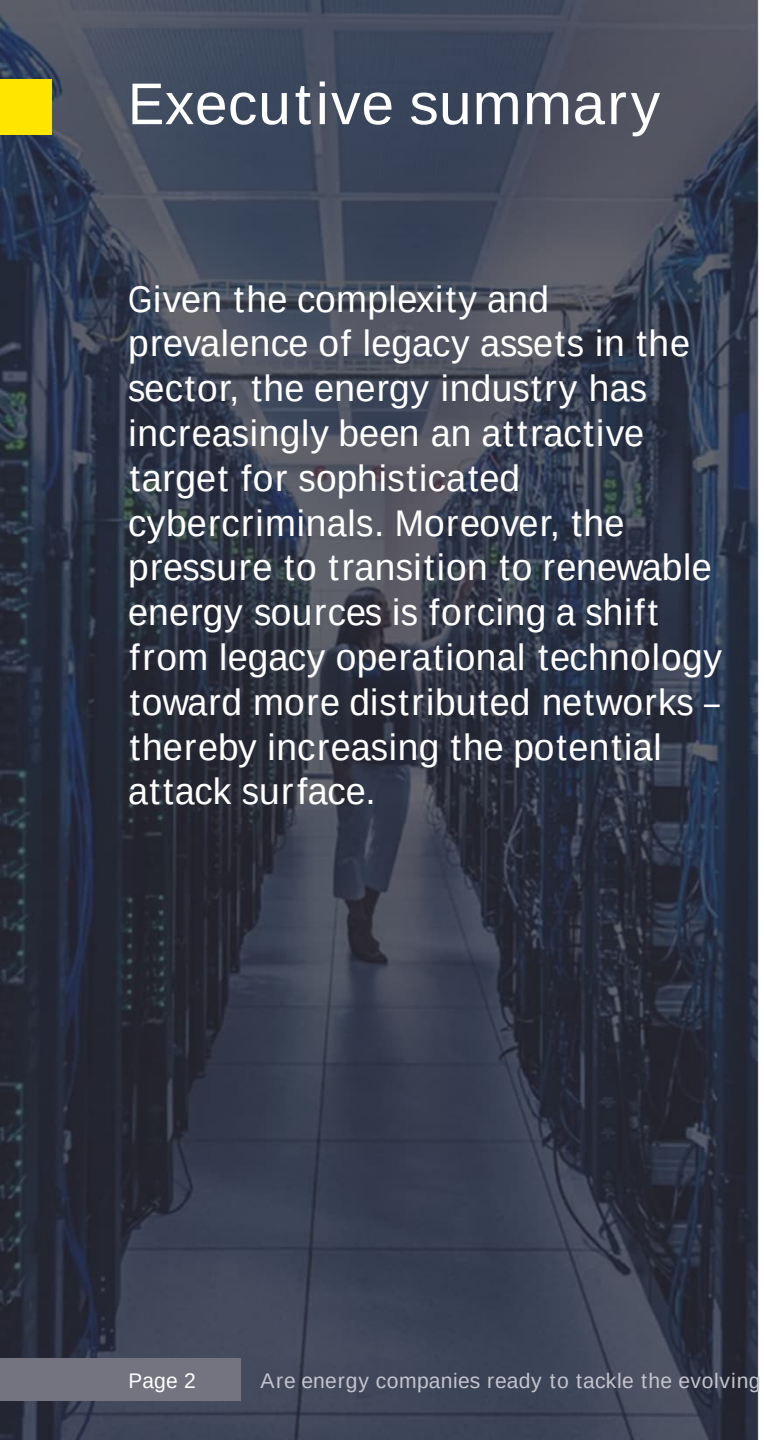

Are energy companies ready to tackle the evolving cyber threats?
Embed trust in your digital business with the EY organization and Microsoft
The better the question. The better the answer.
The better the world works.
EY
Building a better working world
Microsoft

Executive summary



Given the complexity and prevalence of legacy assets in the sector, the energy industry has increasingly been an attractive target for sophisticated cybercriminals. Moreover, the pressure to transition to renewable energy sources is forcing a shift from legacy operational technology toward more distributed networks – thereby increasing the potential attack surface.

Almost every energy company has embarked on a digital transformation journey. The companies have been making significant investments in information technology (IT) and operational technology (OT), including capitalizing on big data and analytics, artificial intelligence (AI), cloud, and Industrial Internet of Things (IIoT) to modernize infrastructure and deliver efficiencies and optimize costs.

However, embracing new technologies and connecting them to legacy systems makes the IT and OT environment difficult to protect.

