
Is there a better way for energy companies to protect against evolving cyber threats?
Embed trust in your digital business with EY and Microsoft
The better the question. The better the answer.
The better the world works.
EY
Building a better working world
Microsoft

Executive summary

As the energy industry continues its transition to cleaner, renewable energy sources, digital technologies are taking center stage — sitting at the heart of strategic plans and the transformative business solutions needed to realize them.

Almost every energy company has embarked on a digital transformation journey, 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 more complex to protect.

Vulnerabilities vary, not only within the energy organization but across a wide and increasingly integrated ecosystem that is at varying stages of maturity. These circumstances create significant cyber risks that have the potential to cause commercial, reputational, human, and societal damage if attacked. Recent high-profile ransomware attacks are just a few examples of the potential impact to critical services stemming from the growing convergence of IT and OT.

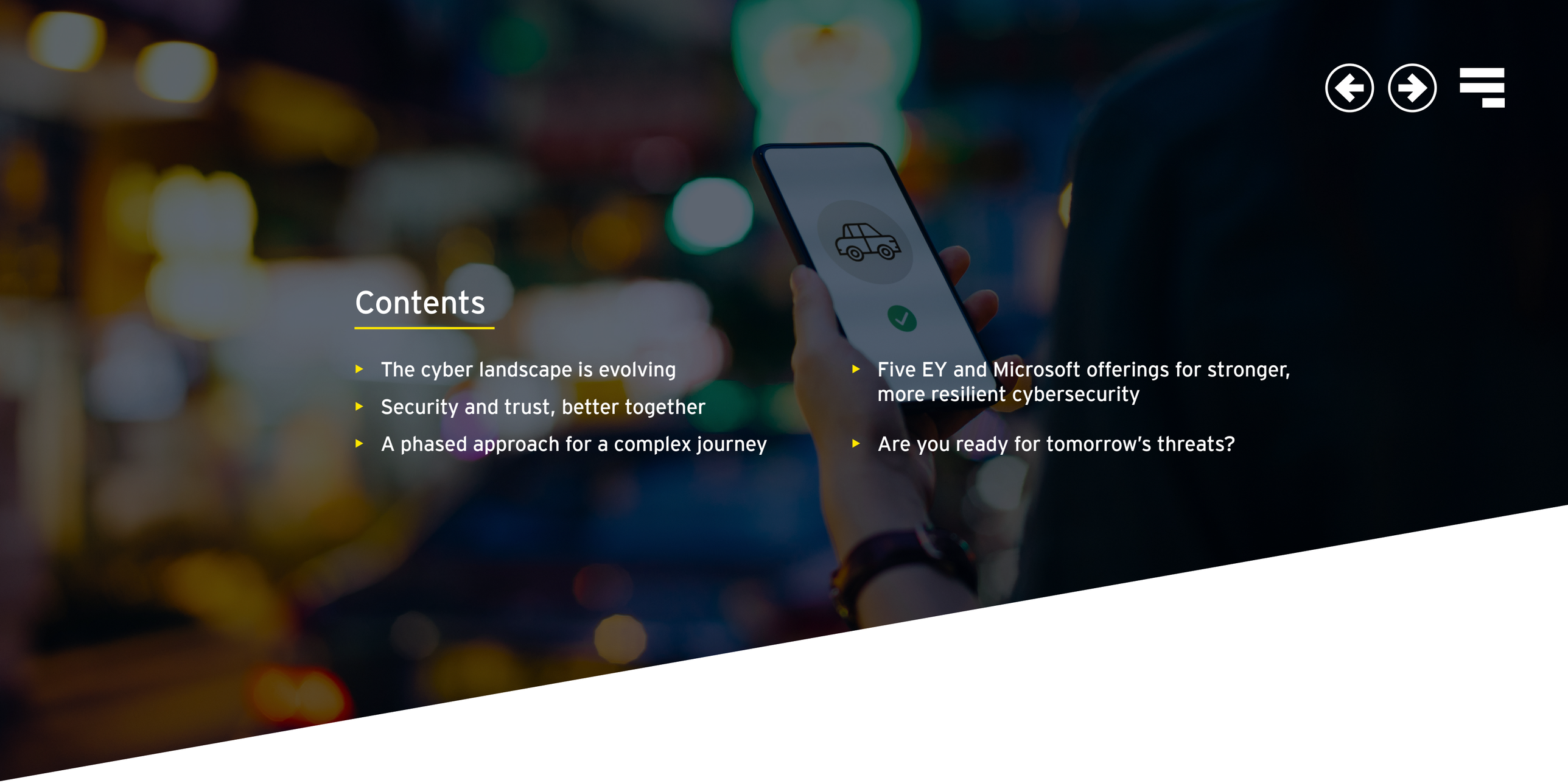
The fact is, legacy OT systems that were never intended to be connected to the internet, as well as the introduction of IIoT sensors and smart infrastructure, are exposing energy companies to a wide range of cyber risks and expanding the potential attack surface. At the same time, cybersecurity threat actors are rapidly increasing their capabilities and their targeting of energy companies with the intention to cause physical damage, impact personnel safety or compromise the quality of the output.

