# EY Sentinel as a Service

**The next-gen security operations services of EY**

**Your digital world. Realized.**

## As cybersecurity threats continue to evolve aggressively, attackers are becoming more patient, persistent and sophisticated, and are deploying new attack strategies

- According to the EY Global Information Security Survey 2020, only 26% of organizations reported that their most significant breaches in the past year were discovered by their security operations center (SOC).
- Therefore, it is imperative that SOCs keep pace by focusing on priority threats, and leveraging the detection and response capabilities available to them.
- Costs and business impact arising from attacks that were not detected or prevented can be attributed to the ineffective or incomplete monitoring and the lack of a unified view across the enterprise environment.
- False positive alerts are consuming time and effort of monitoring teams, reducing time for higher-value tasks. The team is burdened with large volumes of data that need to be analyzed in real time to predict responses and execute actions.
- Threats can originate from any place, any device, any entity and traditional perimeters are complex and are no longer compatible with today's business models. Moreover, detection capabilities are not aligned to the priority threats faced by the business.

## Benefits of EY Sentinel as a Service

- **Visibility:** Quickly gain visibility over your cloud environment, and combine with integrated, on-premises data sources to achieve a broad view
- **Advanced capability:** Apply the capabilities of Microsoft's cloud-scale security analytics, EY teams will help you to harness these capabilities with a threat-centric approach to detection and response
- **Cost-effectiveness:** Avail fusion technology and the capability to detect advanced, multi-stage attacks to prevent or detect potentially undetected persistent attacks ahead of time
- **Initial benefits:** Begin detections within your connected environment from day one, realize cost savings through fast, streamlined cloud-native deployment
- **Long-term benefits:** Realize longer-term efficiency by automating integration of new data sources as they are created, while EY Sentinel as a Service scales automatically to meet your needs
- **Increased return on investment (ROI) over time:** Microsoft Azure Sentinel pricing based on volume of data ingested and stored, or fixed fee based on capacity reservation helps in continuous improvement of the platform, leading to better ROI over time

## EY threat detection and response supported by Microsoft

EY Sentinel as a Service is an advanced cyber intelligence and automation platform for innovation that can assist you to automatically discover "advanced-attack patterns" and proactively strengthen your protection capability. This will include being able to utilize our security professionals who will not only monitor your environment for security threats 24x7, but also will work with your team to customize and improvise the Microsoft Sentinel platform continuously to best fit your environment and use cases.

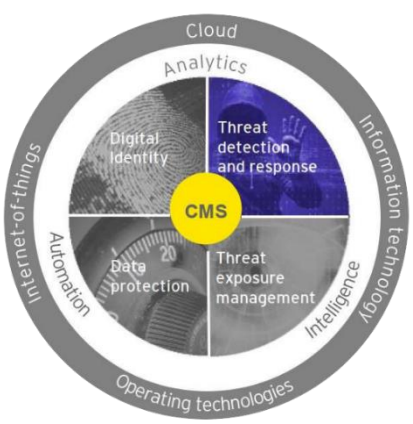
This customization includes, integrating and onboarding standard and customized logs, designing and creating customized dashboards/workbooks, and tuning customized alerts/rules/analytics to help your company manage enterprise cyber risks.

**Service offerings:**

- Broad 24x7 Microsoft Sentinel monitoring and uplift as a service – this can be a mix of off-shore and on-shore
- 8x5 business hours Microsoft Sentinel monitoring and uplift as a service – this can be a mix of off-shore and on-shore
- Platform and threat professionals – can include resources that are dedicated to your business to continuously uplift the platform at a rapid pace

## Key functionality

The EY Sentinel as a Service solution is part of cybersecurity-managed services (CMS), helping to provide for broad cyber protection from advanced cyber threats.




Source: Customer+One-Pager

## EY Sentinel as a Service solution capabilities

### Collection

- Microsoft Azure sources
- O365, M365
- On-premise sources
- In-built connectors
- REST API, Syslog
- Common event format (CEF) integration

### Detection

- Artificial intelligence (AI) and Machine Learning (ML) analytics
- Threat modeling
- Custom queries
- Threat intelligence
- Threat hunting

### Investigation

- Unified view
- Incident alerting
- Investigation UI
- Custom workbooks

### Response

- Orchestration
- Automation
- Logic Apps
- Service integration

## Customer success stories: EY Sentinel as a Service in action

A leading Australian mining institution engaged EY teams to run a broad cyber transformation program, including designing and building a next-generation SOC.

- EY teams deployed, expanded and customized a Microsoft Sentinel instance that was tailored to the mining business' specific needs.
- The solution demonstrated the seamless integration across the broad Microsoft portfolio, including Microsoft Windows Defender Advanced Threat Protection (WDATP), Microsoft Azure ATP, Microsoft Office 365 and others.
- The solution included customized workbooks based on critical assets, users and high-risk watchlists and, in some cases, customized-data integration and parsing to support third-party data integration.

### Client challenges

- The client was struggling to detect and respond to advanced threats across the IT and OT environment, spread across geographies.
- The mining operations were targeted by sophisticated actors, including criminal syndicates and nation states.
- The client wanted a flexible, cost-effective, scalable and customizable solution that could integrate with the existing technology ecosystem and controls deployed.

### Client benefits

- Demonstrate what an efficient security information and event management (SIEM) and security operations team could achieve in less than two months post the uplift of Microsoft Sentinel
- Identify high-risk areas that could be prioritized based on risk reduction and justify appropriate funding for the internal security team and their partners
- Show that the investment made in the Microsoft suite can be leveraged to provide scalable leading-edge security at a reasonable cost and quick time to value

## EY and Microsoft

The digital technologies that are impacting your business today — social, mobile, analytics and cloud — are rapidly expanding to create new employee and customer experiences, fundamentally changing how your organization works, interacts and competes. The EY and Microsoft alliance combines EY deep insights and experience in disruptive industry trends, new business models and evolving processes with Microsoft scalable, enterprise cloud platform and digital technologies. 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. Together, we can help accelerate digital strategy and amplify your business performance to thrive in a digital world.

For more information, visit: ey.com/microsoft.

## Contact information

### EY contacts:

**Darren Simpson**
Partner
EY Asia Pacific Cybersecurity
Ernst & Young Australia
darren.simpson@au.ey.com

### Microsoft contacts:

**Jodi Lustgarten**
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.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. 005691-21Gbl

ED None



ey.com