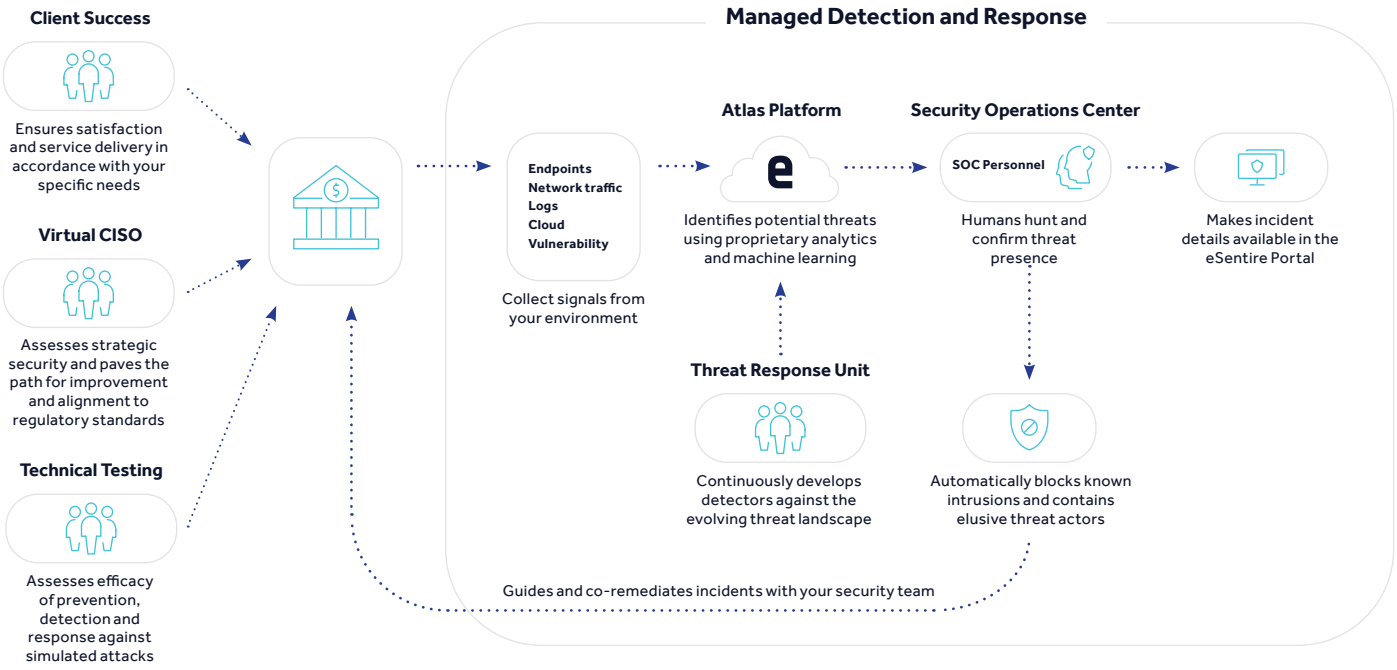
[4] *https://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks/*
[5] *https://www.globenewswire.com/news-release/2018/10/02/1588510/0/en/Bitglass-2018-Financial-Services-Breach-Report-Number-of-Breaches-in-2018-Nearly-Triple-That-of-2016.html*
[6] *2019 Ponemon Cost of a Data Breach Report*

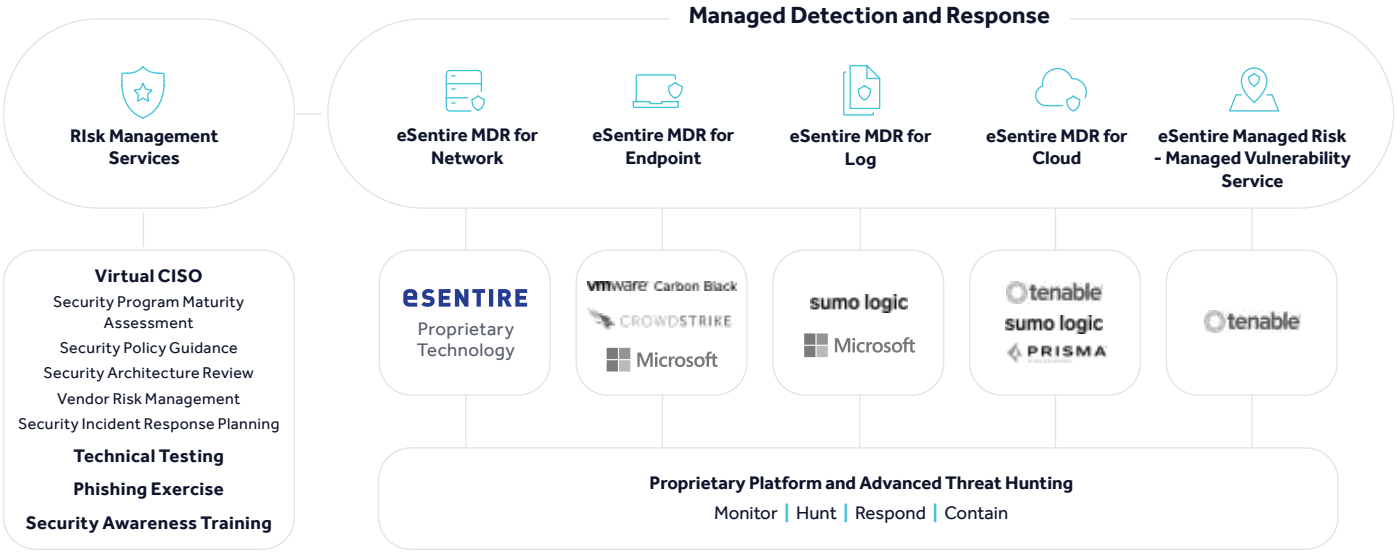
A comprehensive approach to protecting financial companies