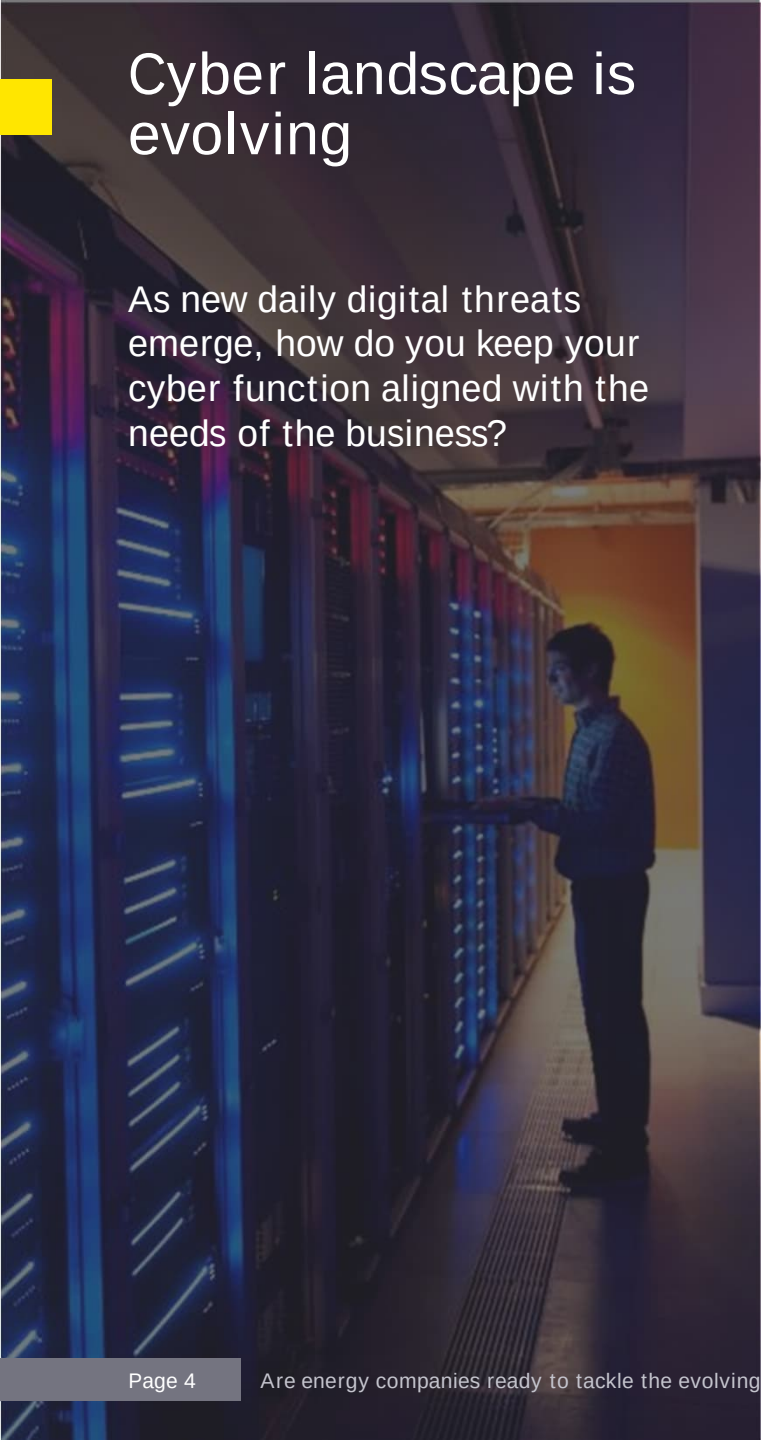
Modernization efforts, driven by digital transformation, have led to the integration of legacy systems with newer technologies, which have escalated security vulnerabilities with the rise in access points for the attackers. Wider adoption of emerging technologies, such as cloud computing at scale and IoT, have increased the openings for cybersecurity breaches, causing disruption of services, damage to equipment, data breaches, and potential threats to public safety and national security.

Therefore, to mitigate the growing cyber risk, energy companies need to build in cybersecurity resilience into every facet of their organization.

Together, the EY organization and Microsoft offer a proven solution to help:

- Identify and better respond to cyber risks.
- Meet changing regulatory and compliance requirements.
- Take informed risks to accelerate transformation and innovation.
- Embed “security-by-design” from the onset.

Contents



Cyber landscape is evolving

As new daily digital threats emerge, how do you keep your cyber function aligned with the needs of the business?

Energy companies today are larger and more globally oriented, with complex infrastructures, systems and processes. This makes cybersecurity a very real and ongoing challenge.

Digital transformation, combined with the transition to clean energy sources is driving energy transition across the world. Thereby, forcing energy companies to shift from legacy operational technology toward more distributed networks, enabled by IIoT, cloud and other technologies.

