Microsoft Security

Microsoft Security Experts

CY2023 Q3 – Industry Solutions Services

Contents

Microsoft Security Experts

Overview 3
Services overview 4
Datacenter locations 5
International availability 5

Microsoft Incident Response

Overview 11
Data collection 11-12
Data storage 12
Compliance 12
Additional Resources 12

Microsoft Security Services for Modernization

Overview 13
Data collection 13-14
Data storage 14
Compliance 15
Additional Resources 15

Microsoft Security Experts

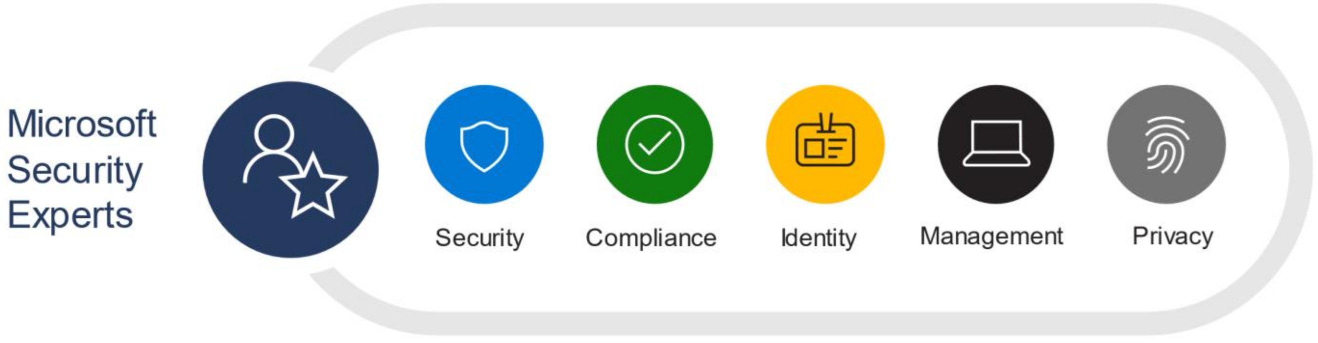
Purpose of this document

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 Incident Response**, and **Microsoft Security Services for Modernization**. All 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.



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 Incident Response

Microsoft Incident Response was created to support customers before, during and after a breach. Microsoft 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

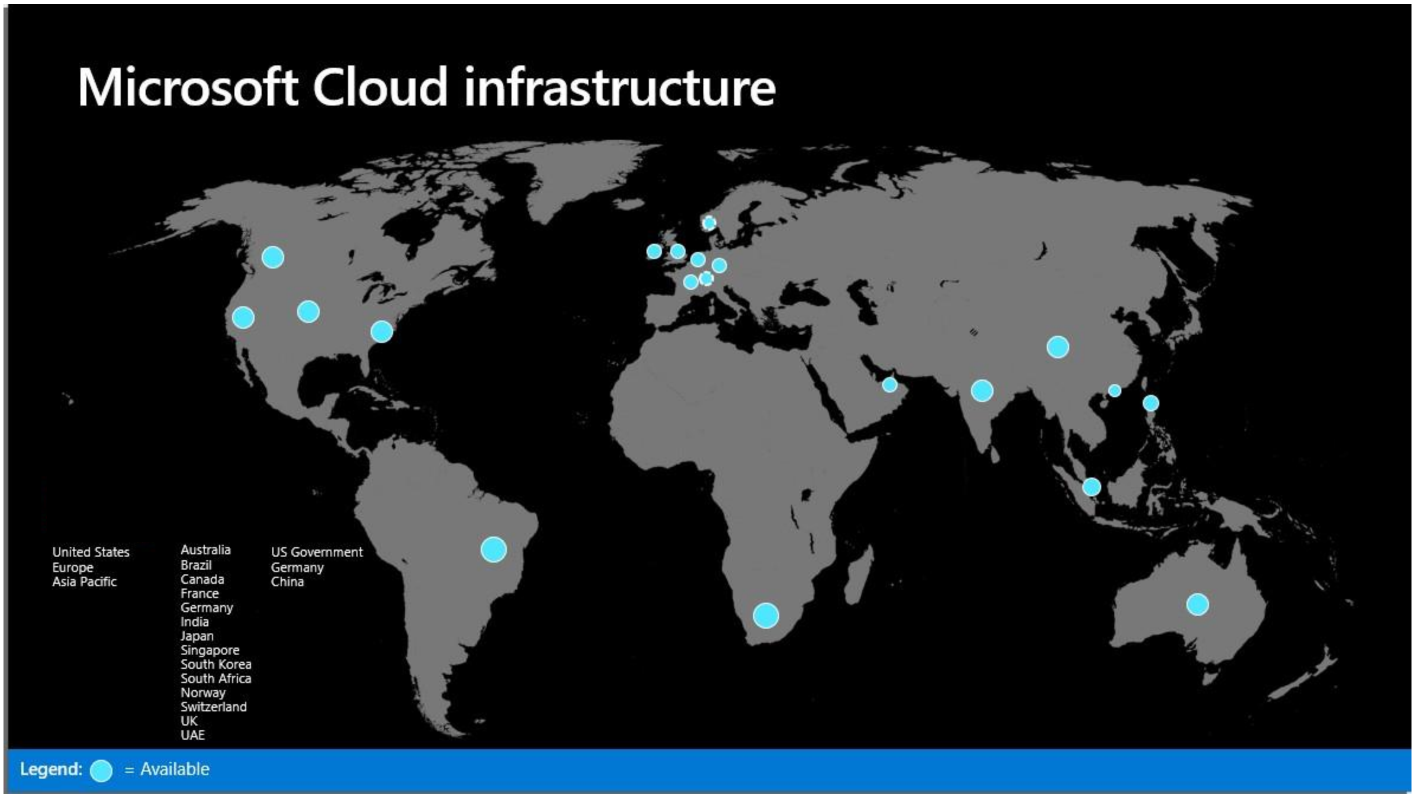
Microsoft Security Services for Modernization

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.



Microsoft Cloud infrastructure

United States
Europe
Asia Pacific

Australia
Brazil
Canada
France
Germany
India
Japan
Singapore
South Korea
South Africa
Norway
Switzerland
UK
UAE

US Government
Germany
China

Legend: ● = Available

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 Incident Response

Overview

Microsoft 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 Incident Response team who provides reactive incident response and remote proactive investigations. Microsoft Incident Response team 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 Microsoft Incident Response team and their compromise recovery 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

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

Compliance

Regulatory standards

Microsoft 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