Together, EY and Microsoft offer a proven engagement model that will help you:

- Identify and respond better to cybersecurity risks
- Meet changing regulatory and compliance requirements
- Embed trust into your services and products from the outset
- Take informed risks to accelerate transformation and innovation

Discover how we can transform cybersecurity from a "bolt-on" function to an integrated part of your business.

To mitigate the growing and significant cyber risks they face, energy companies need to build cybersecurity resilience into every facet of their organization. They must develop strategies that help to establish trust in systems, design and data architecture, and integrate legacy OT systems so they can transform their digital landscape with speed, scale and innovation and be confident in their entire digital ecosystem.



Contents

- The cyber landscape is evolving
- Security and trust, better together
- A phased approach for a complex journey
- Five EY and Microsoft offerings for stronger, more resilient cybersecurity
- Are you ready for tomorrow's threats?

The cyber landscape is evolving

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

Now >> Next >> Beyond

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

Along with heightened privacy concerns around remote working, further vulnerabilities are emerging from developments in IIoT and customer self-service. Structural business changes, like mergers and acquisitions, can bring new risks, too – especially when untested technology and processes are added to established operations.

There's also the continual backdrop of changing legal and regulatory standards, including local variances, which is making the compliance landscape extremely complicated and a real challenge to address.

Current trends in cyber threats and attacks:

- Increase in critical national infrastructure attacks affecting the energy industry
- Phishing, malicious sites and business email compromise
- Extortion or information theft and brand damage
- Business distribution from attacks
- Attackers focusing on cloud-native applications

39%

of energy companies believe hackers are using new strategies, such as exploiting vulnerabilities in procurement and the supply chain, but do not know whether their defenses are strong enough to stop them from getting through.

Source: EY Global Information Security Survey 2021

Now >> **Next** >> Beyond

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 that their current cyber setup will provide the security they need, or that customers and regulators demand.

A positive first step is to understand your cybersecurity program and assess your ability to respond to significant disruptions.