Wider adoption of digital technologies and deeper supply chain have increased the potential openings for cyber breaches. Moreover, given its status as critical national infrastructure, energy companies face tightening regulatory and compliance standards to ensure resilience against attacks and cyber breaches.

Current trends in cyber threats and attacks:

- Increasing state-sponsored cyber attacks on critical national infrastructure
- Emerging technologies and deeper supply chain increasing the attack surfaces
- Phishing and malicious activities to hack and disrupt business operations
- Data breaches, extortion or information theft leading to brand damage

75%

increase in known cyber attacks in the last five years, with energy sector being the fourth most targeted industry.

69%

of energy cybersecurity leaders believe that cloud-at-scale and IoT will pose the biggest cybersecurity risk in the next five years.

Source: EY Cyber Leadership Survey 2023.

Cyber landscape is evolving

Energy companies need to integrate cybersecurity into all aspects of their business operations, including the critical OT and IIoT affecting their core operations.

Only 35% of energy respondents say their organization is well-positioned to take on the threats of tomorrow, compared with 48% of other industries.

Source: EY Cyber Leadership Survey 2023.

Most forward-looking energy companies want to be able to take informed risks to accelerate their transformation and pursue innovation. However, they can't always trust if their current cyber setup will provide the security they need.

A first step is to understand the current cybersecurity program and assess the company's ability to respond to significant disruptions. Reviewing progress toward current state must be done regularly, combined with metrics and KPIs to demonstrate progress.

Key considerations for energy companies:

1. Simplify cyber technology stack.
2. Develop a robust governance structure.
3. Adopt cyber risk quantification mechanism.
4. Develop a cyber-secure workforce.
5. View cybersecurity as a value driver.

How are you ensuring that security and resilience is built into emerging technology by design, and not just bolted on afterward? How will you embed "risk-thinking" ideology throughout the business, so every decision has factored in appropriate security measures?

Answering these questions can help you determine the gaps in your current approach and what strategic input and investments you would need to build cyber resilience.

The EY organization and Microsoft can help you on this journey.

Security and trust, better together

EY

- Leading-class business consulting, risk, process and change management services
- Deep industry knowledge and experience
- Over 7,000 cybersecurity practitioners across 150 countries
- Over 20 years of developing industry leaders in cybersecurity
- Currently, 63 cybersecurity centers across the globe
- Three dedicated OT and IoT Cybersecurity EY Wavespace labs in Singapore, Poland and Houston
- Over 30 platforms and assets to support EY Cybersecurity Managed Services

Microsoft

- A unified security portfolio that provides visibility across on-premise and cloud environments
- Security capabilities built into all products – from identity and access management to enterprise cloud protection
- Microsoft Azure Sentinel, providing a cloud-native security information and event manager platform to quickly analyze large volumes of enterprise data
- Consulting services integrated with the EY organization, offering broad technical experience across all Microsoft solutions

