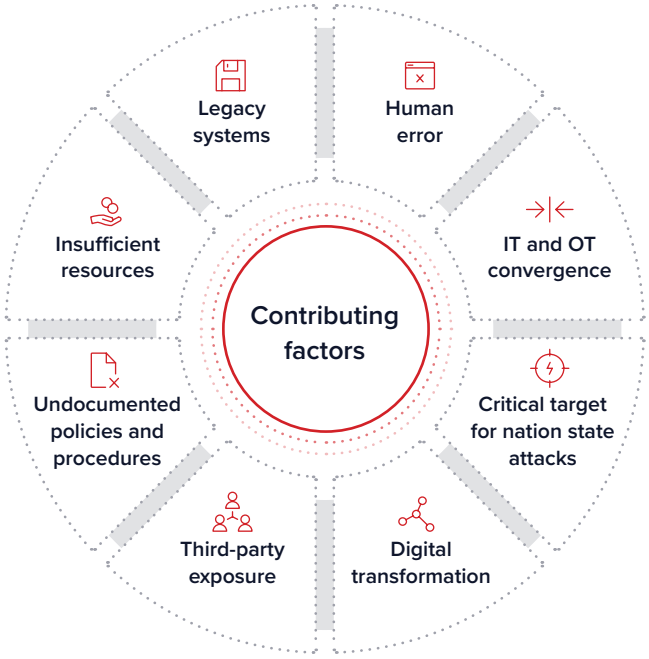
SOLUTION BRIEF:

Focus on Cybersecurity: Energy and Utilities

Effective April 1st, 2020, the regulatory body for power and utility entities in North America (NERC) increased standards for Critical Infrastructure Protection (CIP). These standards are in response to a rapidly evolving threat landscape that compromised 56% of energy and utility providers over the last 12 months.[1] The high convergence of information and operational technologies, and the evolving threat landscape will only increase the pressure on constrained cybersecurity resources. These challenges will be exacerbated by the nature and sophistication of energy and utility attackers that are not only financially motivated but politically driven. Even though only 42% of organizations rate their cyber readiness as high, only 31% of those organizations rate their readiness to respond and contain a threat as high.[2] As energy and utility providers look to bridge the gap, a holistic approach that matures prevention, detection, response and recovery capabilities will be critical in mitigating risk to an increasingly susceptible sector of critical infrastructure.



Top Energy and Utility Security Challenges

1. A clear understanding of risk-based best practices
2. Lack of visibility into IT and OT assets
3. Technical capabilities to identify and contain threats across IT and OT
4. Zero-day risks, often associated with global mega attacks or industrial safety events
5. Lack of internal resources and expertise
6. Lack of alignment between OT and IT
7. Lack of a response plan and a slow response to past incidents
8. Compliance and regulatory regimes

[1] *Ponemon, Are utilities keeping up with the industrial cyber threat?*
[2] *Ponemon, Are utilities keeping up with the industrial cyber threat?*

eSentire: Observing Risks to the Energy and Utility Providers 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 energy and utility providers. In 2019, Energy and Utility companies saw an increase in incidents bypassing their traditional technologies at an alarming rate. For example, in 2019 our Security Operation Centers (SOCs) detected an alarming number of threat actors that were able to bypass energy and utility provider's existing security controls. Based on eSentire SOC data, the below chart shows that for every additional location, the risk of an incident getting passed your traditional security controls significantly increases. .

Locations	1	2	3	4	5	6	7	8	9
The probability of an incident bypassing traditional security controls	43%	67%	81%	89%	94%	96%	98%	99%	99%

And, industry reports indicate that a quarter of these incidents convert to data disclosure. This is due to the speeds at which attackers have reported they can breach the perimeter, identify critical data and exfiltrate before their presence is identified.

Unfortunately, the financial consequences of data disclosure have proven devastating. Detection and escalation, notification, post breach and lost business costs are the third highest amongst observed industries. Due to the sophisticated nature of energy and utility attackers and a multitude of contributing factors, cybersecurity teams continue to see rising timeframes to identify and contain security incidents.

73% Of attackers can breach the perimeter of energy and utility providers and exfiltrate data in 25 hours or less[3]

25% Conversion rate of security events to data disclosure for organizations that operate IoT and OT systems[4]

$165 per record lost[5]

$5.6M average cost of a data breach[6]

- **$2.02M** in lost business cost[7]
- **$1.74M** in detection and escalation costs[8]
- **$1.53M** in post breach costs[9]
- **$302K** in notification costs[10]

