Microsoft Security

Microsoft Security Experts

CY2022 Q3 – Industry Solutions Managed Services

Contents

Microsoft Security Experts

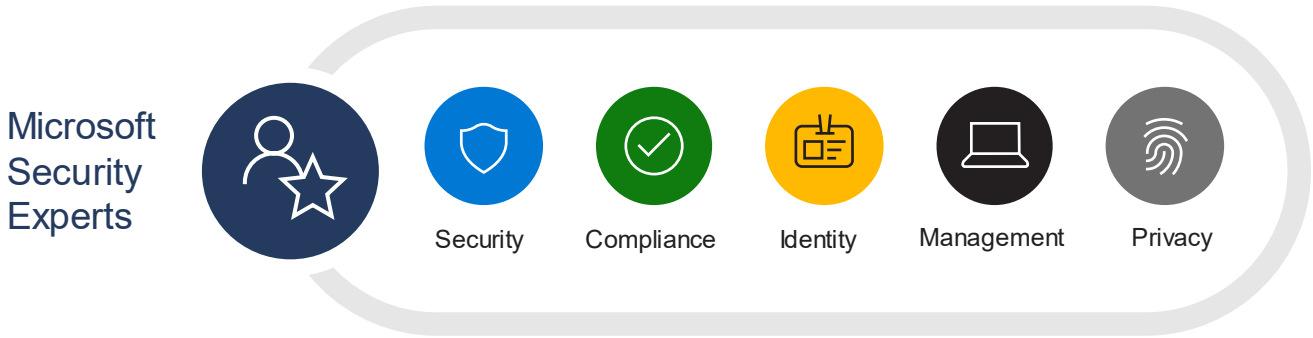
Purpose of this document

Microsoft understands that customers who use our managed services entrust us with their most valued asset, their data. This document will provide additional clarity around how data is stored and used to deliver the services offered by **Microsoft Security Experts**. Specifically, this document covers the following services: **Microsoft Security Services for Enterprise**, **Microsoft Security Services for Incident Response**, and **Microsoft Security Services for Modernization**. All of these services from Industry Solutions will be outlined along with the data collection and privacy questions on how these will operate within a customer's data environment.

Microsoft Security Experts

Today, cybersecurity has reached an inflection point, the United States is facing a cybersecurity talent shortage with nearly one in three—or 2.5 million—security jobs vacant[1] pushing time of detection for a breach to an alarming 287 days.[2] And, even when talent is available, access to highly skilled expertise remains a challenge.

Microsoft created Microsoft Security Experts, a new line of services to help customers achieve better security outcomes that spans across Microsoft Security's product categories: security, compliance, identity, management, and privacy. Security Experts includes managed services, incident response, and advisory services. For more details refer to the announcement blog here.



America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce, Brad Smith, Official Microsoft Blog, Microsoft. October 28, 2021. [1] Cost of a Data Breach Report 2021, IBM.

Services overview

Microsoft Security Services for Enterprise

Security Services for Enterprise was created for large enterprise customers that want Microsoft to "do it for me." This comprehensive, expert-led service combines proactive threat hunting and (Managed Extended Detection and Response (MXDR) with dedicated Microsoft security experts to manage onboarding, daily interaction, practice modernization, and incident response. This service uses Microsoft's complete Security information and event management (SIEM) and Extended Detection and Response (XDR) stack to protect all cloud environments and all platforms.

Website

Microsoft Security Services for Incident Response

Security Services for Incident Response was created to support customers before, during and after a breach. Security Services for Incident Response will help you remove a bad actor from the customers' environment, build resilience for future attacks, and mend defenses after a breach. Microsoft's global team of experts leverages strategic partnerships with security organizations and governments around the world and with internal Microsoft product groups to respond to incidents and help customers secure their most sensitive, critical environments.