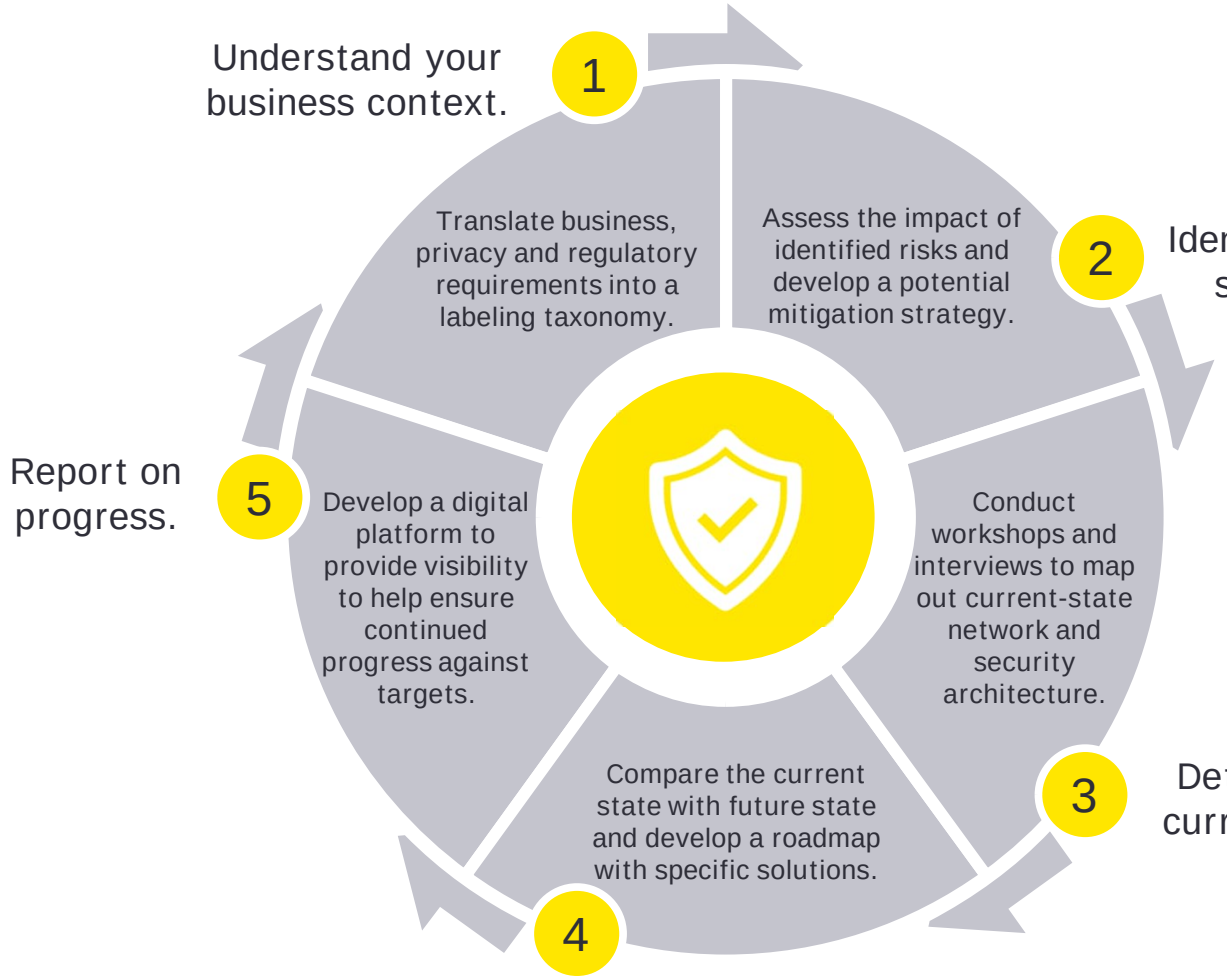
Unique value to you

Together, the EY organization and Microsoft will help realize the full potential of digital technology by securing the enterprise and enhancing business performance. This offering will:

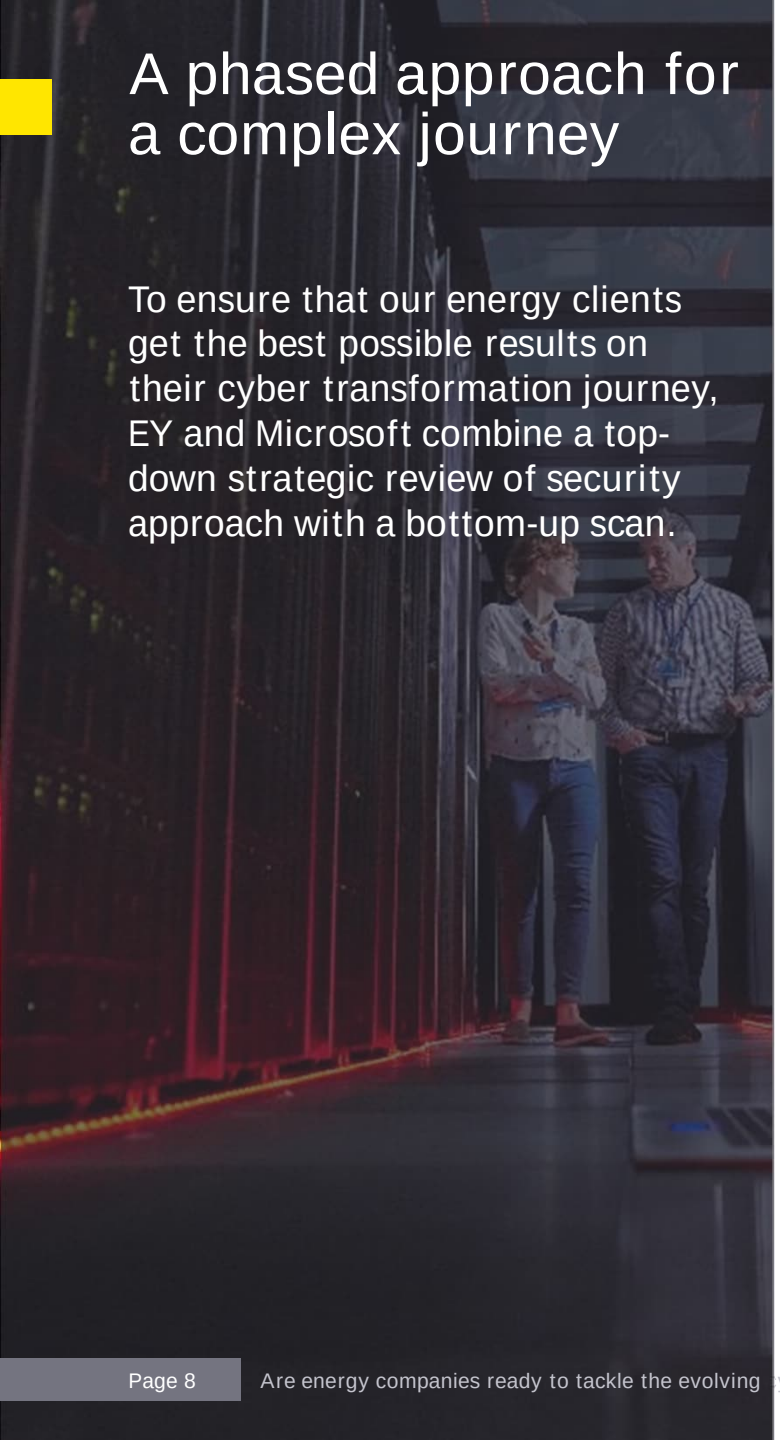
- Collect and analyse limitless security data from both on-premise and cloud environments.
- Expedite threat hunting, incident investigation and response times using built-in AI capabilities.
- Augment cyber teams with a provision of services from selection, integration, implementation and managed services.
- Extend the security operations center (SOC) capabilities and reach across your whole IT landscape.