Whether your organisation is a hedge fund, small credit union, a bank or a large financial services organisation with multiple facilities, threat actors are going to capitalise on vulnerable systems and human nature. Ultimately, the difference between business protection and business disruption will come down to the speed at which you can identify and contain an attack.

At eSentire, our comprehensive approach helps organisations test, mature, measure and protect customers' environments from a multitude of risk factors. Our Managed Detection and Response (MDR) services rapidly identify and contain threats that bypass traditional security controls. Ingesting signals from your on-premises, cloud and hybrid environments, we combine endpoint, network, log, vulnerability and cloud data to identify known and elusive threats.

Averaging 20 minutes from identification to containment, we ensure attackers don't have the time to achieve their objectives. Our managed risk programs test your existing defences against simulated attacks, assess and measure your security posture and pave a path for resiliency that aligns to regulatory frameworks. All of these services are supported by a dedicated team focused on delivering in accordance with your organisation's unique requirements and business objectives.





eSentire service alignment to the finance industry's top challenges

	eSentire Managed Detection and Response	eSentire Managed Risk Programs

A clear understanding of risk-based best practices	N/A	• Virtual CISO
		  • 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 Risk - Managed Vulnerability Service	• Virtual CISO • Vulnerability Management Program

Lack of internal resources and expertise	• eSentire MDR for Network
	• eSentire MDR for Endpoint
	• eSentire MDR for Log
	• eSentire MDR for Cloud
	• eSentire Managed Risk - Managed Vulnerability Service
		• Virtual CISO
		  • 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 Risk - Managed Vulnerability Service
		• Virtual CISO
		  • 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 Risk - Managed Vulnerability Service	• Virtual CISO • Vulnerability Management Program
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 Risk - Managed Vulnerability Service	• Virtual CISO • Vulnerability Management Program
Lack of response plan and/or slow response to past incidents	N/A	• Virtual CISO • Security Incident Response Planning

Helping your organisation meet regulatory requirements

The government and financial authorities impose 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 Managed Risk Programs are designed to help you navigate the complexity of GDPR, FCA, PRA, ISO/IEC 27001, PSD 2 standards and put in place corrective controls.

Experience the eSentire difference

Organisations all over the world trust eSentire as their last line of defence and trusted advisor against an overwhelming threat landscape. Our 92 percent client retention rate is testament to delivering on our core mission: a client's network can never be compromised. Our specialised teams that deliver and support our services are consistently developing the latest methods that ensure your organisation is protected against the latest threat actors and aligned to stringent regulatory requirements that keeps your patients, employees and systems safe from disruption.

20+
Years in operation

1000+
Global customers

Across 6 continents

In 70+ countries

92%
Customer retention rate

$6.5T
in assets under management

	eSentire MDR	Other MDR
24x7 always on monitoring	✓	Limited
Full spectrum visibility (PCAP, Endpoint, Log, Vulnerability, Cloud)	✓	Limited
Detection utilising signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioural analytics	✓	Limited
Continuous elite threat hunting	✓	✗
Alerting of suspicious behaviour	✓	Limited
Alerts	✓	✓
Confirmation of true positive	✓	Limited
Remediation recommendations	✓	✓
Tactical threat containment on client's behalf	✓	Limited
24x7 investigation and SOC support	✓	✗ Need IR Retainer
Incident response plan	✓	✗ Need IR Retainer
Remediation verification	✓	✗ Need IR Retainer

"eSentire has a proven track record that has provided security services for my firm for several years. They have a top notch SOC and a very good product platform that keeps up with the cybersecurity advancements being made."
-- Engineer, financial services company

"eSentire has helped protect my business by building a system that can accurately filter traffic to allow human eyes the time and data necessary to protect my network."
-- IT Director, small business financial services company

If you're experiencing a security incident or breach contact us (0)8000 443242

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.