Microsoft Cloud Security for Enterprise Architects

What IT architects need to know about security and trust in Microsoft cloud services and platforms

This topic is 1 of 5 in a series 1 2 3 4 5

Introduction to Security in a Cloud-Enabled World

Security in the cloud is a partnership

The security of your Microsoft cloud services is a partnership between you and Microsoft.

Microsoft	You
Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications.	You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control (varies by service type).

Microsoft's Trusted Cloud principles

Security	Safeguarding your data with state-of-the-art technology, processes, and encryption is our priority.
Privacy & Control	Privacy by design with a commitment to use customers' information only to deliver services and not for advertisements.
Compliance	The largest portfolio of compliance standards and certifications in the industry.
Transparency	We explain what we do with your data, and how it is secured and managed, in clear, plain language.

The responsibilities and controls for the security of applications and networks vary by the service type.

SaaS
Software as a Service

Microsoft operates and secures the infrastructure, host operating system, and application layers. Data is secured at datacenters and in transit between Microsoft and the customer.

You control access and secure your data and identities, including configuring the set of application controls available in the cloud service.

PaaS
Platform as a Service

Microsoft operates and secures the infrastructure and host operating system layers.

You control access and secure your data, identities, and applications, including applying any infrastructure controls available from the cloud service.

You control all application code and configuration, including sample code provided by Microsoft or other sources.

IaaS
Infrastructure as a Service

Microsoft operates and secures the base infrastructure and host operating system layers.

You control access and secure data, identities, applications, virtualized operating systems, and any infrastructure controls available from the cloud service.

Private cloud

Private clouds are on-premises solutions that are owned, operated, and secured by you. Private clouds differ from traditional on-premises infrastructure in that they follow cloud principles to provide cloud availability and flexibility.

Keys to success

Enterprise organizations benefit from taking a methodical approach to cloud security. This involves investing in core capabilities within the organization that lead to secure environments.

Governance & Security Policy

Microsoft recommends developing policies for how to evaluate, adopt, and use cloud services to minimize creation of inconsistencies and vulnerabilities that attackers can exploit.

Ensure governance and security policies are updated for cloud services and implemented across the organization:

- Identity policies
- Data policies
- Compliance policies and documentation

Administrative Privilege Management

Your IT administrators have control over the cloud services and identity management services. Consistent access control policies are a dependency for cloud security. Privileged accounts, credentials, and workstations where the accounts are used must be protected and monitored.

Identity Systems and Identity Management

Identity services provide the foundation of security systems. Most enterprise organizations use existing identities for cloud services, and these identity systems need to be secured at or above the level of cloud services.

Threat Awareness

Organizations face a variety of security threats with varying motivations. Evaluate the threats that apply to your organization and put them into context by leveraging resources like threat intelligence and Information Sharing and Analysis Centers (ISACs).

Data Protection

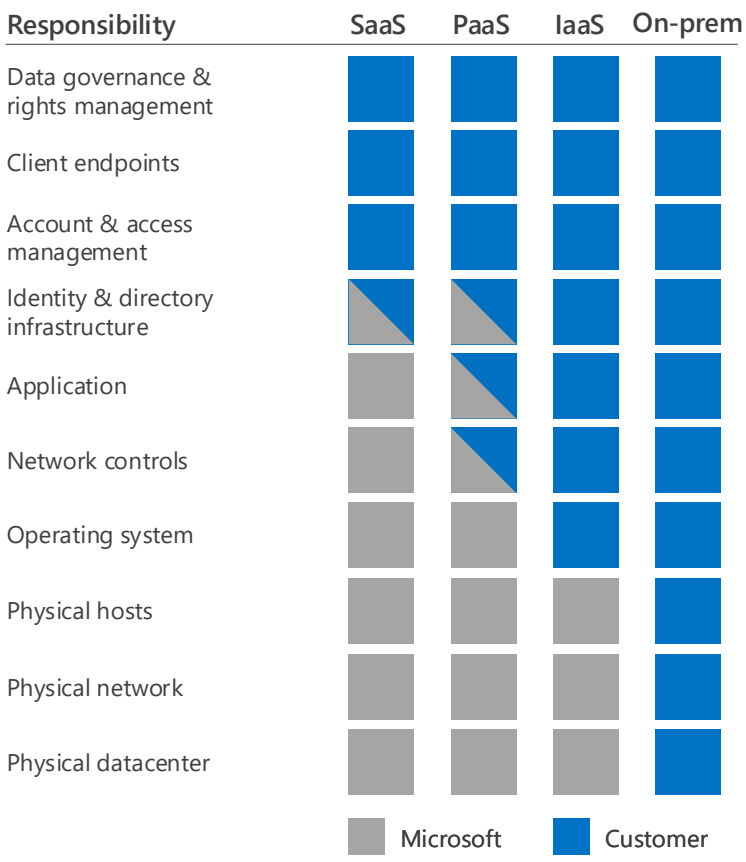
You own your data and control how it should be used, shared, updated, and published.