A phased approach for a complex journey

The EY organization's approach to build "trust by design" principle is by continuously incorporating feedback and threat intelligence inputs from business units into a clear cybersecurity strategy and road map.



A phased approach for a complex journey



To ensure that our energy clients get the best possible results on their cyber transformation journey, EY and Microsoft combine a top-down strategic review of security approach with a bottom-up scan.

Top-down: cybersecurity program maturity assessment

Conduct workshops and meetings, and rollout a multitiered questionnaire to evaluate the current state and report back on key security pain points.

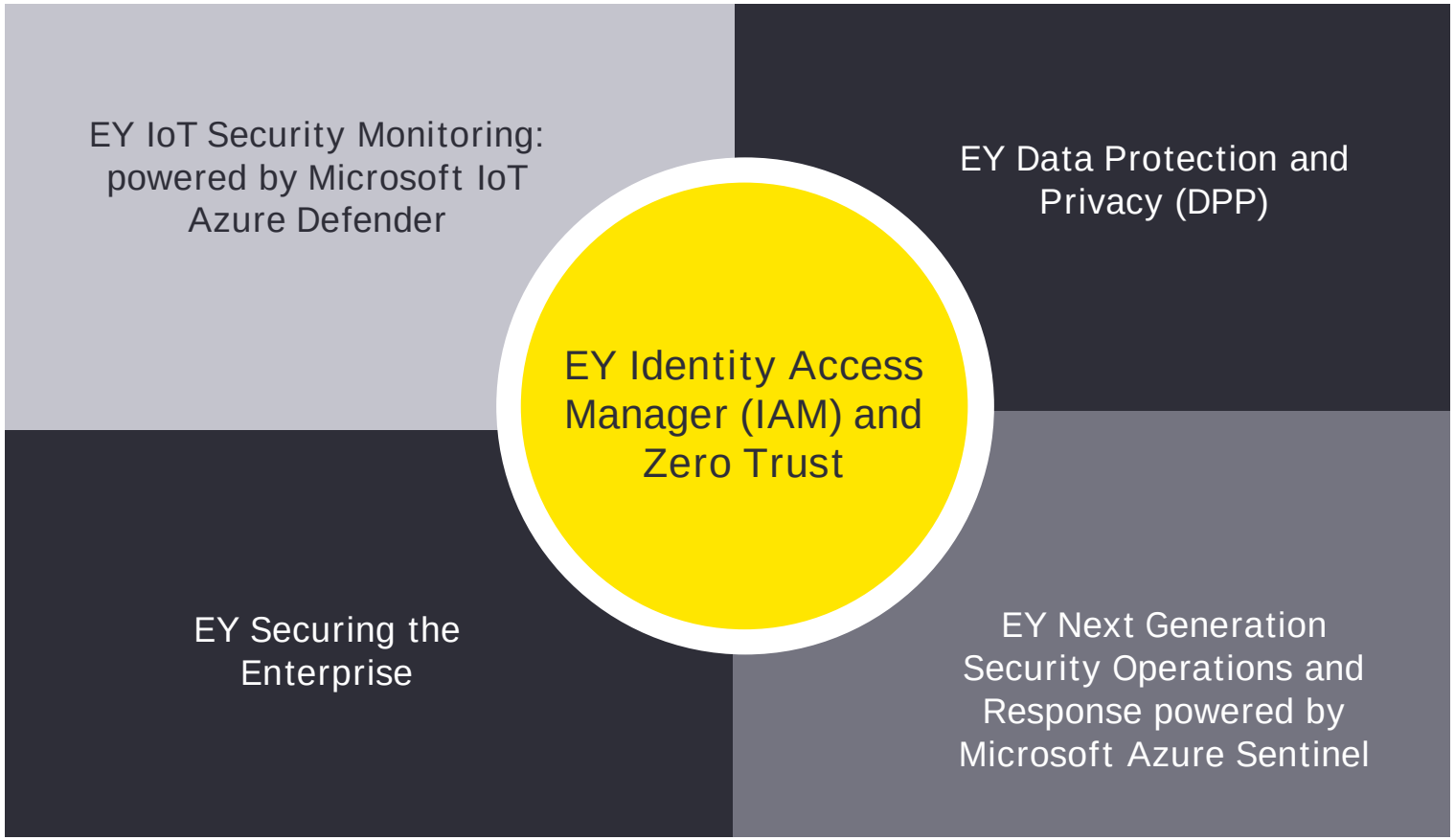
Bottom-up: technical vulnerability assessment

