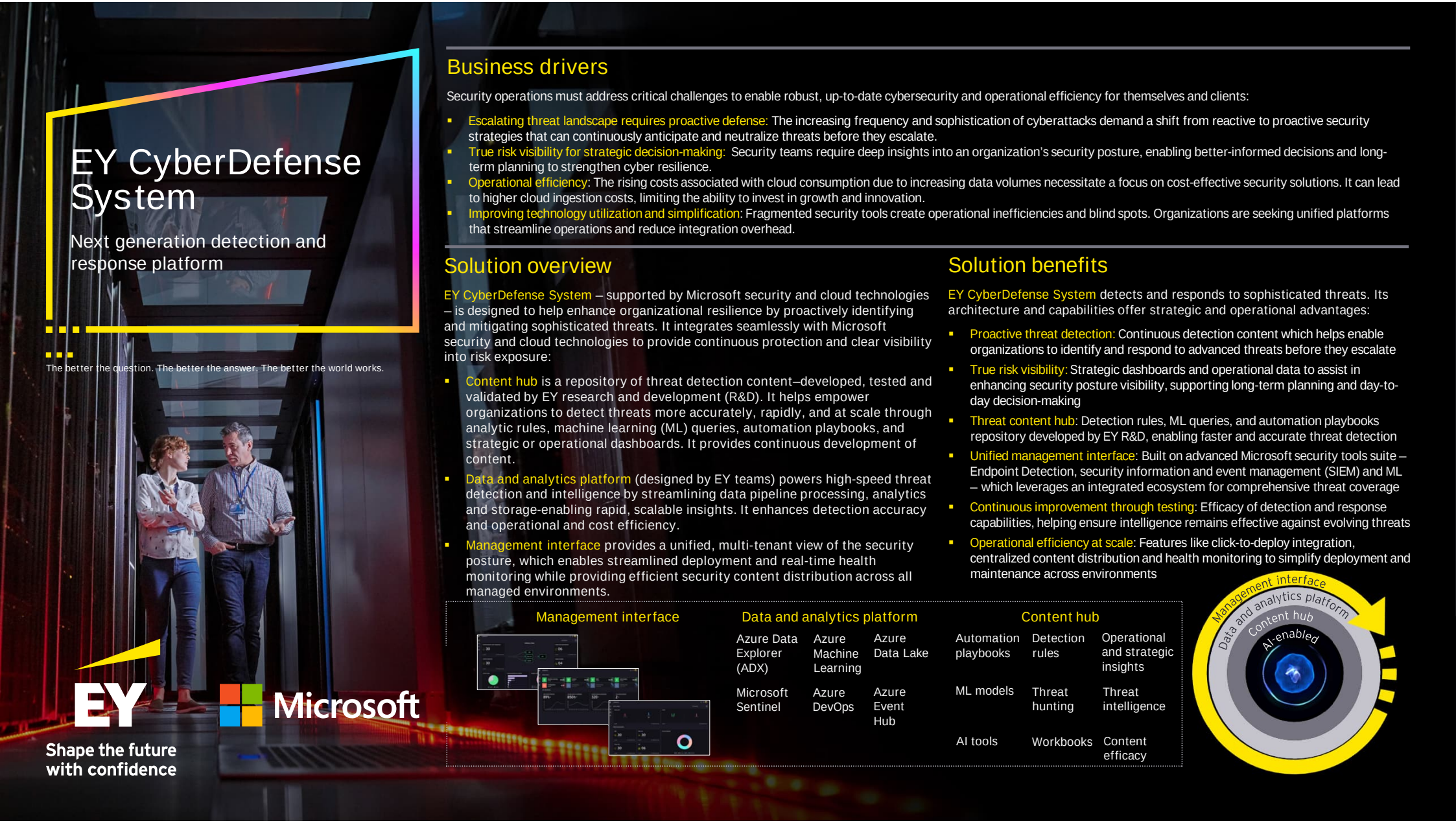
EY CyberDefense System

Next generation detection and response platform

The better the question. The better the answer. The better the world works.



EY Microsoft

Shape the future with confidence

Business drivers

Security operations must address critical challenges to enable robust, up-to-date cybersecurity and operational efficiency for themselves and clients:

- Escalating threat landscape requires proactive defense: The increasing frequency and sophistication of cyberattacks demand a shift from reactive to proactive security strategies that can continuously anticipate and neutralize threats before they escalate.
- True risk visibility for strategic decision-making: Security teams require deep insights into an organization's security posture, enabling better-informed decisions and long-term planning to strengthen cyber resilience.
- Operational efficiency: The rising costs associated with cloud consumption due to increasing data volumes necessitate a focus on cost-effective security solutions. It can lead to higher cloud ingestion costs, limiting the ability to invest in growth and innovation.
- Improving technology utilization and simplification: Fragmented security tools create operational inefficiencies and blind spots. Organizations are seeking unified platforms that streamline operations and reduce integration overhead.