You should classify your sensitive data and ensure it is protected and monitored with appropriate access control policies wherever it is stored and while it is in transit.

Microsoft Virtual Academy

Microsoft Cybersecurity Reference Strategies
http://aka.ms/cyberstrategy

Your responsibility for security is based on the type of cloud service. The following chart summarizes the balance of responsibility for both Microsoft and the customer.



See pages 2-5 for more information and resources.

December 2018

Microsoft

Microsoft Cloud Security for Enterprise Architects

What IT architects need to know about security and trust in Microsoft cloud services and platforms

Top security certifications

Many international, industry, and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards and are trusted. By providing customers with compliant, independently verified cloud services, Microsoft also makes it easier for you to achieve compliance for your infrastructure and applications.

This page summarizes the top certifications. For a *complete list of security certifications* and more information, see the Microsoft Trust Center.

View compliance by service
microsoft.com/en-us/trustcenter/compliance/complianceofferings

Global

- ☑ ISO 27001:2013
- ☑ ISO 27017:2015
- ☑ ISO 27018:2014
- ☑ ISO 22301:2012
- ☑ ISO 9001:2015
- ☑ ISO 20000-1:2011
- ☑ SOC 1 Type 2
- ☑ SOC 2 Type 2
- ☑ SOC 3
- ☑ CSA STAR Certification
- ☑ CSA STAR Attestation
- ☑ CSA STAR Self-Assessment
- ☑ WCAG 2.0 (ISO 40500:2012)

US Gov

- ☑ FedRAMP High
- ☑ FedRAMP Moderate
- ☑ EAR
- ☑ DFARS
- ☑ DoD DISA SRG Level 5
- ☑ DoD DISA SRG Level 4
- ☑ DoD DISA SRG Level 2
- ☑ DoE 10 CFR Part 810
- ☑ NIST SP 800-171
- ☑ NIST CSF
- ☑ Section 508 VPATs
- ☑ FIPS 140-2
- ☑ ITAR
- ☑ CJIS
- ☑ IRS 1075

Regional

- ☑ Argentina PDPA
- ☑ Australia IRAP Unclassified
- ☑ Australia IRAP PROTECTED
- ☑ Canada Privacy Laws
- ☑ China GB 18030:2005
- ☑ China DJCP (MLPS) Level 3
- ☑ China TRUCS / CCCPPF
- ☑ EN 301 549
- ☑ EU ENISA IAF
- ☑ EU Model Clauses
- ☑ EU – US Privacy Shield
- ☑ GDPR
- ☑ Germany C5
- ☑ Germany IT-Grundschutz workbook
- ☑ India MeitY
- ☑ Japan CS Mark Gold
- ☑ Japan My Number Act
- ☑ Netherlands BIR 2012
- ☑ New Zealand Gov CC Framework
- ☑ Singapore MTCS Level 3
- ☑ Spain ENS
- ☑ Spain DPA
- ☑ UK Cyber Essentials Plus
- ☑ UK G-Cloud
- ☑ UK PASF

Industry

- ☑ PCI DSS Level 1
- ☑ GLBA
- ☑ FFIEC
- ☑ Shared Assessments
- ☑ FISC (Japan)
- ☑ APRA (Australia)
- ☑ FCA (UK)
- ☑ MAS + ABS (Singapore)
- ☑ 23 NYCRR 500
- ☑ HIPAA BAA
- ☑ HITRUST

Industry

- ☑ 21 CFR Part 11 (GxP)
- ☑ MARS-E
- ☑ NHS IG Toolkit (UK)
- ☑ NEN 7510:2011 (Netherlands)
- ☑ FERPA
- ☑ CDSA
- ☑ MPAA
- ☑ DPP (UK)
- ☑ FACT (UK)
- ☑ SOX

Microsoft

Microsoft Cloud Security for Enterprise Architects

What IT architects need to know about security and trust in Microsoft cloud services and platforms

Microsoft's role

Microsoft is committed to the privacy and security of your data and applications in the cloud

Through industry-leading security practices and unmatched experience running some of the largest online services around the globe, Microsoft delivers enterprise cloud services customers can trust.