Perform a vulnerability scan of infrastructure, looking for weaknesses that might lead to a cyber breach. The results can also provide key focus areas for the top-down assessment.

Five EY and Microsoft offerings

The EY organization and Microsoft offer a proven engagement model with five key offerings to help energy companies in identifying and responding better to cybersecurity risks, while taking informed decisions to accelerate transformation and innovation.

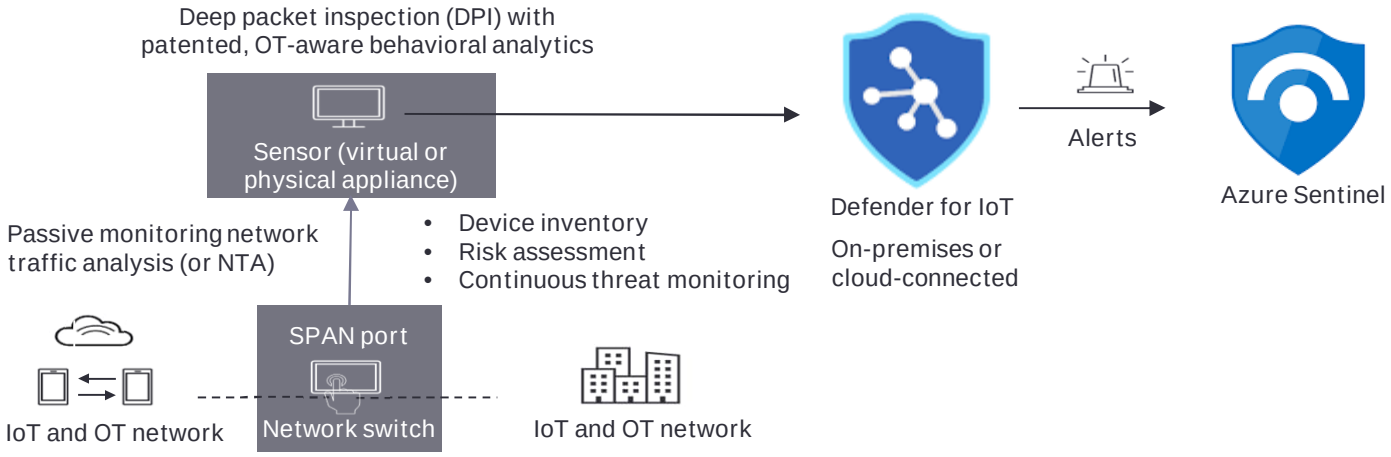
Combined with the EY organization's industry and technical knowledge, these solutions provide advanced technologies from Microsoft to deliver the critical cybersecurity capabilities that energy companies need today.



1. EY IoT Security Monitoring: powered by Microsoft IoT Azure Defender

OT and IIoT security challenges require real-time monitoring and response capabilities to overcome cyber threats. EY IoT Security Monitoring is an asset discovery and security monitoring solution for OT and IIoT environments. For end-user organizations, the solution offers agentless, rapidly deployable network-layer security that works with diverse industrial equipment and interoperates with Microsoft Azure Sentinel and other SOC tools.

The solution usually consists of two main components: probes (sensors) in the form of physical or virtual devices that are placed inside the OT network and the central console. The probes are connected to the switched port analyzer (SPAN) and mirror ports of network switches in the places that are to be monitored. The information from the acquired network traffic is aggregated in the central console, where the data is correlated, visualized and archived.