197 DAYS Mean time to identify[11]

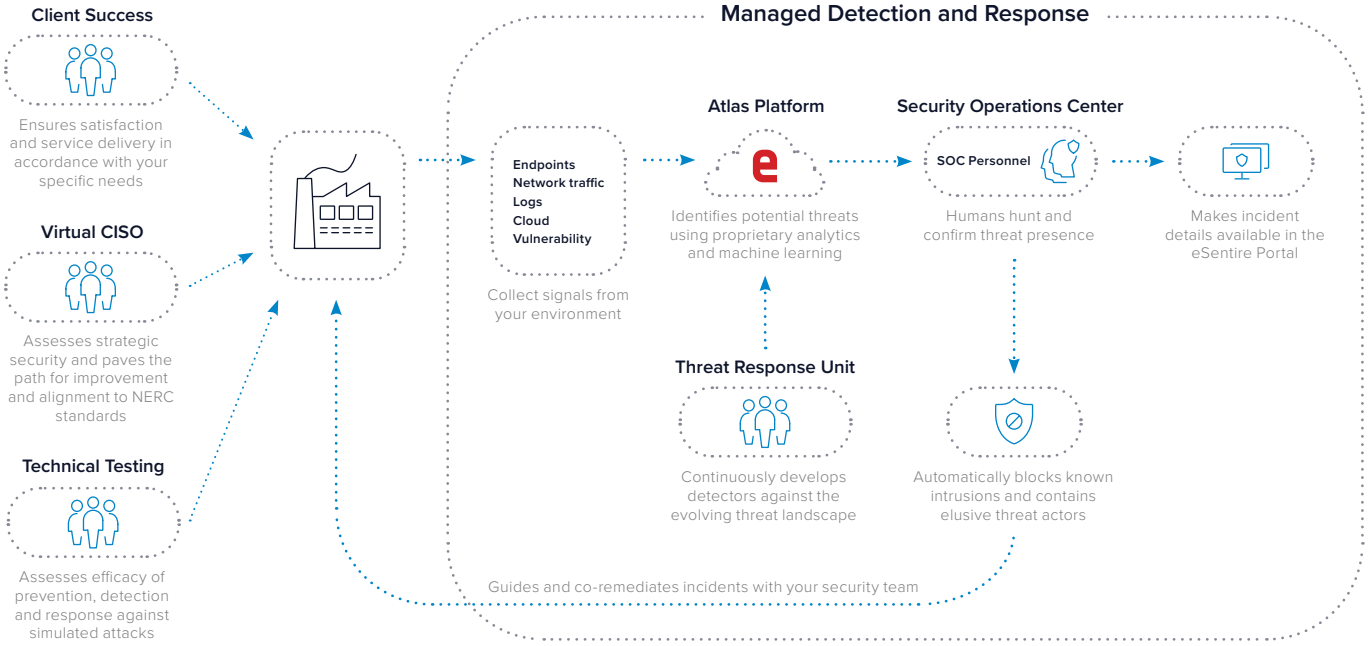
57 DAYS Mean time to contain[12]

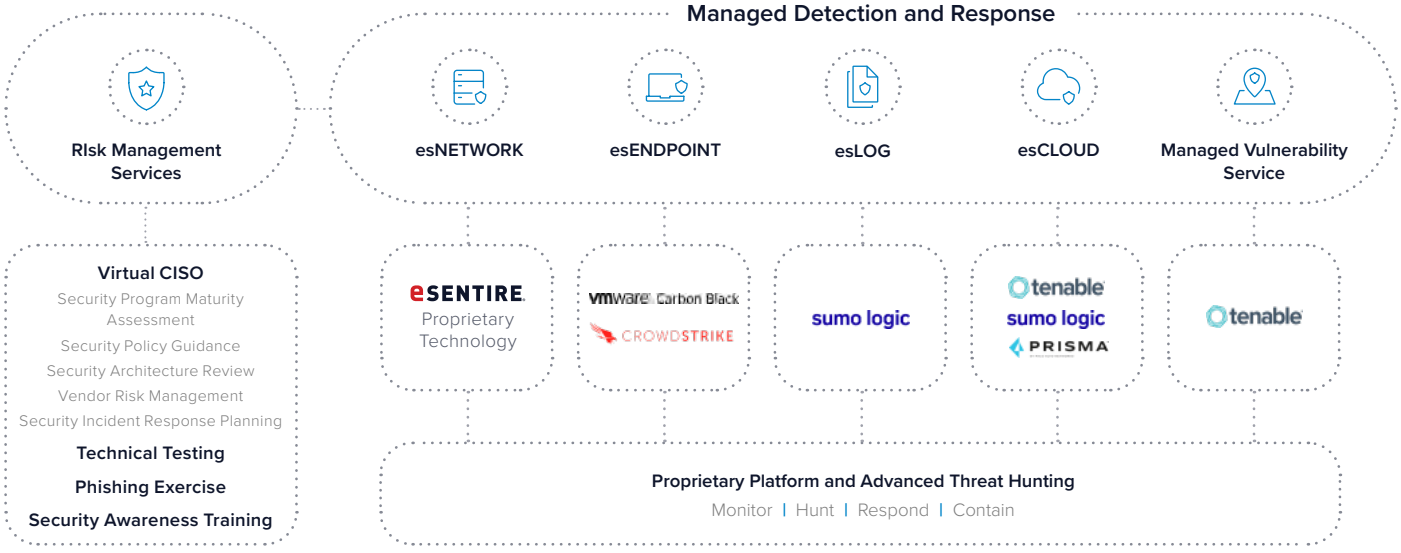
[3] *Nuix Black Report, 2018*
[4] *Verizon DBIR Report, 2019*
[5] *Ponemon Cost of a Data Breach Report, 2019*
[6] *Ponemon Cost of a Data Breach Report, 2019*
[7] *Ponemon Cost of a Data Breach Report, 2019*
[8] *Ponemon Cost of a Data Breach Report, 2019*
[9] *Ponemon Cost of a Data Breach Report, 2019*
[10] *Ponemon Cost of a Data Breach Report, 2019*
[11] *Ponemon Cost of a Data Breach Report, 2019*
[12] *Ponemon Cost of a Data Breach Report, 2019*