Decades of engineering experience has enabled Microsoft to develop leading-edge best practices in the design and management of online services. This page summarizes Microsoft's comprehensive approach, starting with your data and drilling down to the physical media and datacenters. Be sure to review the customer responsibilities to learn about your role in the security partnership.

Learn more...

Microsoft Trust Center

Data Privacy

Data ownership

It's your data.

We define "customer data" as all the data (including all text, sound, software, or image files) that a customer provides, or that is provided on customers' behalf, to Microsoft through use of the Online Services.

Data use

We do not use customer data for purposes unrelated to providing the service, such as advertising. We have a No Standing Access policy — access to customer data by Microsoft personnel is restricted, granted only when necessary for support or operations, and then revoked when no longer needed.

Disclosure of government request for data

If a government approaches us for access to customer data, we redirect the inquiry to you, the customer, whenever possible. We have and will challenge in court any invalid legal demand that prohibits disclosure of a government request for customer data.

Learn more . . .

Law Enforcement Requests Report

Data access

You are in control of your data. You have control over where your data is stored and how it is securely accessed and deleted. Depending on the service, you choose where your data is stored geographically.

Privacy reviews

As part of the development process, privacy reviews are performed to verify that privacy requirements are adequately addressed. This includes verifying the presence of privacy-related features that allow customers to control who can access their data and configure the service to meet the customer's regulatory privacy requirements.

Data portability

It's your data, so if you ever choose to leave the service, you can take your data with you and have it deleted permanently from our servers.

Read more...

Protecting Data and Privacy in the Cloud

Data encryption and rights management

Data in transit

Best-in-class encryption is used to help secure data in transit between datacenters and you, as well as at Microsoft datacenters. Additionally, customers can enable Perfect Forward Secrecy (PFS). PFS uses a different encryption key for every connection, making it more difficult for attackers to decrypt connections.

Encryption for Azure-based solutions

For Azure-based solutions, you can choose to implement additional encryption using a range of approaches — you control the encryption method and keys. Built-in TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.

Azure Key Vault

Safeguard cryptographic keys and other secrets used by cloud apps and services. Microsoft does not see or extract your keys.

Data at rest

Office 365 and other SaaS services use encryption at rest to protect your data on Microsoft servers.

Azure Information Protection

Azure Information Protection uses encryption, identity, and authorization policies to help secure your files and email. Protection stays with the files and emails, independently of the location — inside or outside your organization, networks, file servers, and applications.

- Azure Information Protection for Office 365 is built to work across multiple workloads such as Exchange, SharePoint, and Office documents.
- You can bring your own key to comply with your organization policies.

Learn more...

Azure Information Protection

Identity and access

You control access to your data and applications

Microsoft offers comprehensive identity and access management solutions for customers to use across Azure and other services such as Office 365, helping them simplify the management of multiple environments and control user access across applications.

Conditional access and multi-factor authentication

Azure Active Directory enables customers to manage access to Azure, Office 365, and a world of other cloud apps. Conditional access and multi-factor authentication offer enhanced security.

Third-party SaaS identity management

Azure AD enables easy integration and single sign-on to many of today's popular SaaS applications, such as Salesforce.

Continued on next page

Software and services

Secure Development Lifecycle (SDL)

Privacy and security considerations are embedded through the SDL, a software development process that helps developers build more secure software and address security and privacy compliance requirements. The SDL includes:

- Risk assessments
- Attack surface analysis and reduction
- Threat modeling
- Incident response
- Release review and certification

Secure development across the Microsoft cloud

Microsoft Azure, Office 365, Dynamics CRM Online, and all other enterprise cloud services use the processes documented in the SDL.

Learn more...

Security Development Lifecycle

Proactive testing and monitoring

Learn more...