EY IoT Security Monitoring solution can help energy companies:

- Perform continuous, agentless vulnerability and threat detection with OT and IIoT behavioral analytics.
- Detect human errors and increase awareness via appropriate response.
- Gain broad visibility into assets and risks across OT and IIoT environment.
- Integrate OT and IIoT devices into a secure hub for tailored security management.
- Seamlessly integrate OT and IIoT devices into the company's cloud security information and event management (SIEM) platform and leverage predefined monitoring and response rule sets.
- Provide scalability for single sites in up to over 100 global organizations.
- Help create personalized alarms for critical communication.
- Help create use cases and alarms that highlight potential cyber threats that may impact physical safety aspects.

2. EY Data Protection and Privacy (DPP)

Energy companies struggle to integrate global privacy compliance practices in their day-to-day operations, which can lead to heavy financial penalties and reputational loss. The EY organization's DPP services and solutions are designed to help energy companies protect their sensitive information over the full data lifecycle from a security, legal and ethical perspective. The service offerings help energy companies implement leading practices, change culture, help with compliance and increase cyber resilience in a constantly evolving threat environment and regulatory landscape.

Supported by Microsoft Purview, DPP solution helps organizations meet data protection challenges within one single technology stack. Microsoft Purview is a combination of formerly known Azure Purview and Microsoft 365 compliance solutions. It is a suite of data governance, risk and compliance solutions to help govern, protect and manage an organization's data.

EY DPP services

DPP strategy, governance and transformation	DPP technology enablement	DPP awareness	DPP compliance
Measure, design and help implement DPP program through governance, strategy and roadmap design.	Help implement, activate and integrate technical capabilities via Microsoft information protection advisory solutions.	Raise organizational awareness through data-centric operating model, governance workshops and gamification.	Achieve alignment and assurance with laws and standards linked to DPP with third-party risk management.

With EY DPP solution offerings, energy companies can:

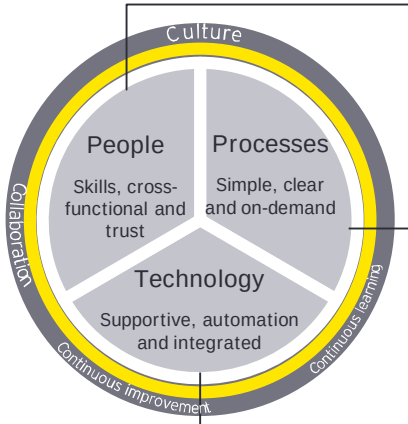
- Provide a connected, frictionless, digitalized and self-service experience to the customers.
- Gain access to modern digital tools and real time data to improve the efficiency and performance of the field workers.
- Support value creation for customers, business and stakeholders via improved operational efficiency.
- Access advanced asset management solutions to maintain, operate and repair assets.

3. EY Identity and Access Management (IAM) Zero Trust

Continuously transforming workspace (with multiple devices from outside the business perimeter) and increasing cloud migration, have exposed energy companies to challenges in effectively managing and governing access to the systems. EY IAM Zero Trust helps companies protect themselves against cyberattacks by moving to a Zero Trust framework – which maintains strict access controls, assumes breach and treats all users same.

The EY IAM Zero Trust framework includes technology and processes to enhance the security of: users, devices, data, network, applications and infrastructure. The framework leverages Microsoft Azure Active Directory E5 for addressing zero trust challenges, as well as Microsoft Azure Key Vault. This acts as a secrets management solution, for helping energy companies define authorization strategies (consent, conditional access and policies) to maximize security.

EY IAM Zero Trust framework



Cross-functional	Learning and adapting	Right-size teams
Operating model	Roles	Change management
Data management	Infrastructure provisioning	Security management
Device management	Planning	Issue management
Release management	Environment management	Feedback integration
Data	Identity	Networks
Applications	Devices	Infrastructure

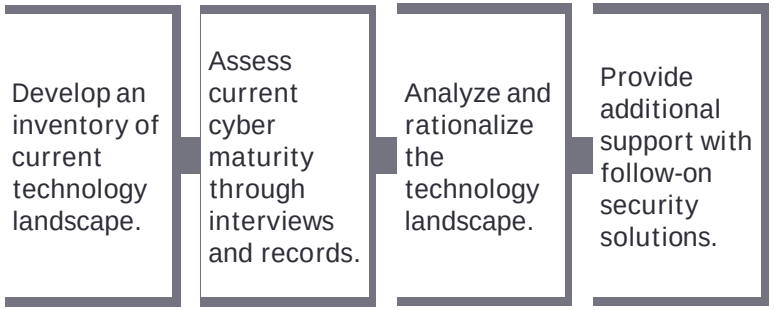
With EY IAM Zero Trust solution, energy companies can:

- Gain visibility into users, devices and components across the entire network and get detailed logs, reports and alerts to detect and respond to threats.
- Reduce costs by eliminating redundant cybersecurity tools and reducing their infrastructure footprint.
- Reduce risk and improve overall security posture by lowering breach potential and increasing secure network coverage.
- Satisfy completeness and accuracy controls related to audits, and consistently enforce policy-based controls and compliance initiatives.
- Boost operational efficiency by automating manual processes and reducing the number of helpdesk calls.
- Prevent customer fraud and strengthen protection against existing and evolving cyber threats.