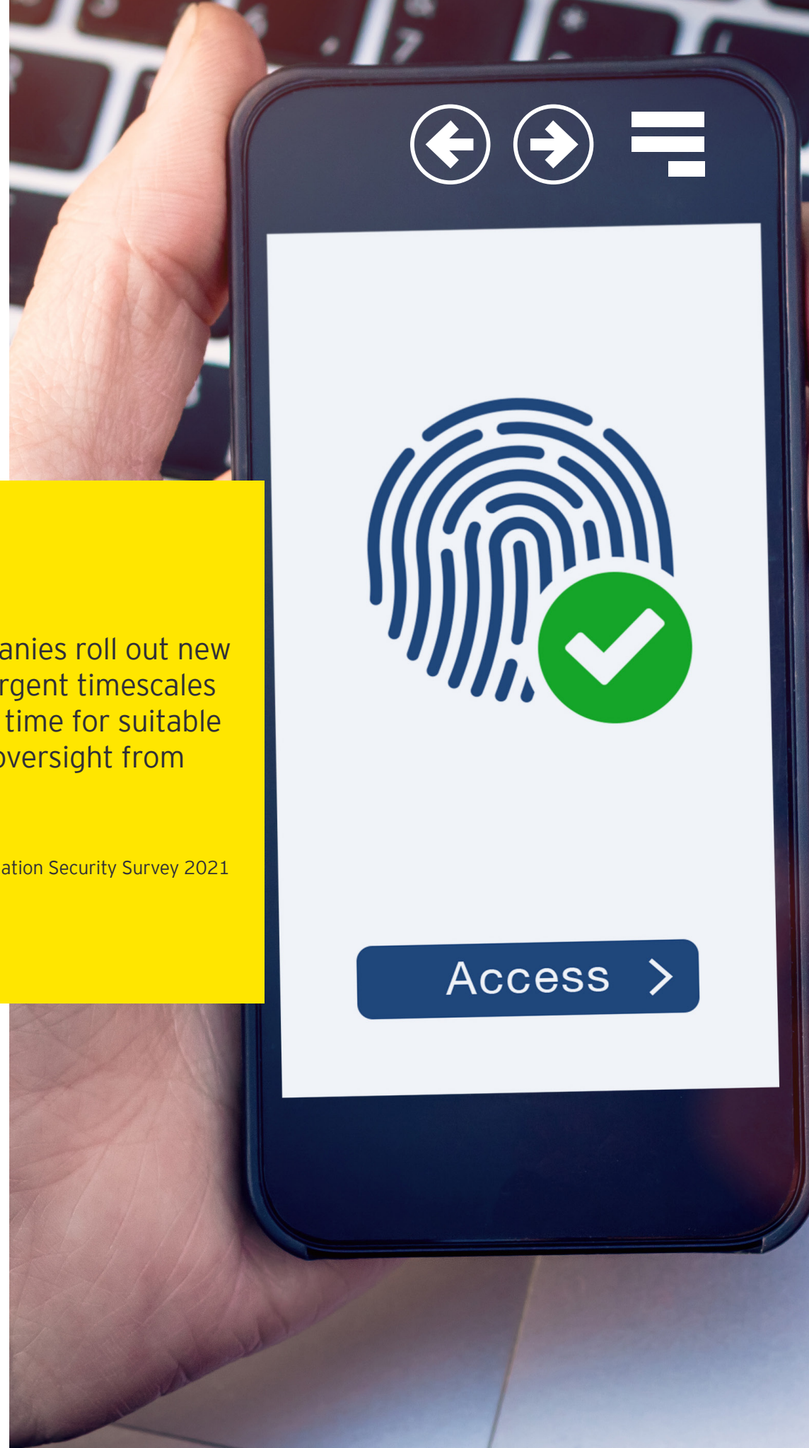
This requires an understanding of what good security looks like. For example, what's best practice for identifying and responding to threats? How can you control people's access to data and systems without compromising productivity?

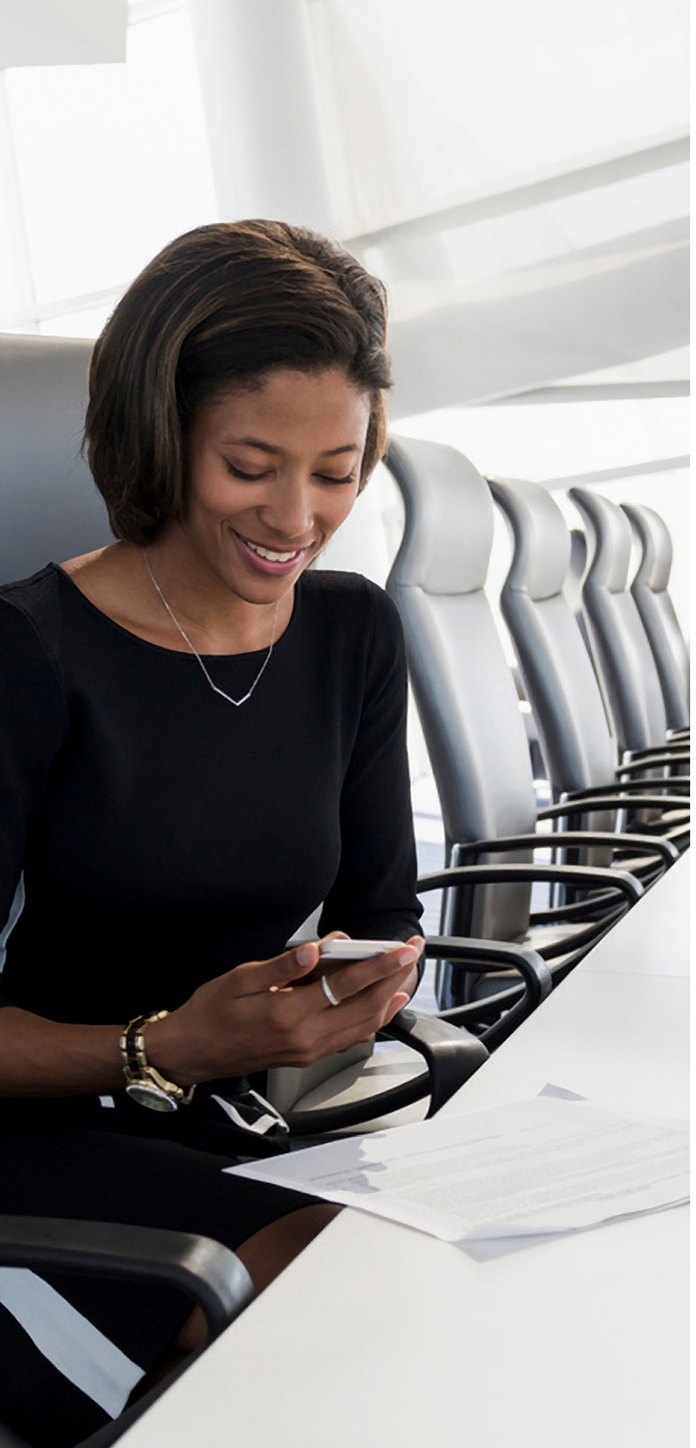
Answering these questions can help determine current gaps in your approach and what strategic input and investments you need to get you to the desired maturity level.