Website

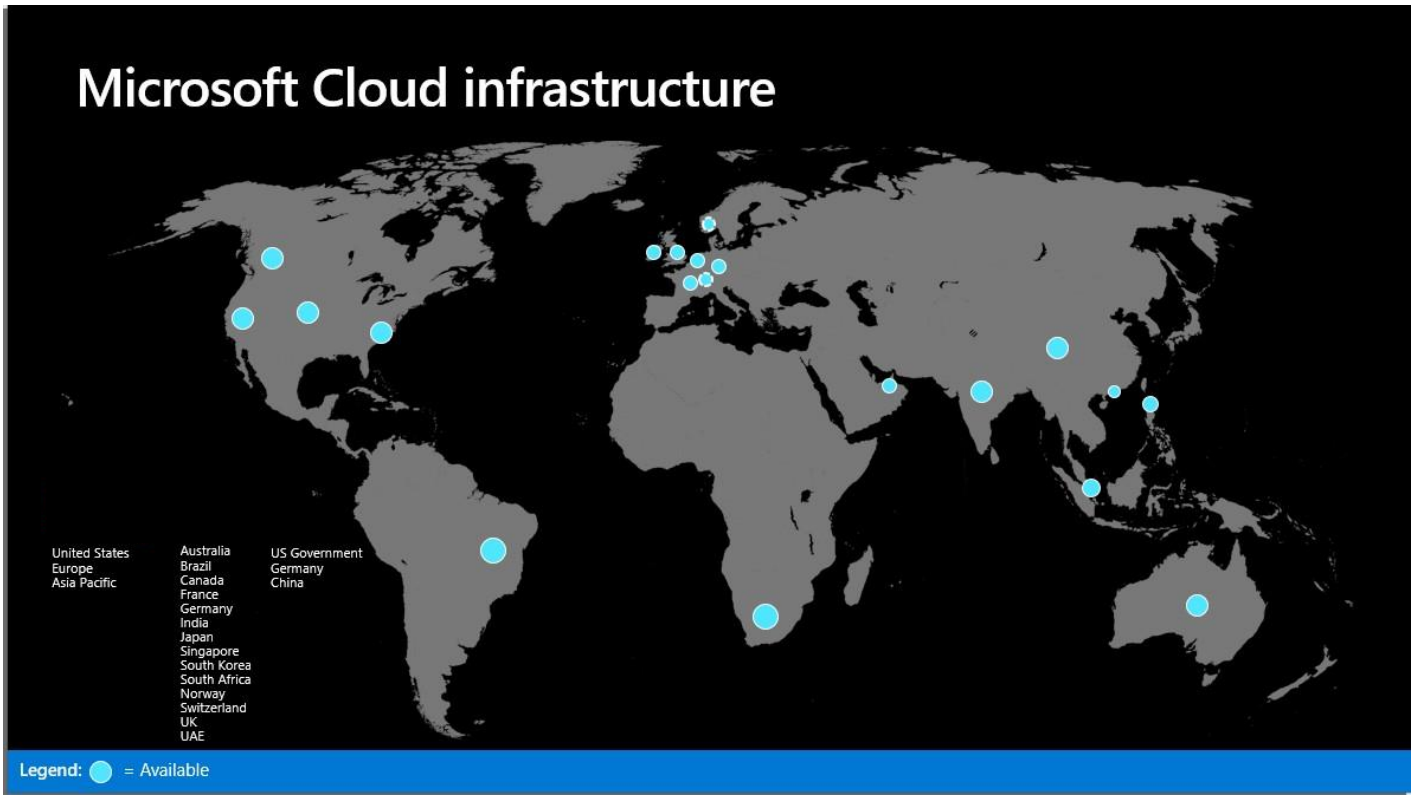
Microsoft Security Services for Modernization

Security Services for Modernization was created for customers that want to leverage Microsoft best practices and know-how as they embrace new modern security capabilities and embark on their Security transformation. Security Services for Modernization provides consulting services that help customers at any stage of their security journey modernize their security posture and embrace a zero-trust approach. Our modernization services utilize extensive cybersecurity knowledge and industry expertise gathered over 35 years to keep customers secure.

Website

Datacenter locations

Microsoft Security Experts benefits from a worldwide network of datacenters. These are set up around the world in 17 different locations, making Microsoft one of the top three global networks. This level of localization helps organizations' more easily meet dataresidency, sovereignty, and compliance requirements. Please see the latest Microsoft's compliance offerings here.



International availability

These services are available to commercial cloud customers worldwide except as limited by applicable regulations. More specifically, these services observe all applicable travel, trade and export regulations, including those from the U.S. Department of State regarding travel restrictions, the U.S. Department of Treasury regarding embargoed and sanctioned countries and the International Trade Administration regarding Export Administration Regulations (EAR).

Microsoft Security Services for Enterprise

Overview

The Microsoft Security Services for Enterprise program utilizes proven security processes and techniques to securely protect the information our team is granted access to view in the customer environment. Because of the sensitive nature of the secure events and incidents that our team is charged with monitoring and remediating for you, we have established a Zero Trust model for our solution to prevent the unauthorized disclosure of any information to unauthorized parties.