Solution overview

EY CyberDefense System – supported by Microsoft security and cloud technologies – is designed to help enhance organizational resilience by proactively identifying and mitigating sophisticated threats. It integrates seamlessly with Microsoft security and cloud technologies to provide continuous protection and clear visibility into risk exposure:

- Content hub is a repository of threat detection content–developed, tested and validated by EY research and development (R&D). It helps empower organizations to detect threats more accurately, rapidly, and at scale through analytic rules, machine learning (ML) queries, automation playbooks, and strategic or operational dashboards. It provides continuous development of content.
- Data and analytics platform (designed by EY teams) powers high-speed threat detection and intelligence by streamlining data pipeline processing, analytics and storage-enabling rapid, scalable insights. It enhances detection accuracy and operational and cost efficiency.
- Management interface provides a unified, multi-tenant view of the security posture, which enables streamlined deployment and real-time health monitoring while providing efficient security content distribution across all managed environments.

Management interface

Data and analytics platform

Azure Data Explorer (ADX)	Azure Machine Learning	Azure Data Lake
Microsoft Sentinel	Azure DevOps	Azure Event Hub

Content hub

Automation playbooks	Detection rules	Operational and strategic insights
ML models	Threat hunting	Threat intelligence
AI tools	Workbooks	Content efficacy

Solution benefits

EY CyberDefense System detects and responds to sophisticated threats. Its architecture and capabilities offer strategic and operational advantages:

- Proactive threat detection: Continuous detection content which helps enable organizations to identify and respond to advanced threats before they escalate
- True risk visibility: Strategic dashboards and operational data to assist in enhancing security posture visibility, supporting long-term planning and day-to-day decision-making
- Threat content hub: Detection rules, ML queries, and automation playbooks repository developed by EY R&D, enabling faster and accurate threat detection
- Unified management interface: Built on advanced Microsoft security tools suite – Endpoint Detection, security information and event management (SIEM) and ML – which leverages an integrated ecosystem for comprehensive threat coverage
- Continuous improvement through testing: Efficacy of detection and response capabilities, helping ensure intelligence remains effective against evolving threats
- Operational efficiency at scale: Features like click-to-deploy integration, centralized content distribution and health monitoring to simplify deployment and maintenance across environments

Solution differentiators

- Advanced detection rules and response tools provide ongoing effectiveness in reducing threats.
- A dedicated R&D team provides higher level of efficacy in detection and response capabilities by continuously developing, testing and updating content for better detection.
- Broad visibility of the risk landscape through an extensive reporting suite helps enable informed decision-making.
- Automated resiliency testing through continuous breach and attacker simulation testing helps in assuring robust coverage and resilience against evolving threats.
- Ease of deployment via preconfigured software suite designed for seamless integration assists in ensuring rapid integration and minimal disruption.

Joint value proposition

- Maximizing investments in Microsoft security
  EY CyberDefense empowers organizations to fully realize the value of their Microsoft investments by seamlessly integrating advanced cyber defense capabilities across the Microsoft ecosystem. It provides protection and operational efficiency, helping organizations maximize Microsoft cyber technologies capabilities.
- Expanding the Microsoft cyber footprint
  As a solution that leverages Microsoft security and cloud solutions, the EY CyberDefense encourages organizations to fully leverage the Microsoft platform. It drives security, cloud consumption workloads through consolidation onto the Microsoft security solution set.
- EY-Microsoft Alliance experience
  By leveraging EY cyber experience and dedicated R&D, the EY organization has created a solution that augments Microsoft cyber security tools. Combined with the unprecedented investment of Microsoft in security, expansive security context and industry-leading cyber tools, the EY CyberDefense System solution provides the highest level of cyber defense.

Contacts

EY

Yogen Appalraju
Partner/Principal
Technology Consulting
Ernst & Young LLP
yogen.appalraju@ca.ey.com

Microsoft

Jodi Lustgarten
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

EY and Microsoft: Helping the world work better to achieve more.

Every day, throughout the world, businesses, governments and capital markets rely on EY business ingenuity and the power of Microsoft technology to solve the most challenging global issues with extraordinary, transformative outcomes.

EY and Microsoft bring a compelling formula to spark the potential of the cloud and unlock the power of data. We solve our clients' most challenging issues by blending trusted industry experience with innovative cloud technology. Our strategic relationship draws on decades of success developing visionary solutions that provide lasting value.

Together, we empower organizations to shape the future with confidence.

For more information, visit: ey.com/microsoft

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 005072-25Gbl
ED None

ey.com