4. EY Securing the Enterprise

Complex infrastructure and widening supply chain can create several security challenges for energy companies. For instance, addressing security complexities originating from a large portfolio of suppliers and vendors is becoming very challenging and resulting in slow deployment of critical security solutions.

The EY Securing the Enterprise solution, supported by Microsoft Defender suite, helps streamline energy companies' security capabilities through a four-step process:



With this offering, security is seamlessly integrated with the business via vendor consolidation, cost takeout and operational optimization through a platform strategy.

EY Securing the Enterprise helps develop compliance blueprints for common energy industry and regional standards and regulations, including custom assessments to meet energy companies' unique compliance needs.

With EY Securing the Enterprise, energy companies can:

- Consolidate vendors offering multiple security capabilities on an integrated platform.
- Dynamically change the level of access and user authentication based on criteria (e.g., location, device risk, user risk, or document confidentiality level).
- Control access to data, even when shared outside an organization or accessed via third-party app.
- Discover shadow IT so it can be secured and managed, reducing exposure to data leakage through inappropriate sharing and unsecured storage.
- Detect potential threats and correlate alerts via security automation to identify a specific attack vector.
- Investigate and remediate threats, reauthenticate high-risk users and take action to limit access to data.
- Decrease total cost of ownership with individual components purpose-built to integrate.
- Simplify deployment and ongoing management and provide built-in security to detect and prevent online threats.
- Simplify compliance with regional cybersecurity standards.

5. EY Next Generation Security Operations and Response

As cybersecurity threats continue to evolve aggressively, attackers are becoming more persistent and sophisticated, and are deploying new attack strategies. EY Next Generation Security Operations and Response, powered by Azure Sentinel, is an advanced cyber intelligence and automation platform that automatically discover “advanced attack patterns” and proactively strengthen the protection capability.

The EY organization and Microsoft security professionals not only monitor company’s environment for security threats 24x7, but also work with the client to customize and improvise the Azure Sentinel platform continuously, to best fit their environment and use cases. This customization includes integrating and onboarding standard and customized logs, designing and creating customized dashboards and workbooks, and tuning customized alerts, rules and analytics to help a company manage enterprise cyber risks.

With EY Next Generation Security Operations and Response powered by Microsoft Azure Sentinel, energy companies can:

- Quickly gain visibility across their cloud environment and on-premise data sources.
- Use fusion technology and the capability to detect and prevent advanced, persistent, multi-stage attacks.
- Begin detections within their connected environment from day one and realize cost savings through fast, streamlined, cloud-native deployment.
- Realize longer-term efficiency by automating the integration of new data sources as they are created, scaling automatically to meet a company’s needs.
- Generate a higher return on their investment in cybersecurity capabilities over time through pricing based on volume of data ingested and stored or a fixed fee based on capacity reservation.
- Help create converged use cases that increase cyber visibility across IT and OT, and link digital with physical security.

Are you ready for tomorrow's threats?

The EY organization and Microsoft can help energy companies embed deeper trust and security across their business – including both IT and critical OT infrastructure and IIoT – so they can pursue innovation confidently and digitally transform to capitalize on the energy transition.

To start your cyber transformation journey, contact us today.

Your EY contacts

Clinton M. Firth
EY Global Energy & Resources Cybersecurity Leader
clinton.firth@ae.ey.com

Alex Campbell
EY UK&I Energy & Resources Cybersecurity Leader
acampbell2@uk.ey.com

Clement Soh
EY Global Mining & Metals Cybersecurity Leader
clement.soh@au.ey.com

Matt Chambers
EY US Power & Utilities Cybersecurity Leader
matt.chambers@ey.com

Richard Bergman
EY Asia-Pacific Cybersecurity Leader
richard.bergman@au.ey.com

Raddad Ayoub
EY MENA Oil & Gas Cybersecurity Leader
raddad.ayoub@ae.ey.com

Brian Masch
EY US Oil & Gas Cybersecurity Leader
brian.masch@ey.com

Jaco Benadie
EY ASEAN Energy & Resources Cybersecurity Leader
jaco.benadie@my.ey.com

Yuval Stern
Microsoft Alliance – Solutions
yuval.stern@ey.com

Jason Green
EY Canada Energy & Resources Cybersecurity Leader
jason.b.green@ca.ey.com

Luiz M. Fernandes
EY South America Cybersecurity Leader
luiz.fernandes@br.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 000795-24Gbl
BMC Agency GA 165247151
ED None

ey.com