The following service also leverages Microsoft Defender Experts for Hunting, whose trust and privacy information can be found here. The service also includes parts of Microsoft Security Services for Incident Response (page 11) and Microsoft Security Services for Modernization (page 13).

Data collection

We limit the data collected into our case management solution to only those events that are populated by the Microsoft Sentinel solution, or from customer generated informational requests or security log data.

Should our analysts' teams need to perform an investigation of a machine in question, those log files are stored in a secure Azure Storage account within the customer's tenant. This will allow the analyst to continue to review the event and subsequent logs without taking ownership of the file(s) itself or placing it in a Microsoft owned storage location.

For any security logs that our team reviews, we fully understand that the ownership of that content belongs to our customer. This means that we will not transfer any content outside of the customers designated cloud service boundary without the customers express approval, and only when our team requires additional services to be performed on the customers behalf, such as forensic analysis activities or deeper analysis, from within Microsoft's secure ecosystem.

As the owner of the data, you control who has access to the information and how you validate industry, government, or other regulatory compliance of that data. As our service is performed, all data is retained within the customers cloud boundaries to maintain compliance with corporate information service controls. This allows the customer to validate compliance using native Microsoft services and highlights any gaps that need remediation. Using our continuous improvement services included in the solution, our team can help define or refine policies to confirm compliance is enforced.

Data processing

Our team engages in the monitoring of selected security logs and services under the controls and limits of our contractual agreements. Should additional processing of data be recommended by our team, it will not be performed without the customers authorized consent. At no time is any of the customers data mined for market research of advertising purposes.

Secure Identity

Our solution makes use of a platform that provides identities and secure workstations to our authorized users. This platform makes use of multiple layers of security controls to prevent unauthorized access using traditional credential theft methods and supply chain attacks. Additionally, we have a dedicated team monitoring the platform itself for threats against individuals and/or the environment in which they operate.

Identity-based access controls

Using our Entitlement Management and access controls services which are native to Azure Active Directory, we continually monitor any privileged or non-privileged access request or group membership. Additionally, we utilize a 'no standing access' principle to remove users from any elevated role when not in use. This is accomplished with Azure Active Directory Privileged Identity Management within our platform that requires users to request access to any elevated privilege role and is validated with Multi-Factor Authentication rules.

Encryption and rights management

In addition to the encryption of data at rest and in transit, content sent to authorized individuals is protected with Azure Rights Management for all document files, emails, and other approved transportation methods.

Data storage

Microsoft Security Services for Enterprise makes use of a case management solution to collect events, alerts, and incidents from the customer's Microsoft Sentinel service. Our service is presently offered to customers from our solution hosted in the Azure US based datacenter region. Future expansion will comply with EU Data boundary requirements and support customers for data hosting in other country regions as demand requires.

Our case management solution is used to collect security events from the customer's Microsoft Sentinel solution so that our SOC analyst team can triage and mitigate the event in the most expeditions way possible. The information that is collected on our case management platform is used only by the Microsoft team performing this service for the customer. Please see the table below for details of sovereignty.

Geography	Current Status
United States (all data center regions)	Available now
Azure Government including DoD (United States Department of Defense), Intel, Fed Civilian and State and Local	Capacity driven – may require specific clearances, physical locations, and network connectivity to support specific regions
All other geographies	Supported from US geography when mutually confirmed by customer, future expansion will evaluate delivery from local Azure datacenter regions based on capacity growth and demand

Securing customer data at rest and in transit

All data within our platform is protected with native data encryption services, and all legacy data transport layer security protocols are blocked for access.

Azure Rights Management is used to protect all Microsoft 365 documentation regardless of its storage location in the platform. This includes content in our Secure Teams Collaboration solution, OneDrive for Business and SharePoint and Exchange Online/Outlook.

Secure Infrastructure

Our solution utilizes Azure Commercial cloud to host all services that our team uses, we do not rely on any legacy on-premises or Hybrid cloud solutions. We utilize the current Azure Security Benchmark and Enterprise Scale guidance to define policies for new service adoption, including restricting traffic to private endpoints and not using VPN services to connect to our customers. Future growth will introduce the transition of the solution to other Microsoft regional and sovereign clouds as the solution demand increases.

We utilize Azure Lighthouse and Entitlement Management to securely connect to our customer's environment and encourage the use of AAD PIM in their platform to additionally control access to their security services. Our least privileged security model ensures that we never have or retain standing privilege in the customer's environment, and we monitor access with audit logs and access reviews.

Secure apps and data

The secure device used by operations and analyst resources is tightly controlled in that it does not permit the end user to install or download any unauthorized applications. Using the AppLocker service, we also prevent users from running unapproved executables that may not require an installation package to be installed.