32%

of energy companies roll out new technology to urgent timescales that don't allow time for suitable assessment or oversight from cybersecurity.

Source: EY Global Information Security Survey 2021





Now >> Next >> **Beyond**

Energy companies should strive to integrate cybersecurity into all aspects of their business operations, including the critical OT and IIoT affecting their core operations. This will require a clear vision of what your security operations should look like over time.

For example, how will you ensure security and resilience is built into emerging technology by design and not just bolted on afterward? How will you embed a "risk-thinking" mindset throughout the business, so every decision has factored in appropriate security measures?

Reviewing progress toward this new level of cyber maturity must be done regularly, underpinned by clear metrics and ratings that allow changes to be agreed upon and executed.

At this point, your organization will be well-placed to manage the evolving pressures of today's threat landscape – whether it's state-sponsored attackers looking to steal data, hacktivists seeking a denial of service or organized crime groups issuing ransom demands.

EY 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 domain experience and understanding
- Over 2,500 cyber engagements delivered in 2021
- 2,000+ full-time information/cybersecurity SMRs
- 20+ years of developing industry leaders in cybersecurity
- 65 cybersecurity centers globally

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 provides a cloud-native security information and event manager platform to quickly analyze large volumes of enterprise data
- Consulting services aligned to EY offering broad technical experience across all Microsoft solutions

Unique value to you

Together, our goal is to support your business performance and help you realize the full potential of digital technology by securing your enterprise. Our joint offering will:

- Extend your security operations center (SOC) across your whole IT landscape
- Collect and analyze limitless security data from both on-premise and cloud environments
- Expedite threat hunting, incident investigation and response times using built-in AI capabilities
- Augment your SOC team with a fully managed security service
- Use threat intelligence insights to prioritize actions for your SOC

A phased approach for a complex journey

We want to help you embed trust into your cybersecurity function so it becomes an enabler for better, faster and more confident decision-making across the organization.

Our approach to building this "trust by design" principle is to incorporate proactive feedback and threat intelligence from business units into the development of a clear cybersecurity strategy and road map.

Five steps to cyber transformation

1

Understand your business context

The starting point is always to fully understand your current position, looking at your business priorities, mission and vision.

We'll get a feel for your security culture and appetite for risk, and how you are operating in the context of market conditions and sector trends.

From a practical perspective, we'll translate your business, privacy and regulatory requirements into a labeling taxonomy.

2

Identify priority scenarios

Next, we'll explore what's driving your need for change — i.e., the specific security threats facing your infrastructure and the business scenarios that need to be assessed.

At this point, it's important to ensure that all stakeholders are agreed on the outcomes we're working toward, as these will help formulate the assessment framework.

We'll assess the impact, urgency, restoration costs, and recovery time of identified risks, and develop a potential mitigation strategy with recommended next steps.