A Comprehensive Approach to Energy and Utility Protection

Whether your organization is a national or regional entity, threat actors are going to capitalize on vulnerable systems and human nature. Ultimately, the difference between organizational protection and potential 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, hybrid and OT 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 risk management services test your existing defenses against simulated attacks, assess and measure your security posture and pave a path for resiliency that aligns to NERC requirements. 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 Energy and Utility Provider's Top Challenges

	eSentire Managed Detection and Response	eSentire Risk Management Services

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 IT and OT assets	• esLOG • Managed Vulnerability Service (MVS)	• Virtual CISO • Vulnerability Management Program
Technical capabilities to identify and contain threats across IT and OT	• esNETWORK • esENDPOINT • esLOG • esCLOUD *Limitations across OT technologies	N/A
Zero-day risks, often associated with global mega attacks or industrial safety events	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service	• Virtual CISO • Vulnerability Management Program

Lack of internal resources and expertise	• esNETWORK
	• esENDPOINT
	• esLOG
	• esCLOUD
	• Managed Vulnerability Service
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management

Lack of alignment between OT and IoT	N/A	• Virtual CISO • Security Architecture Review
Lack of response plan and a slow response to past incidents	N/A	• Virtual CISO • Security Incident Response Planning

Compliance with regulatory regimes	• esNETWORK
	• esENDPOINT
	• esLOG
	• esCLOUD
	• Managed Vulnerability Service
		• Virtual CISO
		  • Security Program Maturity Assessment
		  • Security Policy Guidance
		  • Security Architecture Review
		  • Security Incident Response Planning
		  • Vendor Risk Management

Helping Your Organization Meet NERC Requirements

Since 2009, NERC has served as the regulatory body that specifies the minimum security requirements for the bulk power systems. CIP standards are made up of rules and sub-requirements that require organizational, operational, and procedural controls to identify gaps and mitigate risk against growing cyberattacks.

NERC - Critical Cybersecurity Infrastructure Reliability Standards

Standard	Title of Standard	Purpose	Applicable eSentire Services
CIP - 002	BES Cyber System Categorization	Identify and categorize cyber systems and associated cyber assets	Managed Risk Programs - Virtual CISO
CIP - 003	Cyber Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber systems against compromise which could lead to misoperation or instability.	Managed Risk Programs - Virtual CISO
CIP - 004	Personnel and Training	Require an appropriate level of personnel risk assessment, training and security awareness.	Managed Risk Programs - Virtual CISO
CIP - 007	System Security Management	Manage system security by specifying select technical, operational and procedural requirements in support of protecting BES cyber systems against compromise.	Managed Risk Programs - Virtual CISO
CIP- 008	Incident reporting and response planning	Mitigate the risk to reliable BES systems as a result of a cyber incident by specifying incident response requirements.	Managed Risk Programs - Virtual CISO
CIP - 010	Configuration change management and vulnerability	Prevent and detect unauthorized changes to BES cyber systems by specifying configuration change management and vulnerability assessment requirements to protect from compromise.	Managed Vulnerability Service
CIP - 011	Information Protection	Prevent unauthorized access to BES system information by specifying information protection requirements to protect BES from compromise.	Managed Detection and Response

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 97 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 NERC requirements that keeps your stakeholders, employees and systems safe from disruption.

97%
CUSTOMER RETENTION RATE

750+
GLOBAL CUSTOMERS

ACROSS **6**
CONTINENTS

IN **48**
COUNTRIES

6+
INVESTIGATIONS EVERY MINUTE

640+
CONFIRMED SECURITY INCIDENTS A DAY

	eSentire MDR	PSEUDO 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 helped protect my business by detecting and responding to threats in a timely manner."
>
> -- **IT Manager,** Small Energy and Utilities Company

Ready to get started? We're here to help.

Reach out schedule a meeting to learn more about MDR

eSENTIRE

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $6 trillion AUM, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, **visit www.esentire.com** and follow **@eSentire**.