Microsoft Digital Crimes Unit

Microsoft's Digital Crimes Unit (DCU) seeks to provide a safer digital experience for every person and organization on the planet by protecting vulnerable populations, fighting malware, and reducing digital risk.

Microsoft Cyber Defense Operations Center

The Microsoft Cyber Defense Operations Center is a 24x7 cybersecurity and defense facility that unites our security experts and data scientists in a centralized location. Advanced software tools and real-time analytics help us protect, detect, and respond to threats to Microsoft's cloud infrastructure, products and devices, and our internal resources.

Prevent Breach, Assume Breach

In addition to the "prevent breach" practices of threat modeling, code reviews, and security testing, Microsoft takes an "assume breach" approach to protecting services and data:

- Simulate real-world breaches
- Live site penetration testing
- Centralized security logging and monitoring
- Practice security incident response

Read more...

Microsoft Enterprise Cloud Red Teaming

Datacenter infrastructure and networking security

Operational Security for Online Services (OSA)

OSA is a framework that focuses on infrastructure issues to help ensure secure operations throughout the lifecycle of cloud-based services.

Learn more...

Operational Security for Online Services (OSA)

Private connection

Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.

Learn more...

Microsoft Azure ExpressRoute

Physical datacenter security

24-hour monitored physical security

Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

Zero standing privileges

Microsoft maintains a No Standing Access policy on customer data. We've engineered our products so that a majority of service operations are fully automated and only a small set of activities require human involvement. Access by Microsoft personnel is granted only when necessary for support or operations; access is carefully managed and logged, then revoked when no longer needed. Datacenter access to the systems that store customer data is strictly controlled via lock box processes.

Data destruction

When customers delete data or leave a service, they can take their data with them and have it deleted permanently from Microsoft servers. Microsoft follows strict standards for overwriting storage resources before reuse, as well as for the physical destruction of decommissioned hardware. Faulty drives and hardware are demagnetized and destroyed.

Learn more...

Video: Microsoft Cloud Azure Data Center(s) – The Inside Long Tour

Microsoft

Microsoft Cloud Security for Enterprise Architects

What IT architects need to know about security and trust in Microsoft cloud services and platforms

Customer responsibilities and roadmap

Take a systematic approach to security for on-premises and in the cloud

While Microsoft is committed to the privacy and security of your data and applications in the cloud, customers must take an active role in the security partnership. Ever-evolving cybersecurity threats increase the requirements for security rigor and principles at all layers for both on-premises and cloud assets. Enterprise organizations are better able to manage and address concerns about security in the cloud when they take a systematic approach.

Moving workloads to the cloud shifts many security responsibilities and costs to Microsoft, freeing your security resources to focus on the critically important areas of data, identity, strategy, and governance.

Refer to these example solutions for implementation guidance:

[Microsoft Security Guidance for Political Campaigns, Nonprofit Organizations, and Other Agile Organizations]

[Microsoft 365 Enterprise Documenation]

[Office 365 security roadmap – Top priorities for the first 30 days, 90 days, and beyond]

Important: How to use this page

This page includes a methodical list of actions that Microsoft recommends to defend your data, identities, and applications against cybersecurity threats. These actions are categorized and presented in a stack. Categories at the top of the stack apply across SaaS, PaaS, IaaS, and private cloud. The scope of categories decreases further down the stack.

SaaS Software as a Service	PaaS Platform as a Service	IaaS Infrastructure as a Service	Private cloud

1. Security strategy, governance, and operationalization: Provide clear vision, standards, and guidance for your organization

A. Develop cloud security policies

Policies enable you to align your security controls with your organization's goals, risks, and culture. Policies should provide clear unequivocal guidance to enable good decisions by all practitioners.

- **Document security policies** in enough detail to guide personnel into quick and accurate decisions while adopting and managing cloud services. Ensure you have sufficient detail on policy areas that are well-established and critically important to your security posture.
- **Balance security and usability**. Security controls that overly restrict the ability of admins and users to accomplish tasks will be worked around. Build buy-in through both threat education and inclusion in the security design process.
- **Document protocols and processes** for performing critically important security tasks such as using administrative credentials, responding to common security events, and recovering from significant security incidents.
- **Embrace "Shadow IT."** Identify the unmanaged use of devices, cloud services, and applications. Identify business requirements that led to their use as well as the business risk that they bring. Work with business groups to enable required capabilities while mitigating risks.