3

Determine your current maturity

After validating the scope and level of detail for your assessment, we'll run workshops and interviews to map out your current-state profile.

The aim is to understand whether specific information assets are being protected to the appropriate level of security based on their value to your business.

We'll map out your current network and security architecture, plus any additional IT-enabled controls and policies to be monitored, to get a deep understanding of your defense layers.

4

Define the target state

This stage is about agreeing the level of maturity you're striving for. We'll use a standardized scoring and assessment methodology to compare where you are today with where you want to be.

We'll develop benchmark reports against your regional, industry and market peers (using anonymized historical data), and create a road map for getting to your future state.

This road map could include a blend of people-, process- and technology-based solutions according to your specific business needs.

5

Report on progress

As your project moves forward, we'll provide support for executive reporting.

This can include regular overviews of key strengths, areas of improvements, changes to the cyber threat landscape, road map developments, and the impact of add-on services.

Our digital platform will provide full visibility, tracking and regular health checks of your improvement areas to ensure continued progress against targets.

From every perspective

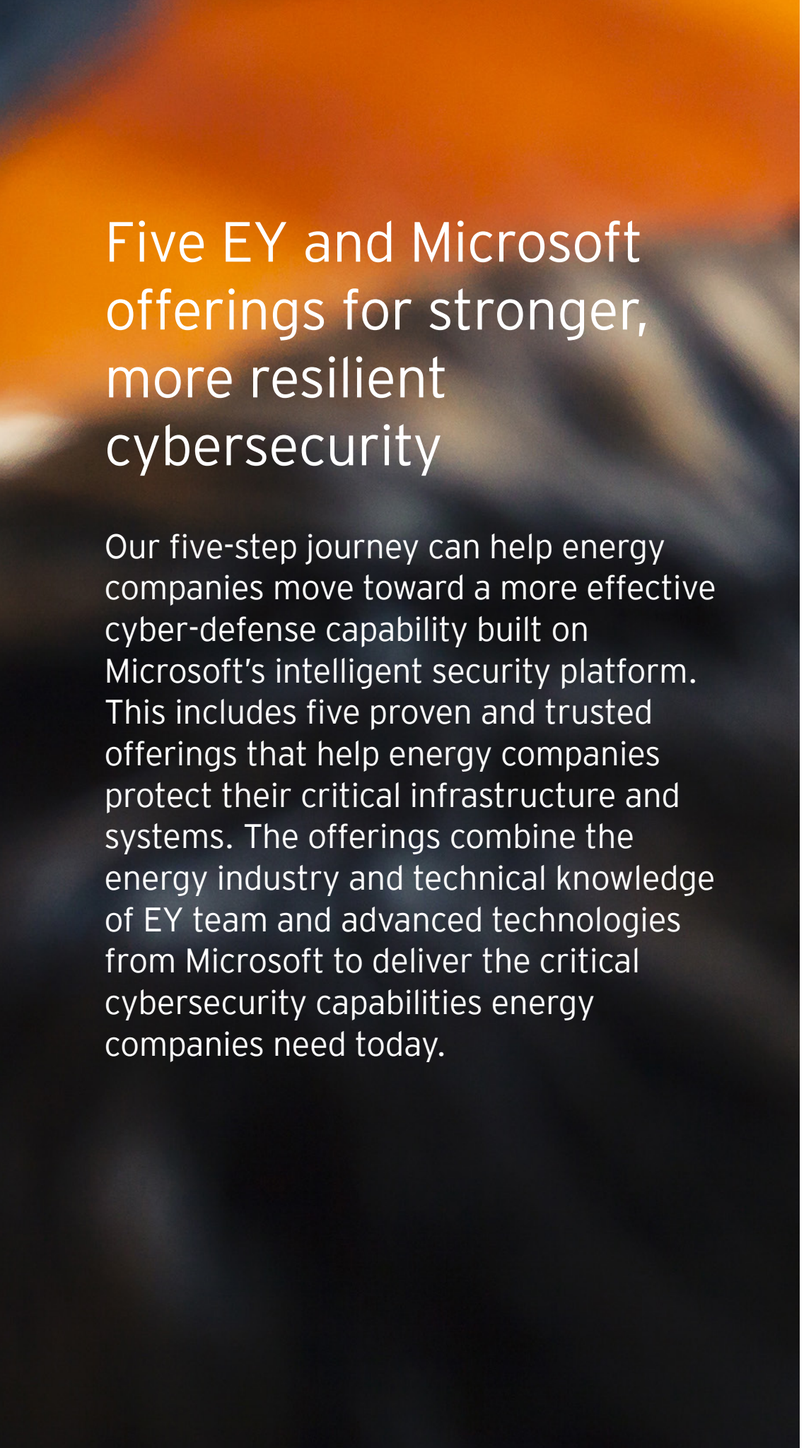
To ensure you get the best possible results on this cyber transformation journey, we combine a top-down strategic review of your security approach with a bottom-up scan of current threats:

TOP-DOWN: cybersecurity program maturity assessment

We'll conduct workshops, meetings and a multitiered questionnaire, and then report back on your organization's key security pain points.

BOTTOM-UP: technical vulnerability assessment

We'll perform a vulnerability scan of your infrastructure, looking for weaknesses that might lead to a breach. The results can provide useful focus areas for the top-down assessment.



Five EY and Microsoft offerings for stronger, more resilient cybersecurity

Our five-step journey can help energy companies move toward a more effective cyber-defense capability built on Microsoft's intelligent security platform. This includes five proven and trusted offerings that help energy companies protect their critical infrastructure and systems. The offerings combine the energy industry and technical knowledge of EY team and advanced technologies from Microsoft to deliver the critical cybersecurity capabilities energy companies need today.

1 EY IoT Security Monitoring: powered by MS IoT Azure Defender

OT and IIoT security challenges require real-time monitoring and response capabilities to overcome cyber threats. EY IoT Security Monitoring is a specialized asset discovery and security monitoring solution for OT/IIoT environments. This solution helps accelerate OT/IIoT innovation with broad security across all OT/IIoT devices. For end-user organizations, EY IoT Security Monitoring offers agent-less, rapidly deployable network-layer security that works with diverse industrial equipment and interoperates with Azure Sentinel and other SOC tools. The EY IoT Security Monitoring solution usually consists of two main components: 1) probes (sensors) in the form of physical or virtual devices that are placed inside the OT network and 2) the central console. The probes are connected to the switched port analyzer (SPAN)/mirror ports of network switches in places that are to be monitored. The place of obtaining information depends on which network traffic will be monitored. Information about the acquired network traffic is aggregated in the central console, where this data is correlated, visualized and archived.

With EY IoT Security Monitoring, EY can help energy companies:

- Perform continuous, agentless vulnerability and threat detection with OT/IIoT behavioral analytics
- Detect human failure affecting the security of the OT/IIoT environment and increase awareness by proper response
- Gain broad visibility into assets and risk across the entire OT/IIoT environment
- Integrate OT/IIoT devices into a secure hub for tailored security management and secure communication in the production area
- Seamlessly integrate OT/IIoT devices into the company's cloud SIEM and leverage pre-defined monitoring and response rulesets
- Provide scalability for single sites in up to 100+ global organizations
- Create personalized alarms for critical communication
- Create use cases and alarms that highlight potential risks related to plant safety systems or cyber threats that may impact HSE and plant safety

2 EY Data Protection and Privacy (DPP) Manager: an overall solution to support compliance with privacy regulations

Many energy companies struggle to integrate global privacy compliance practices in day-to-day operations, which can lead to heavy financial penalties and loss of reputation. With EY DPP Manager, energy companies gain a flexible data privacy and compliance platform through which they can operationalize data protection and privacy measures across the enterprise. Built on Microsoft Azure, this software-as-a-service solution – one of the most complete multi-regulation compliance solutions in the market – enables energy companies to manage, track and prioritize all their privacy compliance activities via a single dashboard and fully integrated, scalable and client-tailored modules. The solution leverages EY energy industry best practices and current intelligence on updates to regulatory changes, includes configurable process automation to reduce manual tasks and increase efficiency, and can be easily integrated with a company's existing environment and other solutions.