All traffic from the secure device is monitored through Microsoft Defender for Cloud Apps so that if needed additional conditional access notifications can be triggered when a user is attempting to perform specific activities, or a malicious user is attempting to compromise the service.

For both the secure workstation and the cloud environments, all data at rest and in transit is encrypted using the highest possible encryption and transport mechanism available. We utilize the latest Endpoint Detection and Response (EDR) tools to prevent unauthorized data egress from the solution to prevent intentional or unintentional distribution of information outside of the solution boundaries.

The firmware of each device is protected with a unique complex password preventing an attacker from booting the machine with a USB storage media. This protection also prevents the unauthorized modification of the firmware settings.

Compliance

For a complete list of the compliance status of the Microsoft Cloud services, please review the following website - Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Docs

Employee compliance

Microsoft's Confidential Information Policy prohibits Microsoft employees from disclosing customers' confidential information. Additionally, the Microsoft Security Services for Enterprise services agreement further requires that customer's confidential information can only be shared with Microsoft employees that have a need-to-know in furtherance of the engagement with the customer.

For the reasons above and given the overall importance of protecting the confidentiality of customers that may have suffered a security incident, Microsoft's position is to strictly limit access to information—even within Microsoft.

Auditing and logging

Our platform performs auditing and compliance against required governance controls to confirm the collection of logs centrally for our solution. Our automated deployment of new services provisions with logging enabled by default and collected into our Microsoft Sentinel SIEM environment for complete visibility across the solution.

Auditing of our own team's usage and access elevation requests are maintained to maintain compliance with internal reporting requirements. Access Reviews are maintained for all security groups to monitor proper assignments of service access for both privileged and non-privileged roles.

The platform security logs are retained securely for the required retention periods based on Microsoft legal requirements, and then expunged when no longer needed.

Additional resources

Microsoft Privacy Statement: https://aka.ms/privacy

Data management at Microsoft: https://www.microsoft.com/en-us/trust-center/privacy/data-management

Data Protection Addendum: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Microsoft Security Services for Incident Response

Overview

Microsoft Security Services for Incident Response (Security Services for Incident Response) will help to identify and then remove a bad actor from a customer environment, build resilience for future attacks, and mend defenses after an incident. This service combines both incident response and recovery.

For incident response, this service utilizes the talent of the Microsoft Detection and Response Team (DART) who provides reactive incident response and remote proactive investigations. DART works in conjunction with Microsoft Security Expert teams and Microsoft product groups to respond to incidents and help customers secure their most sensitive, critical environments.

It also includes recovery services leveraging the Compromise Recovery Security Practice (CRSP) team of security experts that help secure the customers post-breach environment by gaining administrative control and removing attacker from an environment and tactically increasing the customers security posture to prevent future breaches.

Data collection

Security Services for Incident Response support metadata artifacts from endpoints. We perform two types of collection, broad and targeted. Broad collection is performed via three proprietary tools. These tools collect data from common locations where forensic artifacts are left behind by attackers.

For Incident Response Investigation

Most of the data is analyzed from an Azure data explorer cluster. However, in some cases a forensic VM is created for an engagement for additional analysis. Security Services for Incident Response will receive customer consent before collecting this data for analysis.

Data analyzed is collected in Microsoft Azure, and all are geographically aligned with the region that is specified during the provisioning, for more information on these regions please see documentation here.

For Compromise Recovery

Microsoft Defender for Endpoint and Microsoft Defender for Identity are cloud-based storage tools. For questions regarding data storage and privacy information, please view the links below:
Microsoft Defender for Endpoint data storage and privacy | Microsoft Docs
Microsoft Defender for Identity frequently asked questions | Microsoft Docs

Analysis also requires read access for Microsoft Defender for Endpoint, Microsoft Defender for Identity, Azure Active Directory, and Office 365.

Data storage

The Microsoft Security Services for Incident Response delivery team complies with the following guidance for data storage found here.

Compliance

Regulatory standards

Microsoft Security Services for Incident Response conforms to the same regulatory compliance standards that Azure, Dynamics 365, and Microsoft 365 products and services. You can find more details here.

Employee compliance

Microsoft's Confidential Information Policy prohibits Microsoft employees from disclosing customers' confidential information. Additionally, the Microsoft Security Services for Enterprise services agreement further requires that customer's confidential information can only be shared with Microsoft employees that have a need-to-know in furtherance of the engagement with the customer.