B. Manage continuous threats

The evolution of security threats and changes require comprehensive operational capabilities and ongoing adjustments. Proactively manage this risk.

- **Establish operational capabilities** to monitor alerts, investigate incidents, initiate remediation actions, and integrate lessons learned.
- **Build external context** of threats using available resources such as threat intelligence feeds, Information Sharing and Analysis Centers (ISACs), and other means.
- **Validate your security posture** by authorized red team and/or penetration testing activity.

[White paper: Microsoft Enterprise Cloud Red Teaming]

C. Manage continuous innovation

The rate of capability releases and updates from cloud services requires proactive management of potential security impacts.

- **Define a monthly cadence** to review and integrate updates of cloud capabilities, regulatory and compliance requirements, evolving threats, and organizational objectives.
- **Prevent configuration drift with periodic reviews** to ensure technologies, configurations, and operational practices stay in compliance with your policies and protocols.

D. Contain risk by assuming breach

When planning security controls and security response processes, assume an attacker has compromised other internal resources such as user accounts, workstations, and applications. Assume an attacker will use these resources as an attack platform.

Modernize your containment strategy by:

- **Identifying your most critical assets** such as mission-critical data, applications, and dependencies. Security for these must be at a higher level without compromising usability.
- **Enhancing isolation between security zones** by increasing rigor of exception management. Apply threat modelling techniques to all authorized exceptions and analysis of these application data flows including identities used, data transmitted, application and platform trustworthiness, and ability to inspect interaction.
- **Focus containment within a security zone** on preserving integrity of the administrative model rather than on network isolation.

Continued on next page

SaaS Software as a Service	PaaS Platform as a Service	IaaS Infrastructure as a Service	Private cloud

2. **Administrative control:** Defend against the loss of control of your cloud services and on-premises systems

A. Least privilege admin model

Apply "least privilege" approaches to your administrative model, including:

- Limit the number of administrators or members of privileged groups.
- Delegate less privileges to accounts.
- Provide privileges on demand ("just in time").
- Have existing administrators perform tasks instead of adding additional administrators.
- Provide processes for emergency access and rare use scenarios.

Securing Privileged Access

Enable Azure AD Privileged Identity Management

Use privileged access management in Office 365

B. Harden security dependencies

Security dependencies include anything that has administrative control of an asset. Ensure that you harden all dependencies at or above the security level of the assets they control. Security dependencies for cloud services commonly include identity systems, on-premises management tools, administrative groups and accounts, and workstations where these accounts logon.

Microsoft Advanced Threat Analytics

C. Use strong authentication

Use credentials secured by hardware, multi-factor authentication (MFA), and conditional access for all identities with administrative privileges. This mitigates risk of stolen credentials being used to abuse privileged accounts.

Azure Multi-Factor Authentication

Conditional access in Azure Active Directory

Authenticating identities without passwords through Microsoft Passport

D. Use dedicated admin accounts and workstations

Separate high impact assets from highly prevalent internet browsing and email risks:

- Use dedicated accounts for privileged administrative roles for cloud services and on-premises dependencies.
- Use dedicated, hardened workstations for administration of high-business impact IT assets.
- Do not use high privilege accounts on devices where email and web browsing take place.

Securing Privileged Access

White paper: Security Management in Microsoft Azure

E. Enforce stringent security standards

Administrators control significant numbers of organizational assets. Rigorously measure and enforce stringent security standards on administrative accounts and systems. This includes cloud services and on-premises dependencies such as Active Directory, identity systems, management tools, security tools, administrative workstations, and associated operating systems.

F. Monitor admin accounts

Closely monitor the use and activities of administrative accounts. Configure alerts for activities that are high impact as well as for unusual or rare activities.

Enable Azure AD Privileged Identity Management

Cloud App Security

G. Educate and empower admins

Educate administrative personnel on likely threats and their critical role in protecting their credentials and key business data. Administrators are the gatekeepers of access to many of your critical assets. Empowering them with this knowledge will enable them to be better stewards of your assets and security posture.

3. **Data:** Identify and protect your most important information assets

A. Establish information protection priorities

The first step to protecting information is identifying what to protect. Develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets anywhere they reside.

File Protection Solutions in Office 365

Data classification toolkit

B. Protect High Value Assets (HVAs)

Establish the strongest protection for assets that have a disproportionate impact on the organizations mission or profitability. Perform stringent analysis of HVA lifecycle and security dependencies, and establish appropriate security controls and conditions.

C. Find and protect sensitive assets

Identify and classify sensitive assets. Define the technologies and processes to automatically apply security controls.

File Protection Solutions in Office 365

Secure SharePoint Online sites and files

Prevent data loss in Office 365

Office 365 information protection for GDPR

Azure Information Protection

Azure Key Vault

Always Encrypted (Database Engine)

SQL database dynamic data masking

D. Set organizational minimum standards

Establish minimum standards for trusted devices and accounts that access any data assets belonging to the organization. This can include device configuration compliance, device wipe, enterprise data protection capabilities, user authentication strength, and user identity.

Identity and Device Protection for Office 365

Identity and device access for Office 365 and other SaaS apps

E. Establish user policy and education

Users play a critical role in information security and should be educated on your policies and norms for the security aspects of data creation, classification, compliance, sharing, protection, and monitoring.

4. **User identity and device security:** Strengthen protection of accounts and devices

A. Use Strong Authentication

Use credentials secured by hardware or multi-factor authentication (MFA) for all identities to mitigate the risk that stolen credentials can be used to abuse accounts.

- User identities hosted in Azure Active Directory (Azure AD).
- On-premises accounts whose authentication is federated from on-premises Active Directory.

Azure Multi-Factor Authentication

Microsoft Passport and Windows Hello

Password-less phone sign-in with the Microsoft Authenticator app

B. Manage trusted and compliant devices

Establish, measure, and enforce modern security standards on devices that are used to access corporate data and assets. Apply configuration standards and rapidly install security updates to lower the risk of compromised devices being used to access or tamper with data.

Identity and device protection for Office 365 and other SaaS apps

C. Educate, empower, and enlist users

Users control their own accounts and are on the front line of protecting many of your critical assets. Empower your users to be good stewards of organizational and personal data. At the same time, acknowledge that user activities and errors carry security risk that can be mitigated but never completely eliminated. Focus on measuring and reducing risk from users.

- Educate users on likely threats and their role in protecting business data.
- Increase adversary cost to compromise user accounts.
- Explore gamification and other means of increasing user engagement.

Protect your account and devices from hackers and malware

4 ways to stay safe online (pdf)

4 ways to stay safe online (PowerPoint template)

D. Monitor for account and credential abuse

One of the most reliable ways to detect abuse of privileges, accounts, or data is to detect anomalous activity of an account.

- Identify activity that is normal and physically possible. Alert on unusual activity to enable rapid investigation and response.
- Use Cloud App Security to detect and alert on anomalous activity.
- For accounts in Azure AD, use the integrated analytics to detect unusual activity.

Cloud App Security

White paper: Microsoft Azure Security and Audit Log Management

Activity Reports in the Office 365 admin center

Continued on next page

PaaS
Platform as a Service

IaaS
Infrastructure as a Service

Private cloud

5. Application security: Ensure application code is resilient to attacks

A. Secure applications that you acquire

- Review the security development processes and operational practices of vendors before acquiring applications. Build this into your acquisition process.
- Follow security configuration guidance and recommendations provided by the vendor for the application.
- Apply all vendor security updates as rapidly as your testing requirements allow. Ensure to update middleware and dependencies installed with the applications.
- Discontinue your use of software before it reaches end of support status.

B. Follow the Security Development Lifecycle (SDL)

Software applications with source code you develop or control are a potential attack surface. These include PaaS apps, PaaS apps built from sample code in Azure (such as WordPress sites), and apps that interface with Office 365.

Follow code security best practices in the Microsoft Security Development Lifecycle (SDL) to minimize vulnerabilities and their security impact.

See: www.microsoft.com/sdl

6. Network: Ensure connectivity, isolation, and visibility into anomalous behavior

A. Update your network security strategy and architecture for cloud computing

Ensure your network architecture is ready for the cloud by updating your current approach or taking the opportunity to start fresh with a modern strategy for cloud services and platforms. Align your network strategy with your:

- Overall security strategy and governance
- Containment model and identity strategy
- Cloud services capabilities and constraints

Your design should address securing communications:

- Inbound from the Internet
- Between VMs in a subscription
- Across subscriptions
- To and from on-premises networks
- From remote administration hosts

Microsoft Cloud Networking for Enterprise Architects

Azure security best practices and patterns

B. Optimize with cloud capabilities

Cloud computing offers uniquely flexible network capabilities as topologies are defined in software. Evaluate the use of these modern cloud capabilities to enhance your network security auditability, discoverability, and operational flexibility.

C. Manage and monitor network security

Ensure your processes and technology capabilities are able to distinguish anomalies and variances in configurations and network traffic flow patterns. Cloud computing utilizes public networks, allowing rapid exploitation of misconfigurations that should be avoided or rapidly detected and corrected.

- Closely monitor and alert on exceptions.
- Apply automated means to ensure your network configuration remains correct and unusual traffic patterns are detected.

IaaS
Infrastructure as a Service

Private cloud

7. Operating system and middleware: Protect integrity of hosts

A. Virtual operating system

Secure the virtual host operating system (OS) and middleware running on virtual machines. Ensure that all aspects of the OS and middleware security meet or exceed the level required for the host, including:

- Administrative privileges and practices
- Software updates for OS and middleware
- Security Configuration Baseline
- Use of Group Policy Objects (GPOs)
- Installation methods and media
- Use of scheduled tasks
- Anti-malware and intrusion detection/prevention
- Host firewall and IPsec configurations
- Event log configuration and monitoring

B. Virtual OS management tools

System management tools have full technical control of the host operating systems (including the applications, data, and identities), making these a security dependency of the cloud service. Secure these tools at or above the level of the systems they manage. These tools typically include:

- Configuration Management
- Operations Management and Monitoring
- Backup
- Security Update and Patch Management

Microsoft Cloud Services and Network Security

Microsoft Azure Security blog

Azure security best practices and patterns

Continued on next page

Private cloud

8. Private cloud or on-premises environments: Secure the foundation

A. Physical network

Secure the networks you install and operate in your datacenters. Follow the guidelines and principles outlined in the Operating system and middleware section (above).

B. Fabric and datacenter identities

The accounts used to manage the fabric have technical control of the fabric, making them a security dependency of the fabric and all the services hosted on it. These include local and domain accounts with administrative privileges over systems including:

- Active Directory domains where fabric resources are joined
- Virtualization host operating systems
- Fabric management tools

Follow the security guidelines in the Administrative privileges and identities section (above) for these resources.

C. Server and device firmware

Firmware, the software embedded into the fabric hardware, is a security dependency of cloud services and a potential attack vector. Validate and harden this software, including the following:

- Baseboard Management Controllers (BMCs) for hardware "lights out" or remote access
- Server motherboard firmware
- Interface card firmware
- Dedicated appliance firmware/software

D. Storage

The security assurances of on-premises services depend on the security of the storage systems. These include:

- Storage management tools
- Storage administrator accounts and groups
- Workstations used by storage administrators
- Storage device operating systems and firmware

Secure these systems at or above the level required for all applications, identities, operating systems, and data hosted on them.

E. Physical operating systems and middleware

Operating systems and middleware installed on physical server hardware are a security dependency of the services that run on them. Secure these resources at or above the level required for the services and data hosted on the fabric using the guidelines in the Operating system and middleware section (above).

F. Physical security

Physical security assurances of the hardware hosting a cloud service must be at or above the level required for all of the applications, data, and identities hosted on it. Physical security protects all of the security dependencies, including:

- Server hardware
- Storage devices
- Network devices
- Administrative workstations
- Installation media
- Smart cards, one-time password tokens, and any passwords written on paper

G. Fabric management

The security assurances of the fabric are dependent on the security integrity of the software and tools used to manage it. These can include:

- Configuration management
- Operations management
- Virtual machine management
- Backup

Secure these resources at or above the level required for the services and data hosted on the fabric.

H. Virtualization solution

Virtual machines depend on the virtualization fabric for security assurances. The fabric includes:

- Virtualization management tools
- Virtualization administrators
- Workstations used by these administrators
- VM host operating systems
- Firmware on the VM host hardware

Secure these systems at or above the level required for all applications, identities, and data hosted on the virtualization solution.

For information about how Azure datacenters are secured, see:

- Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance
- Operational Security for Online Services Overview

More information

Microsoft Trust Center
http://www.microsoft.com/trustcenter

December 2018

Microsoft

Microsoft Cloud Security for Enterprise Architects

What IT architects need to know about security and trust in Microsoft cloud services and platforms

This topic is 5 of 5 in a series 1 2 3 4 5

A Cloud Security Journey

Microsoft has extensive experience in cybersecurity and threat detection and response. We provide professional services to our customers. The Microsoft Services Cybersecurity team is a team of world-class architects, consultants, and engineers that empowers organizations to move to the cloud securely, modernize their IT platforms, and avoid and mitigate breaches. Services include:

- High value asset protection
- Risk assessments
- Network monitoring and threat detection
- Incident response and recovery

This page lays out a typical cloud security roadmap based on our experience realizing business value from the cloud and defending cloud-based assets against cybersecurity threats.

A typical journey to the cloud includes key security transformations that span your organization's IT culture, governance, policy, processes technology, and security controls. The most common changes and challenges are:

- Establishing and validating trust of cloud providers.
- Shifting primary defenses to identity, data, and application layers.
- Keeping up with cloud security capabilities and controls.
- Keeping up with cybersecurity threats.

How can Microsoft Services help you?

Assessing and planning cloud security

Building a complete roadmap for cloud security requires knowing where you stand. Microsoft can help you build a tailored roadmap for:

- Security strategy and capabilities.
- Identity strategy and alignment.
- Office 365 security.
- Azure subscription and workload security.
- Information protection and rights management.

Threat detection and incident response

Microsoft has world-class incident response teams with extensive experience handling targeted attacks by determined adversaries. Microsoft can help you with detecting these threats, hunting for adversaries in your environment, responding to incidents, and recovering IT service integrity and availability after an attack. Services include:

- Incident response support (over the phone and onsite).
- Proactive hunt for persistent adversaries in your environment.
- Recovery from cybersecurity attacks.

Cloud workload migration and hardening

Microsoft can help you harden your current cloud assets, securely migrating workloads to the cloud, and creating new workloads in the cloud that are hardened from day one. Microsoft has expertise and experience to help you maximize your security assurances of cloud infrastructure and brand presence assets, including:

- Office 365 security configuration hardening.
- Azure workload analysis, migration, and security hardening.
- Hardened workstations for social media and brand management.
- Hardened consoles for cloud infrastructure administration.
- Hardening applications and application development processes for PaaS and hybrid applications using the Microsoft Security Development Lifecycle (SDL) and international standard ISO 27034-1.
- Designing, implementing, and securing private clouds.

Support, operations, and service management: sustaining the gains

Security in the cloud is a journey. Sustaining your security assurances requires ongoing investment into a maintainable operations model that encompasses people, processes, and technology. Microsoft Services provides a wide range of cloud and security IT support services, including IT staff training, health and risk assessments, and assistance with adoption of recommended practices. Microsoft IT Service Management (ITSM) services empower you to implement lifecycle management within IT by addressing the readiness of people and processes required to leverage technology capabilities effectively.

Administration, identity, and host security

Securing administrative privileges is critical for cloud services and the on-premises identity and security capabilities they depend on. Microsoft has developed industry leading solutions to protect and monitor administrative privileges that address challenges with people, process, and technology elements, including:

- Hardening administration of cloud services.
- Hardening administration of Active Directory and identity systems.
- Hardening infrastructure management tools and systems.
- Just-in-time and just enough administrative privileges.

Where to start?

Microsoft recommends starting with a view of your entire organization and addressing your top risks first:

- Assess your cloud security position to get a broad view of the road ahead.
- Enable advanced threat detection.
- Address top risks — protect business-critical social accounts and cloud administrative privileges accounts with hardened workstations and security tailored to those roles.

Getting started

Engaging Microsoft professional services

If you would like assistance with any of the cybersecurity or Trusted Cloud security capabilities described on this page, contact your Microsoft Services representative, or visit www.microsoft.com/services.

Security incident response

Customers with a Premier Support Agreement have ready access to highly specialized security support engineers and onsite incident response teams. For customers with an existing Premier agreement, no additional contracting action is necessary to initiate incident response activities from Microsoft. Contact your technical account manager (TAM) for more information.

More Microsoft cloud IT resources

Identity
aka.ms/cloudarchidentity

Networking
aka.ms/cloudarchnetworking

Hybrid
aka.ms/cloudarchhybrid

December 2018

Microsoft