With EY DPP Manager, energy companies can:

- Reduce risk and regulatory exposure by identifying and reducing privacy risks and managing multi-regulation compliance
- Avoid costs by gaining a clear picture of the privacy compliance activities that can help head off fines, audit costs and other expenditures

3 EY Identity Access Manager (IAM) Zero Trust: helping you adapt to a new threat landscape

Due to ongoing cyberattacks, as well as the modern workforce's increased use of applications from multiple devices outside of the business perimeter, energy companies face growing challenges in effectively managing and governing identities and access to systems. EY IAM Zero Trust helps energy companies protect themselves against the ongoing surge of cyberattacks by moving to a zero trust framework – i.e., one that maintains strict access controls and doesn't trust anyone by default, even those already inside the network perimeter. The EY IAM Zero Trust framework includes technology and processes to secure six different types of assets: users, devices, data, network, analytics, and automation. The framework leverages Microsoft Azure Active Directory E5 for addressing zero trust challenges, as well as Microsoft Azure Key Vault as a secrets management solution, while helping energy companies define authorization strategies (consent, conditional access and policies) that maximize security.

With EY IAM Zero Trust, energy companies can:

- Reduce risk and improve their overall security posture by lowering their 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
- Gain visibility into users, devices and components across the entire network and get detailed logs, reports and alerts to detect and respond to threats
- Prevent customer fraud and strengthen protection against existing and evolving cyber threats
- Reduce costs by eliminating redundant cybersecurity tools and reducing their infrastructure footprint

4 EY Securing the Enterprise

Growing complexity can create many security challenges for energy companies. Case in point: it's becoming increasingly difficult to address the security complexities originating from a large portfolio of point products and vendors, which results in slow deployment of critical security solutions. The EY Securing the Enterprise offering helps streamline energy companies' security capabilities through a four-step process: 1) inventory the technology landscape; 2) assess the business through stakeholder interviews and documentation evaluation; 3) analyze and rationalize the technology landscape; and 4) provide additional support with immediate follow-on security solutions. 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 also 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:

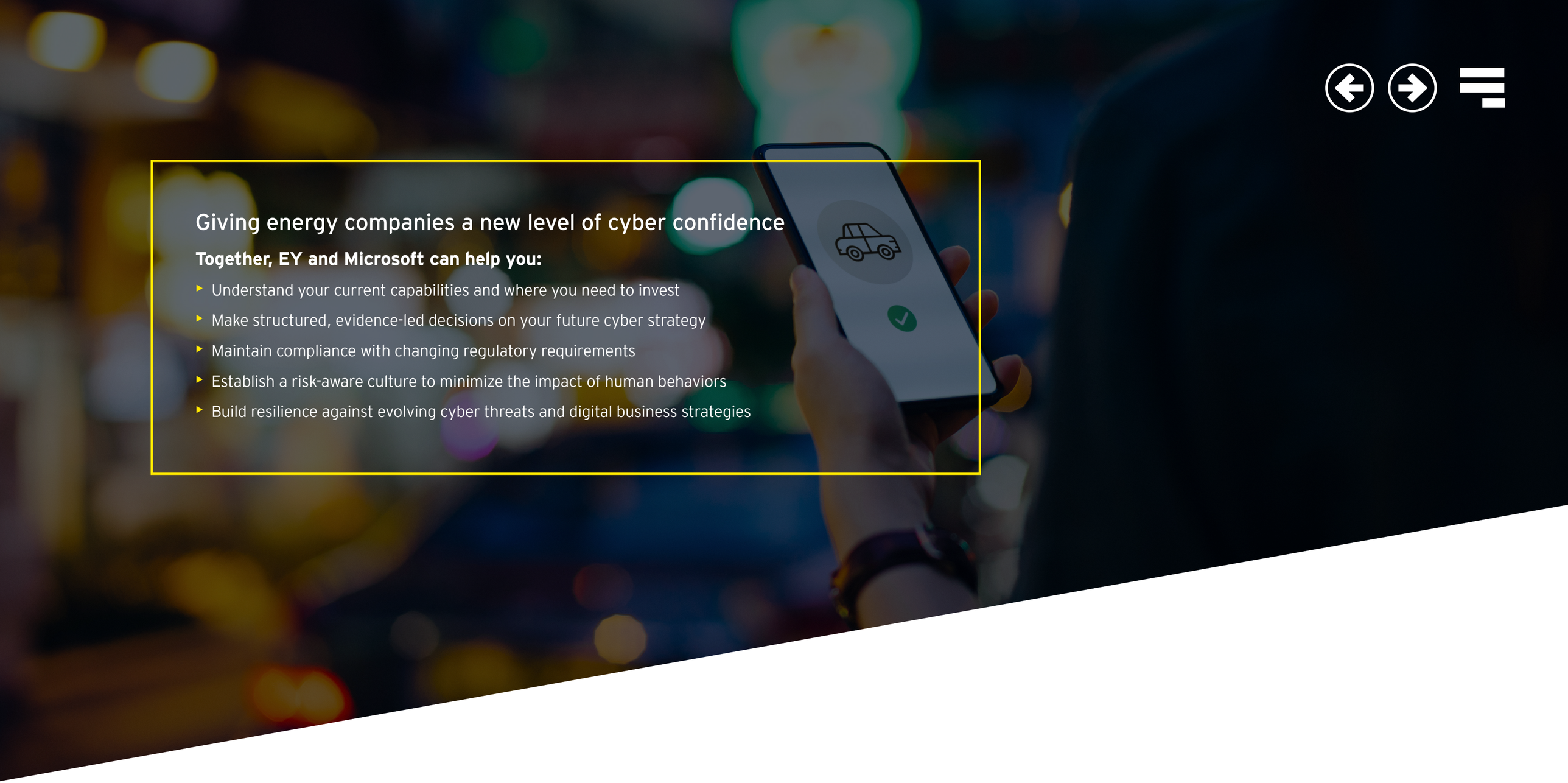
- Consolidate vendors offering multiple holistic security capabilities on an integrated platform
- Dynamically change the level of access and user authentication based on criteria (e.g., location, device risk, user risk, or document confidentiality level)
- Control access to data, even when shared outside 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 powered by Azure Sentinel

As cybersecurity threats continue to evolve aggressively, attackers are becoming more patient, 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 for innovation that can help energy companies automatically discover "advanced attack patterns" and proactively strengthen their protection capability. This includes using EY and Microsoft security experts who will not only monitor a company's environment for security threats 24x7 but also work with a company's team to customize and improvise the Azure Sentinel platform continuously to best fit its environment and use cases. This customization includes integrating and onboarding standard and customized logs, designing and creating customized dashboards/workbooks, and tuning customized alerts/rules/analytics to help a company manage enterprise cyber risks. The result: end-to-end cyber protection from advanced cyber threats.

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

- Quickly gain full 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
- Create converged use cases that increase cyber visibility across IT/OT and link digital with physical security



Giving energy companies a new level of cyber confidence

Together, EY and Microsoft can help you:

- Understand your current capabilities and where you need to invest
- Make structured, evidence-led decisions on your future cyber strategy
- Maintain compliance with changing regulatory requirements
- Establish a risk-aware culture to minimize the impact of human behaviors
- Build resilience against evolving cyber threats and digital business strategies

Are you ready for tomorrow's threats?

The world continues to digitize, bringing more convenience to people's lives and new opportunities for energy companies to generate value.

But with that comes new risks for this critical national infrastructure we all rely on. Cybercriminals and hackers have an ever-broadening range of attack targets which energy companies need to protect — proactively.

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

Dillon Dieffenbach
US Energy & Resources Cybersecurity Leader
dillon.dieffenbach@ey.com

Brian Masch
Canada Energy & Resources Cybersecurity Leader
brian.masch@ca.ey.com

Alex Campbell
EMEIA Energy & Resources Cybersecurity Leader
acampbell2@uk.ey.com

Raddad Ayoub
MENA Energy & Resources Cybersecurity Leader
raddad.ayoub@ae.ey.com

Richard Bergman
APAC Cybersecurity Leader
richard.bergman@au.ey.com

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

Marcus Semola
LAS Cybersecurity Leader
marcus.semola@br.ey.com

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

Piotr Ciepiela
Global OT Cybersecurity Leader
piotr.ciepiela@pl.ey.com

Building a better working world

Microsoft

EY and Microsoft

The EY and Microsoft alliance combines deep EY insights and experience in disruptive industry trends, new business models and evolving processes with scalable, enterprise cloud platform and digital technologies from Microsoft. EY and Microsoft can help accelerate digital transformation with advanced solutions that support enterprise strategy, transform customer and workforce experiences, create new, data-driven business models, build intelligent, automated operations and bring confidence that these innovative solutions are secure, compliant and trusted

For more information, visit ey.com/microsoft

EY and Microsoft alliance | EY – Global

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.

BMC Agnecy
GA 14525663

2201-3974665
EYG no. 001255-22Gbl
ED None

ey.com