For the reasons above and given the overall importance of protecting the confidentiality of customers that may have suffered a security incident, Microsoft's position is to strictly limit access to information—even within Microsoft.

Additional resources

Microsoft Privacy Statement: https://aka.ms/privacy
Data management at Microsoft: https://www.microsoft.com/en-us/trust-center/privacy/data-management
Data Protection Addendum: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Microsoft Security Services for Modernization

Overview

Rapid transformation has come at a potential cost; many businesses have been left more exposed to security and compliance risks, and others don't have the right technologies to enable secure remote access to corporate resources at scale. Microsoft Security Services for Modernization (Security Services for Modernization) helps customers embrace digital innovation and modernize their platforms to enable their people to be productive from anywhere and on any device, while maintaining the security and privacy of their data.

Microsoft Security Services for Modernization has developed a Modern Enterprise Security Framework for end-to-end security transformations, covering Security, Compliance, Identity, Management, and Privacy. This Framework brings to our customers the value of all aspects of Microsoft's Intelligent Security capabilities across Azure and M365, spanning Identity and Access Management, Threat Protection, Information Protection and Cloud Security, while aligning with the principles of Zero Trust. Security Services for Modernization provides a cohesive customer value proposition with associated solutions to address each customer's specific enterprise security needs.

Data collection

Encryption and rights management

Technological safeguards, such as encryption, enhance the security of support and consulting data. For data in transit, Security Services for Modernization uses industry-standard encrypted transport protocols between user devices and Microsoft datacenters as well as within the datacenters themselves.

Identity-based access controls

Security Services for Modernization develops requirements and designs systems that prevents personnel with authorized access to support and consulting data from using it for purposes beyond those identified for their roles. Systems have limited export functionality and often employ field-level security (for example, a system may not display data fields that are not relevant to an individual's role, even though the individual has authorized access to the system). These controls also help prevent support and consulting data from being read, copied, altered, or removed without authorization.

Security Services for Modernization conducts user access reviews on an ongoing basis. Our password controls enforce complexity, periodic rotation, and suspension when specified periods of user inactivity are detected. We restrict data and system access to individuals who have a genuine business need based on the principle of least privilege. Employees and contingent staff who have access to support and consulting data, or who are in a role that could impact customer information, have privacy and security requirements embedded in their roles and responsibilities.

Data storage

Security Services for Modernization stores data worldwide based on the location of the consulting work, along with the United States and other locations where Microsoft may have Global Delivery service centers. Customer data can be deployed into the Microsoft Azure datacenters (also referred to as "regions") listed here.

Security Services for Modernization stores Commercial Technical Support data in in the United States, along with the following locations:

- Data with increased sensitivity is stored regionally in either the United States, the European Union or APAC depending on the location of the sender of a file
- Call recordings are stored in either United States or locally in call centers worldwide. For information on the location of a call center, ask the agent who responded to a call for their location
- To provide support, data may be viewed or downloaded onto a laptop at the location of Microsoft personnel. A full list of geographies where Microsoft support is provided is available upon request through the customers' account team.

With Security Experts for Modernization, customers can specify the region where their customer data will be stored. Microsoft may replicate customer data to other regions available within the same geography for data durability, except as specified below. No matter where customer data is stored, Microsoft does not control or limit the locations from which customers, or their end users may access customer data.

Data location

Microsoft will not transfer customer data outside the selected Azure geographic location (geo) for Security Services for Modernization. Microsoft is committed to data sovereignty in the European Union (EU) through our EU Data Boundary (EUDB) initiative. More information can be found here.

Compliance

Regulatory standards

Microsoft Security Services for Modernization conforms to the same regulatory compliance standards that Azure, Dynamics 365, and Microsoft 365 products and services. You can find more details here.

Employee and Subcontractor compliance

Microsoft Security Services for Modernization employees are required to sign agreements that commit them to confidentiality regarding support and consulting data. Internal tools contain data protection notices to remind employees and data handlers of their responsibility for any sensitive data that the tool may contain. Security Services for Modernization holds all third parties, including contractors and subcontractors, to the same security standards as full-time employees.

Subcontractors who work with Microsoft Security Services for Modernization must follow Microsoft's data protection standards. All other subcontractors must follow equivalent data protection standards. Microsoft subcontractor agreements are designed to ensure the safeguarding of customer information, including regular monitoring of the subcontractors' work.

Additional resources

Microsoft Privacy Statement: https://aka.ms/privacy

Data management at Microsoft: https://www.microsoft.com/en-us/trust-center/privacy/data-management

Data Protection Addendum: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA