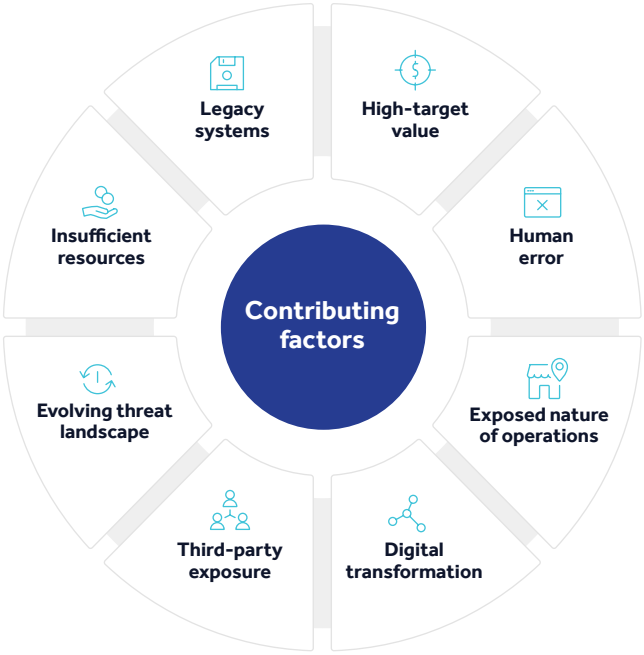
SOLUTION BRIEF

Focus on Cybersecurity: Architecture, Engineering and Construction

The architecture, engineering and construction industries are increasingly reliant on technology and the use of online networks to share project/client data and connect to third-party supplier networks, often doing so remotely from job sites. Technology has replaced paper documents for business-critical information like project drawings, purchase orders and permitting. For construction and related companies, costly assets are no longer just heavy equipment and materials, but the technology devices that fuel their operations.

With these advances come operational efficiency, but also risk. Often overlooked across the types of organizations cyber attackers target, companies in this space are quickly becoming a lucrative target due to the value of their data and susceptible nature of business operations. Confidential and proprietary information is digitally stored and shared across projects and their supply chains, which are often small businesses with limited, if any, resources devoted to IT security.



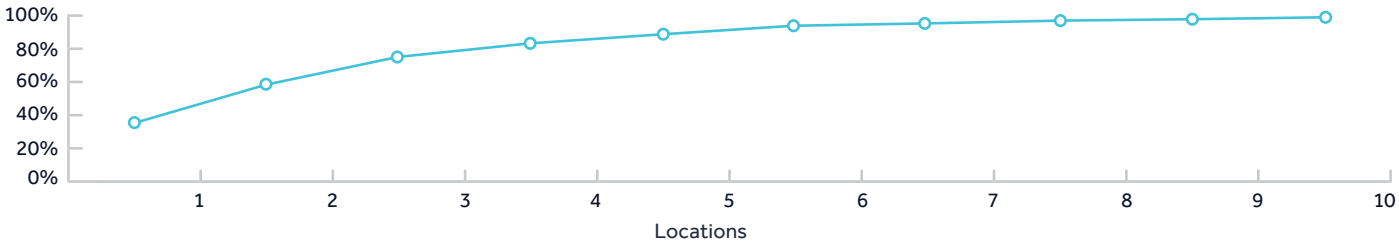
Top Construction-Related Industry Security Challenges

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. Risks of sharing data with supply chain partners
5. Lack of visibility into IT and OT assets
6. Technical capabilities to identify and contain threats
7. Exposure from conducting business on mobile devices in the field
8. Lack of response plan and/or slow response to past incidents

eSentire: Observing Risks Within the 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 the construction industry and their partners. Under resourced in the fight to protect their environment and users against a growing threat landscape, it's only a matter of time until attackers find a blind spot.

Based on eSentire SOC data, the below chart shows that for every additional location, the risk of an attacker bypassing your traditional security controls over a 12-month period significantly increases.[1]



Root Causes

54%
Malicious Attacks

23%
System Glitch

23%
Human Error

Construction and related firms are not highly regulated, and since they aren't an obvious target, there is little cybersecurity guidance out there. However, the threats exist as long as companies rely on technology and remote connectivity in order to conduct business. The construction and building business has always focused on physical security as job sites are often plagued by theft and vandalism, but failure to address cybersecurity threats can result in business disruption, unplanned costs and reputational damage if a breach occurs.

Costs of a data breach are the second highest amongst observed industries, 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

$5.2M[2]
average cost of a data breach

$160[3]
per record lost

220 DAYS[4]
mean time to identify a data breach

82 DAYS[5]
mean time to contain a data breach

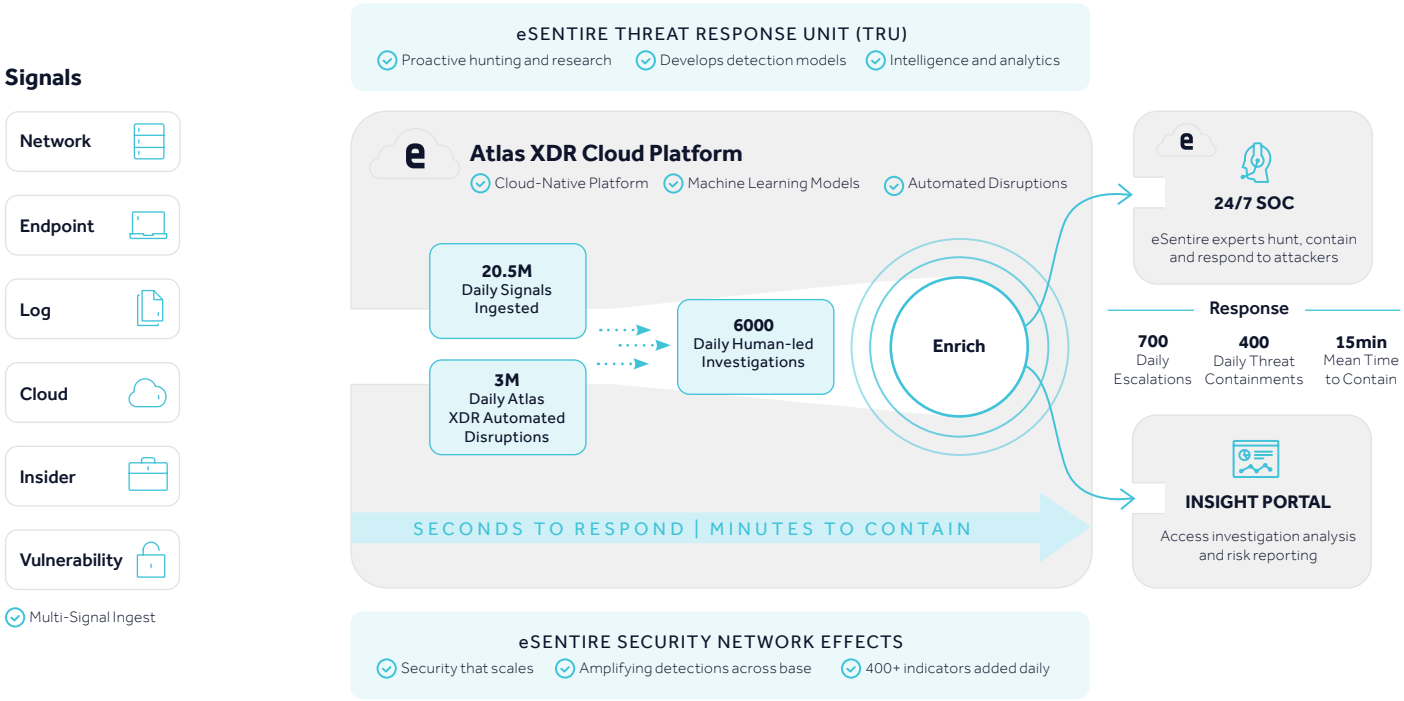
High Profile Industry Breaches

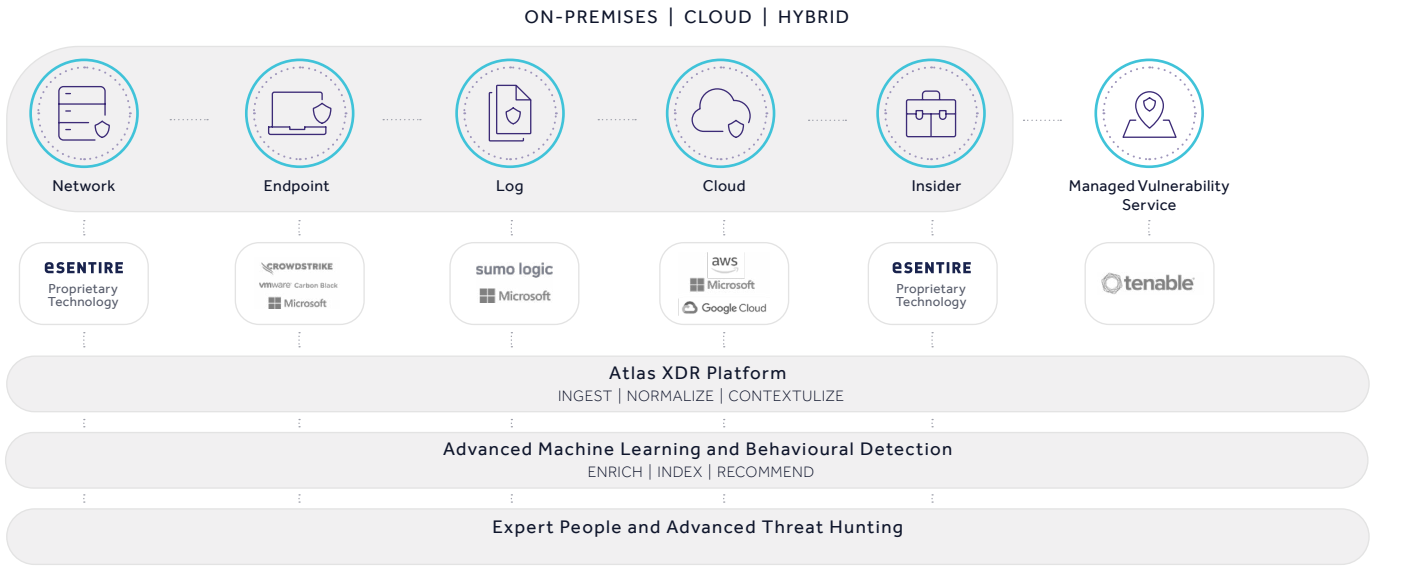
Bird Construction (Dec 2019), Maze Ransomware attack exposes 60 GBs of data
Bouygues Construction (Jan 2020), Ransomware attack exposes 200 GBs of data
Turner Construction (Mar 2016), Phishing scam exposes employee tax data

[1] Using data from more than 2,000 deployed eSentire sites, depicts risk rates for organizations that do not have a threat monitoring service in place. Statistical projections are based on the ongoing and cumulative chance attack categories would have been picked up by an eSentire Security Operations Center, which watches for things bypassing traditional security measures in unmonitored environments.
[2-5] 2019 Ponemon Cost of a Data Breach

A Comprehensive Approach to Protecting Construction-Related Companies

Whether your organization is a major construction firm, a small business home builder or a construction equipment renter, threat actors are going to capitalize 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 organizations test, mature, measure and protect their 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 defenses 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 organization's unique requirements and business objectives.





eSentire Service Alignment to the Top Challenges for Architecture, Engineering and Construction Companies

	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 Managment
Lack of visibility into personal devices (BYOD)	• eSentire MDR for Log • eSentire Managed Risk - Managed Vulnerability Service	Virtual CISO • Vulnerability Managment 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 Managment
Risks of sharing data with supply chain partners	• 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 Managment
Lack of visibility into IT and OT assets	• eSentire MDR for Log • ESentire Managed Risk - Managed Vulnerability Service	Virtual CISO • Vulnerability Managment 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
Exposure from conducting business on mobile devices in the field	• 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 • Security Architecture Review • Security Incident Response Planning • Vendor Risk Managment
Lack of response plan and/or slow response to past incidents	N/A	Virtual CISO • Security Incident Response Planning

Experience the eSentire Difference

Organizations all over the world trust eSentire as their last line of defense 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 specialized teams that deliver and support our services are consistently developing the latest methods that ensure your organization is protected against the latest threat actors and aligned to stringent regulatory requirements that keeps your clients, employees and systems safe from disruption.

20+
Years in operation

1200+
Global customers

Across **6** continents

In **75+** countries

92%
Customer retention rate

$6.5T
in assets under management

	eSentire MDR	Other MDR
Detection utilising signatures and IOCs	✓	✓
Alerts	✓	✓
Remediation recommendations	✓	✓
Continuous elite threat hunting	✓	✗
24/7 investigation and SOC support	✓	✗ Need IR Retainer
Incident response plan	✓	✗ Need IR Retainer
Remediation verification	✓	✗ Need IR Retainer
24/7 always on monitoring	✓	Limited
Full spectrum visibility (PCAP, Endpoint, Log, Vulnerability, Cloud)	✓	Limited
Detection of unknown attacks leveraging patterns and behavioural analytics	✓	Limited
Alerting of suspicious behaviour	✓	Limited
Confirmation of true positive	✓	Limited
Tactical threat containment on client's behalf	✓	Limited

What eSentire customers are saying

"The quality of the service is great value from a cost perspective. There's no way I can put together a security team to deal with the same threats at the same cost—I see eSentire as an augmentation of our team."

Vice President, Director of Information Technology, Large Architectural Firm

"eSentire has helped protect my business by being able to collect information from various sources and quickly filter to find the real threats."

Network Administrator, Medium Enterprise Construction Company

"eSentire has helped protect my business by bringing in best of breed tools to Manage detect and respond with a top tier eyes-on-glass SOC."

Director, Large Enterprise Construction Company

Get Started

If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries 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**.