EBOOK

McAfee
Together is power.

Definitive Guide to Azure Security

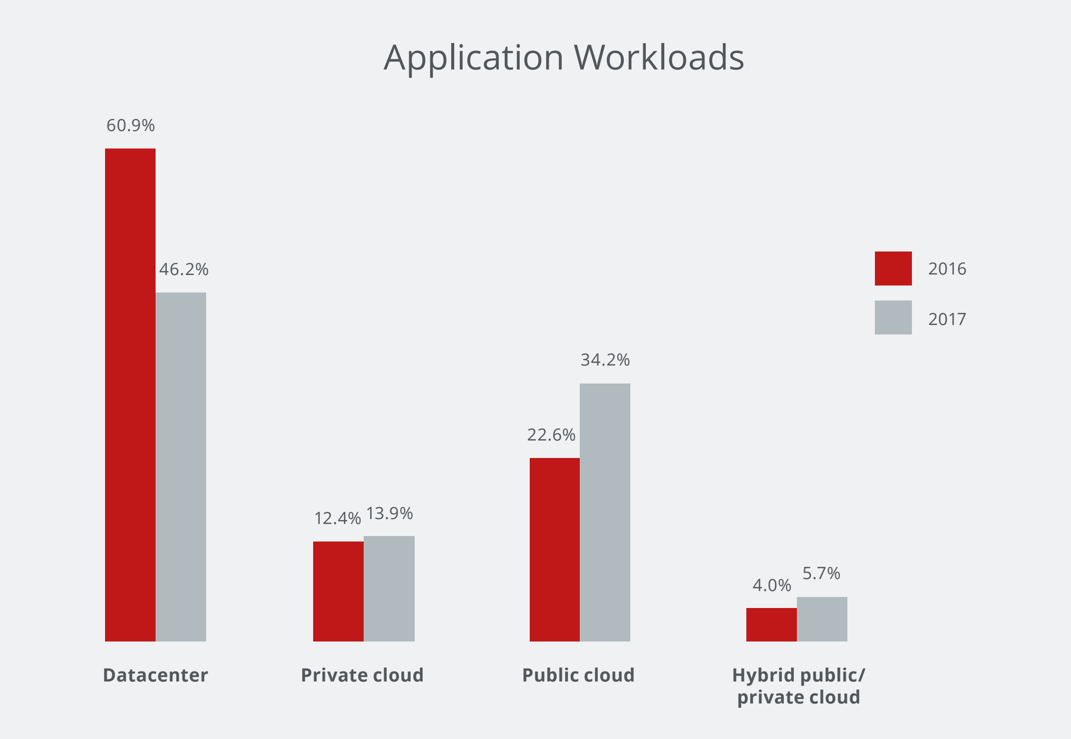
Table of Contents

Definitive Guide to Azure Security

Introduction: While popular out-of-the-box SaaS products like Salesforce, Box, Dropbox, and Office 365 are becoming common in the workplace, many enterprises have business needs that require custom-made applications.

At one time, enterprises relied on custom, in-house developed applications hosted in their own data centers. Having recognized the advantages of cloud computing, over the last 10 years these applications have slowly migrated to the public, private, or hybrid cloud. According to a Cloud Security Alliance report in 2017[1], 60.9% of all custom applications were being hosted in private datacenters as recently as 2016. However, cloud usage has reached a tipping point, and deployment of test and production application workloads in the public cloud is accelerating at the expense of enterprise data centers.

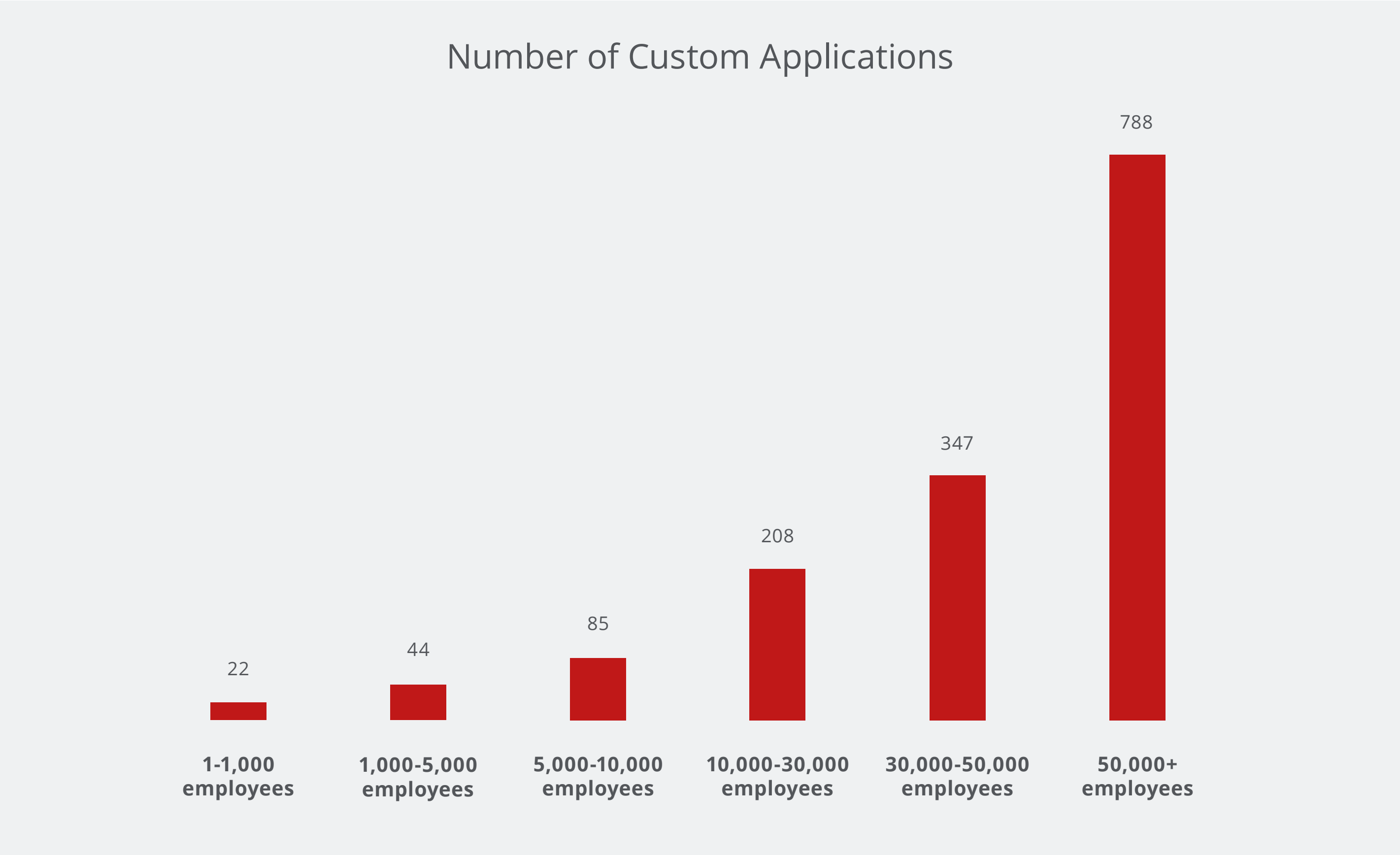
Not only are enterprises increasingly developing new custom applications on infrastructure-as-a- service (IaaS) platforms like Microsoft Azure, but enterprises are also migrating their existing custom applications and workloads to the public cloud. Collectively, these two trends have driven the percentage of custom applications running in the datacenter to an all-time low of 46.2% in 2017.



Application Workloads: Percentage deployed by infrastructure type

Connect With Us

[1] Custom Applications and IaaS Trends 2017, CSA Report



Number of Custom Applications: By company size

> “In terms of vendor share, Gartner expects 70 percent of public cloud services revenue to be dominated by the top 10 public cloud providers through 2021.”
>
> —Gartner

While the number of custom applications at an enterprise varies, the average enterprise has 465 custom applications deployed. Larger enterprises tend to have more applications—organizations with more than 50,000 employees have an average of 788 custom applications. Enterprises increasingly rely on these applications to handle business-critical functions. Most organizations today have at least one custom application that, if it experienced several hours of downtime, could have a significant impact on its business. Given the operational and financial disruption this could cause, these applications and the infrastructure they run on are increasingly lucrative as targets of cyber-attacks.

The worst-case scenario can be far worse than downtime

The Guardian released an article in 2016 about a data breach. One of the world's "big four" accountancy firms Deloitte was hacked. Deloitte provides auditing, tax, accounting, and high-end cybersecurity support to some of the world's largest banks, multinational firms, government agencies, pharmaceutical and media companies.

Attackers gained access to Deloitte's Azure cloud service they use to store emails that the staff sends and receives. The attackers gained access to an administrator account of the email service, which gave them control of sensitive data. They exposed emails to and from Deloitte's 244,000 staff. They may have also retrieved usernames, passwords, IP addresses, architectural diagrams for businesses and health information, but that hasn't yet been confirmed.

> "Platforms from leading CASB vendors were born in the cloud, designed for the cloud, and have a deeper understanding of users, devices, applications, transactions and sensitive data than CASB functions that are designed as extensions of traditional network security and SWG security technologies."
>
> —Gartner, Magic Quadrant for Cloud Access Security Brokers

Deloitte wasn't making security their number one priority. They could have protected their information and avoided this situation if they had used two-factor authentication instead of a single password.

The threat landscape is evolving rapidly, but with the right preparation, any company can implement security practices that significantly reduce the potential impact of a cyber-attack. In this eBook, we will discuss the current state of Azure adoption, Microsoft's model for Azure security, security challenges and threats to applications and data in Azure, and Azure infrastructure security best practices. Lastly, we will explore how a cloud access security broker (CASB) can help enterprises secure their Azure environments and the custom applications deployed in them.

Azure Adoption Trends

The IaaS market consists of three dominant players: Microsoft, Amazon, and Google. Azure has the highest growth rate almost doubling what AWS achieved. In their recent Q1 FY 2018 earnings report Microsoft reported[2] that revenue generated from Azure grew at 90% compared to Q1 FY 2017, which follows a similar growth (97%) they reported in their Q4 FY 2017 earnings report.

With the increase in Azure adoption, it isn't surprising to see that enterprises are gradually divesting from their data centers and moving application workloads to the public cloud. According to the CSA survey report, in 2016, 60.9% of applications workloads were still in enterprise datacenters. By the end of 2017, however, fewer than half (46.2%) remained there. This is, in part, due to new applications primarily being deployed in the cloud.

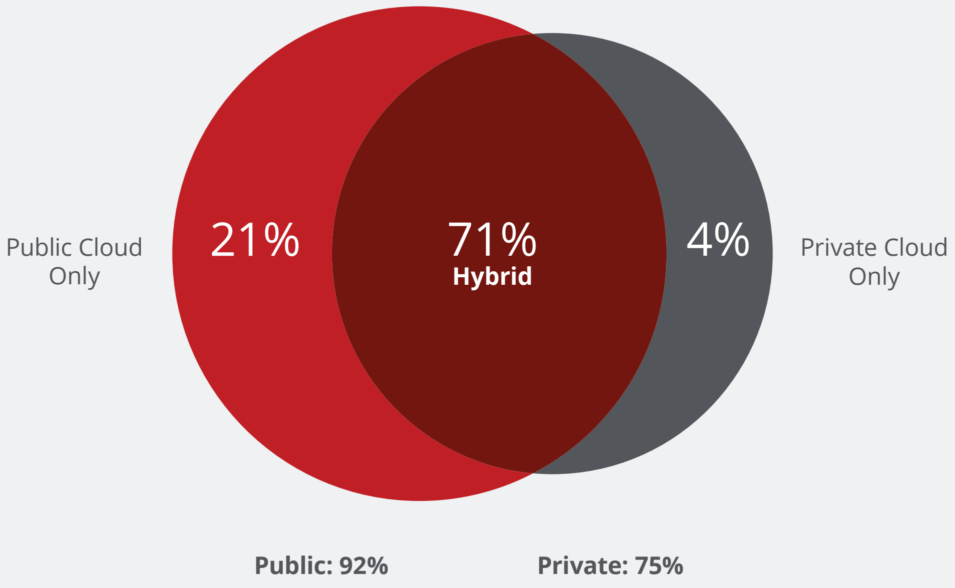
> "Cloud access security brokers have become an essential element of any cloud security strategy, helping organizations govern the use of cloud and protect sensitive data in the cloud."
>
> —Gartner, Magic Quadrant for Cloud Access Security Brokers

[2] Tech CNBC

Key public cloud adoption trends[3]

- Overall Azure adoption grew from 34% to 45% between 2017 to 2018
- Among enterprises, Azure increased adoption significantly, from 43% to 58%
- Public cloud adoption increased to 92% in 2018 from 89% in 2017
- More enterprises see public cloud as their top priority, up from 29% in 2017 to 38% in 2018
- 26% of enterprises spend more than $6 million a year on public cloud, while 52% spend more than $1.2 million annually
- 20% of enterprises plan to more than double their public cloud spend in 2018, and 71% will grow their public cloud spend by more than 20%

96% of Respondents Are Using Cloud



Source: RightScale 2018 State of the Cloud Report

[3] RightScale 2018 State of the Cloud Report

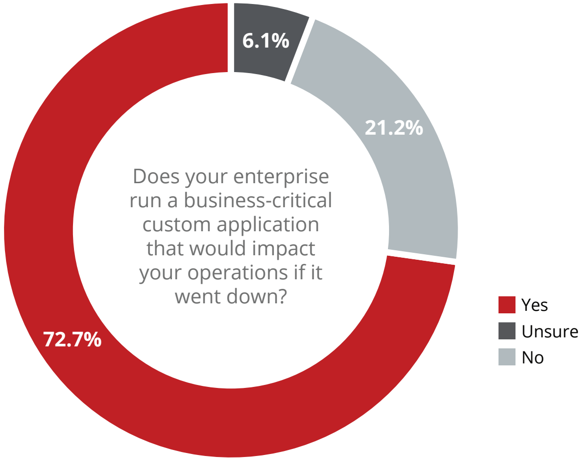
Azure Security Challenges

Threats to data and applications on Azure

Enterprises can't afford to have their Azure environment or the custom applications running on Azure, compromised. Enterprises store sensitive data such as credit card numbers and Social Security numbers in custom applications. 72.2% of enterprises have business critical applications–defined as an application that, if it experienced downtime, would greatly impact the organization's ability to operate. For example, an airline cannot operate if their flight path application goes down.

Business Critical Applications

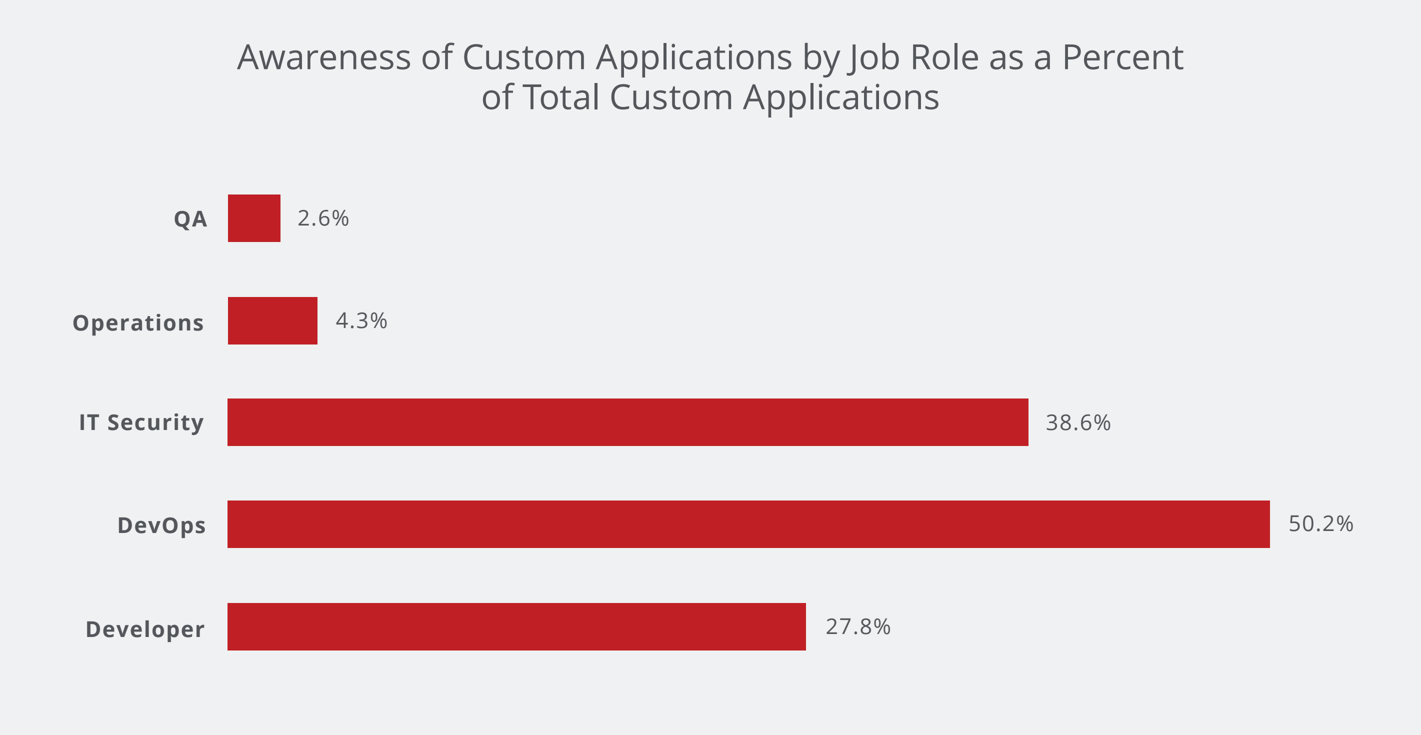
Percent of enterprises with at least one



Threats to applications running on Azure and the data stored within them can take many forms:

- **Denial-of-Service (DoS) attack on an application:** Azure has developed sophisticated DoS protection capabilities delivered in Azure Marketplace. However, it's possible a large attack could overwhelm Azure's defenses and take an application running on the platform offline for a period of time until the attack is remediated.
- **Insider threats and privileged user threats:** The average enterprise experiences 10.9 insider threats and 3.3 privileged user threats each month. These incidents include both malicious and negligent behavior. In most cases, well-intentioned employees will misconfigure an Azure service or otherwise overlook a critical security control that will expose the enterprise to security risks, but threats can come from privileged or malicious users as well.
- **Third-party account compromise:** According to the Verizon Data Breach Investigations Report[4], 63% of data breaches were due to a compromised account where the hacker exploited a weak, default, or stolen password. Misconfigured security settings or accounts that have excessive identity and access management (IAM) permissions can increase the potential damage.
- **Sensitive data uploaded against policy/regulation:** Many organizations have industry-specific regional regulations or internal policies, that prohibit certain types of data from being uploaded to the cloud. In some cases, data can be safely stored in the cloud, but only in certain geographic locations (e.g. datacenter in China but not in the United States).
- **Software development lacks security effort:** Unfortunately, IT security isn't always involved in the development or security of custom applications.

[4] 2016 Data Breach Investigations Report, Verizon



Awareness of custom applications by job role as a percent of total custom applications

IT security professionals are only aware of 38.6% of the custom apps. This means when it comes to custom application development, IT security is often bypassed, making the task of securing these applications more difficult.

According to Gartner, from now through 2020, 95% of security incidents in the cloud will be the fault of the customer, not the cloud provider. As enterprises continue to migrate to or build their custom applications in Azure, the threats they face will no longer be isolated to on-premises applications and endpoint devices. While the move to the cloud transfers some security responsibilities from the enterprise to the cloud provider, as we will see in the next section, preventing many of these threats is in the hands of the customers.

Shared responsibility model

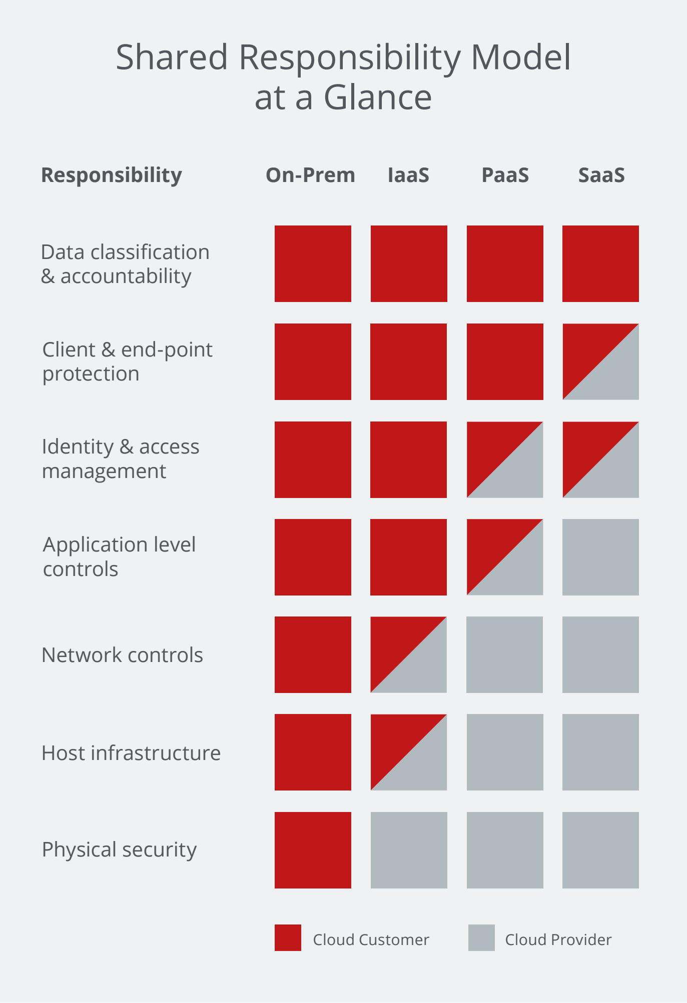
Like most cloud providers, Azure operates under a shared responsibility model. Azure takes responsibility for the security of its infrastructure and has made platform security a priority in order to protect customers' critical information. Azure detects fraud and abuse and responds to incidents by notifying customers. However, the customer is responsible for ensuring their Azure environment is configured securely, data is not shared with someone it shouldn't be shared with, identifying when a user misuses Azure, and enforcing compliance and governance policies.

Azure's Responsibility

Since Microsoft has little control over how Azure is used by its customers, Microsoft has focused on the security of Azure's infrastructure which includes computing, storage, and networking. Physical security of Azure infrastructure is the one responsibility that is wholly owned by Microsoft. Microsoft is responsible for the security of the software, hardware, servers, buildings, hypervisor, configuration of managed services, and the physical facilities that host Azure services.[5]

Customer's Responsibility

Azure customers are responsible for or share the responsibility for securing and managing the operating system, network configuration, applications, identity, clients, and data with Azure. Customers are responsible for ensuring that the data and its classification are done correctly, and that the solution will be compliant with regulatory obligations. The customer is responsible for managing their users and end-point devices.



Shared Responsibility Model at a Glance

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟥	🟥	🟥	🟥
Client & end-point protection	🟥	🟥	🟥	◩
Identity & access management	🟥	🟥	◩	◩
Application level controls	🟥	🟥	◩	⬜
Network controls	🟥	◩	⬜	⬜
Host infrastructure	🟥	◩	⬜	⬜
Physical security	🟥	⬜	⬜	⬜

🟥 Cloud Customer ⬜ Cloud Provider

[5] Microsoft Azure Security Blog

Detailed division of Azure security responsibility

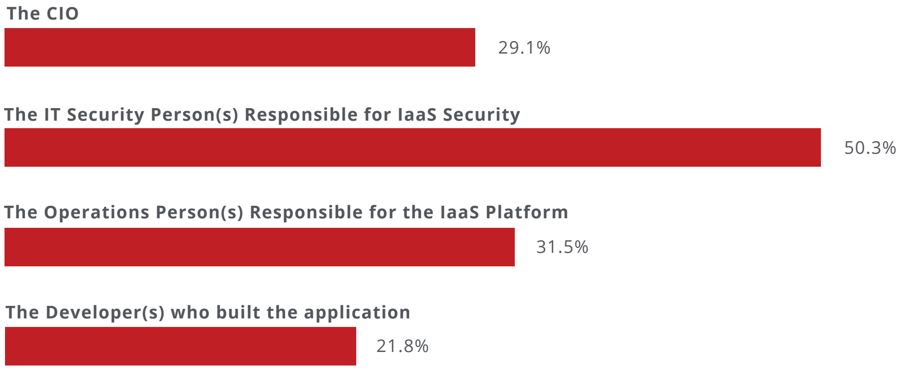
	Customer	Azure
Preventing or detecting when an Azure account has been compromised	•	
Preventing or detecting a privileged or regular Azure user behaving in an insecure manner	•	
Preventing sensitive data from being uploaded to or shared from applications in an inappropriate manner	•	
Configuring Azure services in a secure manner	•	
Restricting access to Azure services or custom applications to only those users who require it	•	
Updating Guest Operating Systems and applying security patches	•	
Ensuring Azure and custom applications are being used in a manner compliant with internal and external policies	•	
Ensuring network security (DoS, MITM, port scanning)	•	•
Providing physical access control to hardware/software		•
Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters		•
Database patching		•
Protecting against Azure zero-day exploits and other vulnerabilities		•
Business continuity management (availability, incident response)		•

Data breach fallout

An incident that results in downtime of even a few hours could have a considerable impact. For example, in August 2016, a six-hour application outage at Delta Airlines delayed flights for hundreds of thousands of passengers and is estimated to have cost the company tens of millions of dollars. With stakes this high, a data breach will likely lead to people getting fired. Both the CEO and CIO of Target were fired after a breach of 2014 that compromised payment card numbers for upwards of 40 million customers. In a 2017 survey of IT security leaders, 29.1% said the top IT leader would be let go following a damaging and costly data breach.

Who is Fired After a Breach

Percent of respondents



Azure Security Best Practices

Below are actionable best practices derived by McAfee Skyhigh Security Cloud customers. The list of best practices described below are meant for SecDevOps, Cloud Security Architects, Security Analysts, and Security Administrators.

Below are best practices for 7 critical areas of security in Azure that customers must follow to ensure their Azure workloads are secure:

1. Security Policy
2. Identify and Access Management
3. Storage Accounts
4. SQL Services
5. Networking
6. Virtual Machines
7. Miscellaneous

Security policy

1. **Ensure that 'data collection' is set to on.** Enable automatic provisioning of monitoring agent to collect security data. When Automatic provisioning of monitoring agent is turned on, Azure Security Center provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring agent provides alerts and scans for various security-related configurations and events such as system updates, OS vulnerabilities, and endpoint protection.

> **"McAfee's expansion of its security controls beyond SaaS is a key way IT can empower the business to fully leverage custom applications running in public IaaS, as well as having the confidence in protecting the IaaS platforms themselves."**
>
> —David Smoley, Chief Information Officer, AstraZeneca

2. **Ensure that 'system updates' is set to on.**
   Enable system updates recommendations for virtual machines. When this setting is enabled, Azure Security Center retrieves a daily list of available security and critical updates from Windows Update or Windows Server Update Services. The retrieved list depends on the service that's configured for that virtual machine and recommends that the missing updates be applied. For Linux systems, the policy uses the distro-provided package management system to determine packages that have available updates. It also checks for security and critical updates from Azure virtual machines.
3. **Ensure that 'OS vulnerabilities' is set to on.**
   Enable OS vulnerabilities recommendations for virtual machines. When this setting is enabled, it analyzes operating system configurations daily to determine issues that could make the virtual machine vulnerable to attack. The policy also recommends configuration changes to correct these vulnerabilities.
4. **Ensure that 'endpoint protection' is set to on.**
   Enable endpoint protection recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends endpoint protection be provisioned for all Windows virtual machines to help identify and remove viruses, spyware, and other malicious software.
5. **Ensure that 'disk encryption' is set to on.**
   Enable disk encryption recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends enabling disk encryption in all virtual machines to enhance data protection at rest.
6. **Ensure that 'network security groups' is set to on.**
   Enable network security groups recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends that network security groups be configured to control inbound and outbound traffic to virtual machines (VMs) that have public endpoints. Network security groups that are configured for a subnet is inherited by all virtual machine network interfaces unless otherwise specified. In addition to checking that a network security group has been configured, this policy assesses inbound security rules to identify rules that allow incoming traffic.
7. **Ensure that 'web application firewall' is set to on.**
   Enable web application firewall recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends that a web application firewall be provisioned on virtual machines when either of the following is true:
   - Instance-level public IP (ILPIP) is used and the inbound security rules for the associated network security group are configured to allow access to port 80/443.
   - Load-balanced IP is used and the associated load balancing and inbound network address translation (NAT) rules are configured to allow access to port 80/443.

8. **Ensure that 'next generation firewall' is set to on.**
   Enable next generation firewall recommendations for virtual machines. When this setting is enabled, it extends network protections beyond network security groups, which are built into Azure. Security Center will discover deployments for which a next generation firewall is recommended and enable you to provision a virtual appliance.
9. **Ensure that 'vulnerability assessment' is set to on.**
   Enable vulnerability assessment recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends that you install a vulnerability assessment solution on your VM.
10. **Ensure that 'storage encryption' is set to on.**
    Enable storage encryption recommendations. When this setting is enabled, any new data in Azure Blobs and Files will be encrypted.
11. **Ensure that 'JIT network access' is set to on.**
    Enable JIT network access for virtual machines. When this setting is enabled, the Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic should be locked down. Just-in-time VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
12. **Ensure that 'SQL auditing & threat detection' is set to on.**
    Enable SQL auditing & threat detection recommendations. When this setting is enabled, Azure Security Center recommends that auditing of access to Azure Database be enabled for compliance, advanced threat detection, and post-incident forensic investigations.
13. **Ensure that 'SQL encryption' is set to on.**
    Enable SQL encryption recommendations. When this setting is enabled, Azure Security Center recommends that encryption at rest be enabled for your Azure SQL Database, associated backups, and transaction log files. Even if your data is breached, it will not be readable.
14. **Ensure that 'security contact emails' and 'security contact phone number' is set to on.**
    Provide a security contact email address and phone number. This ensures that you are made aware of any potential compromise for timely incident response.
15. **Ensure that 'send email also to subscription owners' and 'send me emails about alerts' is set to on.**
    Enable security alerts emailing to security contact and subscription owners. This ensures that you are made aware of any potential compromise for timely incident response.

Identify and access management

1. **Ensure that for all users, multi-factor authentication is enabled.**
   Enable multi-factor authentication for all user credentials who have write access to Azure resources. Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.
2. **Ensure that there are no guest users.**
   Do not add guest users unless absolutely necessary. Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account. Until you have a business need to provide guest access to any user, avoid creating such users. Guest users are typically added out of your employee on-boarding/off-boarding process and could potentially still continue to access your resources unnoticed leading to a potential vulnerability.
3. **Ensure that 'allow users to remember multi-factor authentication on devices they trust' is disabled.**
   Do not allow users to remember multi-factor authentication on devices. Remembering multi-factor authentication (MFA) for devices and browsers allows you to give users the option to by-pass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that MFA is not bypassed.
4. **Ensure that 'number of methods required to reset' is set to 2.**
   Ensure that two alternate forms of identification are needed before allowing password reset. Setting up dual identification before allowing a password reset ensures that the user identity is confirmed via two separate forms of identification. With dual identification set, an attacker would require compromising both identity forms before they could maliciously reset a user's password.
5. **Ensure that 'number of days before users are asked to re-confirm their authentication information' is not set to 0.**
   Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0. If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user, such as a phone number or email changes, then the password reset information for that user goes to the previously registered authentication information.

6. **Ensure that 'notify users on password resets' is set to yes.**
   Ensure that the users are notified on their primary and secondary emails on password resets. User notification on password reset is a passive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.
7. **Ensure that 'notify all admins when other admins reset their password?' is set to yes.**
   Ensure that all administrators are notified if any other administrator resets her password. Administrator accounts are sensitive. Any password reset activity notification, when sent to all administrators, ensures that all administrators can passively confirm if such a reset is a common pattern within their group. For example, if all administrators change their password every 30 days, any password reset activity before that may inspect such an activity and confirm.
8. **Ensure that 'users can consent to apps accessing company data on their behalf' is set to no.**
   Require administrators to provide consent for the apps before use. Until you are running Azure Active Directory as an identity provider for third-party applications, do not allow users to use the identity outside of your cloud environment. User's profile information contains private information such as phone number and email address which could then be sold off to other third parties without requiring any further consent from the user.
9. **Ensure that 'users can add gallery apps to their Access Panel' is set to no.**
   Require administrators to provide consent for the apps before use. Until you are running Azure Active Directory as an identity provider for third-party applications, do not allow users to use the identity outside of your cloud environment. User's profile information contains private information such as phone number and email address which could then be sold off to other third parties without requiring any further consent from the user.
10. **Ensure that 'users can register applications' is set to no.**
    Require administrators to register third-party applications. It is recommended to let administrators register custom-developed applications. This ensures that the application undergoes a security review before exposing active directory data to it.
11. **Ensure that 'guest users permissions are limited' is set to yes.**
    Limit guest user permissions. Limiting guest access ensures that the guest accounts do not have permission for certain directory tasks, such as enumerate users, groups or other directory resources, and cannot be assigned to administrative roles in your directory.
12. **Ensure that 'members can invite' is set to no.**
    Restrict invitation through administrators only. Restricting invitation through administrators ensures that only authorized accounts have access to cloud resources. This helps to maintain 'Need to Know' and inadvertent access to data.

13. **Ensure that 'guests can invite' is set to no.**
    Restrict guest invitations. Restricting invitation through administrators ensures that only authorized accounts have access to cloud resources. This helps to maintain 'Need to Know' and inadvertent access to data.
14. **Ensure that 'restrict access to Azure AD administration portal' is set to yes.**
    Restrict access to Azure AD administration portal to administrators only. Azure AD administrative portal has sensitive data. You should restrict all non-administrators from accessing any Azure AD data in the administration portal to avoid exposure.
15. **Ensure that 'self-service group management enabled' is set to no.**
    Restrict group creation to administrators only. Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory (Azure AD). Until your business requires this day-to-day delegation to some users, it is good to disable self-service group management.
16. **Ensure that 'users can create security groups' is set to no.**
    Restrict security group creation to administrators only. When 'Users can create security groups' is enabled, all users in your directory are allowed to create new security groups and add members to these groups. Until your business require this day-to-day delegation, you should restrict security group creation to administrators only.
17. **Ensure that 'users who can manage security groups' is set to none.**
    Restrict security group management to administrators only. Restricting security group management to administrators only does not allow users to make changes to security groups. This ensures that security groups are appropriately managed, and their management is not delegated to any other user.
18. **Ensure that 'users can create Office 365 groups' is set to no.**
    Restrict Office 365 group creation to administrators only. Restricting Office 365 group creation to administrators only ensures that there is no proliferation of such groups. Appropriate groups should be created and managed by the administrator and such rights should not be delegated to any other user.
19. **Ensure that 'users who can manage Office 365 groups' is set to none.**
    Restrict Office 365 group management to administrators only. Restricting Office 365 group management to administrators only does not allow users to make changes to Office 365 groups. This ensures that Office 365 groups are appropriately managed, and their management is not delegated to any other user.

20. **Ensure that 'enable "all users" group' is set to yes.**
    Enable All Users group for centralized administration of all users. The All Users group can be used to assign the same permissions to all the users in your directory. For example, you can grant all users in your directory access to a SaaS application by assigning access for the All Users dedicated group to this application. This ensures that you can have a common policy created for all users and need not restrict permissions individually.
21. **Ensure that 'require multi-factor auth to join devices' is set to yes.**
    Joining devices to the active directory should require Multi-factor authentication. Multi-factor authentication is recommended when adding devices to Azure AD. When set to 'Yes' users that are adding devices from the internet must first use the second method of authentication before their device is successfully added to the directory. This ensures that rogue devices are not added to the directory for a compromised user account.

Storage accounts

1. **Ensure that 'secure transfer required' is set to enabled.**
   Enable data encryption is transit. The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When you are using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client.
2. **Ensure that 'storage service encryption' is set to enabled.**
   Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its data centers, and automatically decrypts it for you as you access it.

SQL services

1. **On SQL servers, ensure that 'auditing' is set to on.**
   Enable auditing on SQL Servers. Auditing tracks database events and writes them to an audit log in your Azure storage account. It also helps you to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
2. **On SQL servers, ensure that 'auditing type' is set to blob.**
   Enable object-level auditing on SQL Servers. Blob based auditing allows you to perform database object level auditing.

3. **On SQL servers, ensure that 'threat detection' is set to on.**
   Enable threat detection on SQL Servers. SQL Threat Detection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users will receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.
4. **On SQL servers, ensure that 'threat detection types' is set to all.**
   Enable all types of threat detection on SQL Servers. Enabling all threat detection types, you are protected against SQL injection, database vulnerabilities and any other anomalous activities.
5. **On SQL servers, ensure that 'send alerts to' is set.**
   Provide the email address to which alerts will be sent upon detection of anomalous activities on SQL Servers. Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.
6. **On SQL servers, ensure that 'email service and co-administrators' is enabled.**
   Enable service and co-administrators to receive security alerts from SQL Server. Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.
7. **On SQL servers, ensure that firewall rules are set as appropriate.**
   Enable firewall rules for SQL Server. To help protect your data, firewalls prevent all access to your database server until you specify which computers have permission. The firewall grants access to databases based on the originating IP address of each request.
8. **Auditing on SQL databases.**
   Enable auditing on SQL databases. Auditing tracks database events and writes them to an audit log in your Azure storage account.
9. **Threat detection on SQL databases.**
   Enable threat detection on SQL databases. SQL Threat Detection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. SQL Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.
10. **Threat detection types for SQL databases.**
    Enable all types of threat detection on SQL databases. Enabling all threat detection types, you are protected against SQL injection, database vulnerabilities and any other anomalous activities.

11. **On SQL Databases, ensure that 'send alerts to' is set to on.**
    Provide the email address to which alerts will be sent upon detection of anomalous activities on SQL databases. Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.
12. **Email service and co-administrators is enabled.**
    Enable service and co-administrators to receive security alerts from SQL databases. Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.
13. **Transparent data encryption on SQL databases.**
    Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Networking

1. **Disable RDP access on network security groups from internet.**
   Disable RDP access on Network Security Groups from Internet. The potential security problem with using RDP over the Internet is that attackers can use various brute-force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure.
2. **Disable SSH access on network security groups from internet.**
   Disable SSH access on Network Security Groups from Internet. The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure.
3. **Disable Telnet (port 23) access on network security groups from internet.**
   Disable unrestricted access on Network Security Groups (i.e. 0.0.0.0/0) on TCP port 23 and restrict access to only those IP addresses that require it in order to implement the principle of least privilege and reduce the possibility of a breach. TCP port 23 is used by the Telnet server application (Telnetd). Telnet is usually used to check whether a client is able to make TCP/IP connections to a particular service.

Virtual machines

1. **Install endpoint protection for virtual machines.**
   Install endpoint protection for virtual machines. Installing endpoint protection systems (antivirus/antimalware) provides real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems.
2. **Enable latest OS patch updates for virtual machines.**
   Ensure Latest OS Patches for virtual machines. Windows and Linux virtual machines should be kept updated to:
   - Address a specific bug or flaw
   - Improve an OS or application's general stability
   - Fix a security vulnerability
3. **Enforce disk encryption on virtual machines.**
   Ensure that data disks (non-boot volumes) are encrypted, where possible. Encrypting your IaaS VM's data disks (non-boot volume) ensures that its entire content is fully unrecoverable without a key and protects the volume from unwarranted reads.
4. **Enable VM agent on virtual machines.**
   Install VM agent on virtual machines. The VM agent must be installed on Azure virtual machines (VMs) in order to enable Azure Security Center for data collection. Security Center collects data from your VMs to assess their security state, provide security recommendations, and alert you to threats.

Miscellaneous

1. **Secure the subscription.**
   A secure cloud subscription provides a core foundation upon which subsequent development and deployment activities can be conducted. An engineering team should have the capabilities to deploy and configure security in the subscription including elements such as alerts, ARM policies, RBAC, Security Center policies, JEA, Resource Locks, etc. Likewise, it should be possible to check that all settings are in conformance to a secure baseline.
2. **Enable secure development.**
   During the coding and early development stages, developers should have the ability to write secure code and to test the secure configuration of their cloud applications.
3. **Minimize the number of admins/owners.**
   Each additional person in the Owner/Contributor role increases the attack surface for the entire subscription. The number of members in this role must be kept as low as possible.
4. **Justify all identities that are granted with admin/owner access on your subscription.**
   Accounts that are a member of these groups without a legitimate business reason, increase your risk. By carefully reviewing and removing accounts that shouldn't be there in the first place, you can avoid attacks if those accounts are compromised.

5. **Deprecated/stale accounts must not be present on the subscription.**
   Deprecated accounts are ones that were once deployed to your subscription for some trial/pilot initiative (or some other purpose). These are not required anymore and are a standing risk if present in any role on the subscription.
6. **Do not grant permissions to external accounts (i.e., accounts outside the native directory for the subscription).**
   Non-AD accounts (i.e. xyz@hotmail.com) present at any scope with a subscription, subject your cloud assets to undue risk. These accounts are not managed to the same standards as enterprise tenant identities. They don't have multi-factor authentication enabled.
7. **Service accounts cannot support MFA and should not be used for subscription activity.**
   Service accounts are typically not multi-factor authentication capable. Using service accounts in any privileged role in a subscription exposes it to 'credential theft'-related attack vectors.
8. **Azure Security Center (ASC) must be correctly configured on the subscription.**
   The Security Center feature in Azure helps with important central settings for the subscription such as configuring a security point of contact. It also supports key policy settings (e.g., is patching configured for VMs?, is threat detection enabled for SQL? etc.) and alerts about resources which are not compliant to those policy settings. Correctly configuring ASC is critical as it gives a baseline layer of protection for the subscription and commonly used resource types.
9. **Pending Azure Security Center (ASC) alerts must be resolved.**
   Based on the policies that are enabled in the subscription, Azure Security Center raises alerts. It is important that these alerts/actions are resolved promptly in order to eliminate the exposure to attacks.
10. **Service Principal Names (SPNs) should not be Owners or Contributors on the subscription.**
    Just like AD-based service accounts, SPNs have a single credential and most scenarios that use them cannot support multi-factor authentication. As a result, adding SPNs to a subscription in 'Owners' or 'Contributors' roles is risky.
11. **Critical application resources should be protected using a resource lock.**
    A resource lock protects a resource from getting accidentally deleted. With proper RBAC configuration, it is possible to setup critical resources in a subscription in such a way that people can perform most operations on them but cannot delete them. Resource locks can help ensure that important data is not lost by accidental/malicious deletion of such resources thus ensuring that availability is not impacted.

12. **Do not use custom-defined RBAC roles.**
    Custom RBAC role definitions are usually tricky to get right. As much as possible, customers should use these roles for their RBAC needs. Using custom roles is treated as an exception and must be rigorously reviewed.
13. **Do not use any classic resources on a subscription.**
    You should use new AzureRM (v2) resources as the ARM model; it provides stronger access control (RBAC) and auditing features.
14. **Do not use any classic virtual machines on your subscription.**
    You should use new AzureRM (v2) resources as the ARM model. It provides several security enhancements such as: stronger access control (RBAC), better auditing, ARM-based deployment/governance, access to managed identities, access to key vault for secrets, AAD-based authentication, support for tags and resource groups for easier security management, etc.
15. **Verify the list of public IP addresses on your subscription.**
    Public IPs provide direct access over the internet exposing a cloud resource to all type of attacks over the public network. Hence use of public IPs should be carefully scrutinized/reviewed.

> "McAfee helps us understand how employees use cloud to identify insider threats, compromised credentials, and excessive privileged user access."
>
> —Mark Bartholomy, Senior Manager Information Security, Western Union

Security Best Practices of Custom Applications

Information security is a shared responsibility, and not just between Azure and its customers. While developers may prioritize speed above all, IT security needs to be part of the software development process. They are an essential role in the architecture planning, auditing, and testing of applications. Application security is improved when the IT security team is involved from the beginning rather than bringing them in after an application has been developed.

Below are recommendations for creating a successful DevOps workflow that integrates security:

1. **Inventory and categorize all existing custom applications by the types of data stored and their compliance requirements and possible threats they face.**
   The first step in securing custom application development and usage is to inventory all existing applications and the data uploaded to them. IT security and audit teams should have visibility not only in the number of these apps running on Azure but also on whether sensitive data is being uploaded. Visibility into sensitive data enables the security team to identify which internal and external regulations apply to an app and its data and what kind of security controls must be in place.

2. **IT security should be involved in testing throughout the development process.** DevOps should invite the IT security team to bring their own application testing tools and methodologies when pushing production code without slowing down the process. Security should team up with the QA team to define test cases and qualifying parameters that should be met before code can be promoted. Developing a secure application isn't enough. IT security should also ensure that end users are using the application in a secure manner. With that in mind, there are a few steps the security team can take to ensure appropriate use of these applications.
3. **Grant the fewest privileges possible for users.** Unrestricted or overly permissive user accounts increase the risk and damage of an external or internal threat. Internally, a user with too many permissions might inadvertently cause data loss. Externally, a hacker who compromises an account with too many permissions can easily wreak havoc. For this reason, application administrators should limit a user's permission to a level where they can only do what's necessary to accomplish their job duties.

> "Through 2020, 95% of cloud security failures will be the customer's fault."
>
> —Gartner, Top Predictions for IT Organizations and Users for 2016 and Beyond

4. **Enforce a single set of data loss prevention policies across custom applications and all other cloud services.** The first step in enforcing DLP policies is inventorying existing DLP policies for all cloud services, on-premises applications, and endpoints, and identifying the policies that would apply to custom applications. Enterprises also need to understand how a custom application is being used, including the number of files containing sensitive data, the number of files being shared, and anomalous usage events indicative of threats. Some of the types of sensitive data that should be protected are:
   - Credit card numbers
   - Social Security numbers
   - Account numbers
   - Salaries
   - IP addresses
   - Account credentials
   - Intellectual property
5. **Encrypt highly sensitive data such as protected health information (PHI) or personally identifiable information (PII).** It is important to encrypt files containing sensitive information such as Social Security numbers or protected health information. In some cases, policies may be put in place that would block users from uploading files containing sensitive data that may not be encrypted.

How a CASB Helps Secure Workloads Running on Azure

Azure offers many built-in security capabilities, giving enterprises the ability to enforce a wide range of security, compliance, and governance policies. However, Azure settings can be very deep. In sprawling Azure environments, it can be prohibitive from a resource standpoint to manually check security configurations and user permissions for potential risks, and next to impossible to sift through the events provided to uncover potential threats. A cloud access security broker (CASB) helps automate the process of securing Azure– both the Azure platform and services as well as the custom applications you deploy in Azure.

On the infrastructure side, a mature CASB can provide comprehensive threat protection, monitoring, auditing, and remediation to secure all your Azure accounts. What follows are some of the things a CASB enables you to do.

1. **Analyze and audit Azure security configuration to ensure compliance and lower risk.**
   While Azure has provided a set of configurable controls to help protect an Azure account, it is entirely up to the customer to ensure these settings are configured appropriately, and any misconfiguration or change in configuration is identified and remediated in real-time. To that end, CASBs provide enterprises with the necessary security auditing that can automatically flag any security misconfiguration across all Azure accounts.

2. **Detect compromised accounts, insider threats, and privileged access misuse across Azure.** CASBs combine machine learning and user and entity behavior analytics (UEBA) to analyze cloud activity across multiple heuristics. This allows a CASB to develop a model for typical user behavior and detect anomalous activity patterns across Azure accounts and other cloud services that may be indicative of a threat. For example, if a user generally logs into Azure from New York then one day they log in from Bangkok, in a time frame so short it would be impossible to travel, a CASB can highlight this event and flag it for further investigation.

   CASBs detect compromised accounts based on impossible travel as well as excessive failed login attempts, brute-force attacks, login attempts from untrusted or disparate locations, etc. CASBs can also detect potential insider or privileged user threats by monitoring inappropriate escalation of privileges or repeated authorization failures. Machine learning makes it possible to detect these threats without configuring any rules or policies. CASBs also support the ability to tune the sensitivity of detection to narrow in on certain threats or cast a wider net.

3. **Perform forensic investigations with a complete audit trail of user activity.** CASBs provide complete and granular visibility into how users are using Azure. Using a CASB, an enterprise can readily detect (in real-time) creation, modification, or removal of Azure resources by any user. Security analysts can view the entire audit trail and filter by activity type, user, geography, and other dimensions. In doing so, a CASB can dramatically accelerate post-incident investigations and decrease incident response time.

4. **Identify excessive IAM permissions and dormant accounts.** A CASB can highlight dormant user accounts that have a heightened risk of being compromised. For example, if a user has been inactive for 90 days, a security alert can be triggered by the CASB for further investigation. Once the IAM user has been disabled, the alert will be resolved automatically without requiring any further action by the Azure administrator. CASBs can also identify excessive user permissions.

5. **Prevent unauthorized sensitive data from being stored in Azure storage services.** A CASB can leverage its content analytics engine to discover sensitive data stored in Azure based on keywords and phrases indicative of sensitive information, pre-defined alpha-numeric patterns with validation (e.g. credit card numbers), regular expressions, and file metadata, fingerprints of structured and unstructured information, and keyword dictionaries. CASBs help remediate DLP incidents by blocking or quarantining the action or notifying an administrator.

How a CASB Helps Secure Custom Applications Deployed on Azure

Traditionally, CASBs have focused on securing SaaS applications such as Salesforce, Box, and Office 365 by providing DLP, activity monitoring, threat protection, access control, and encryption. Today, a mature CASB can extend these same controls to all custom applications an enterprise deploys on Azure. One of the challenges today is that IT security is often not involved in the development process for new custom applications. A CASB makes it possible to extend these security controls to custom applications without any code changes, enabling organizations to secure their existing applications without any development resources. What follows are some of the things a CASB enables you to do.

1. **Capture a complete audit trail of user activity within the application.**
   CASBs provide complete and granular visibility into user and administrator activity within custom applications and across all other cloud services. CASBs reveal who is accessing which applications, what types of data are being uploaded or downloaded with what kind of device, and by whom. This level of visibility into activity supports compliance requirements and helps accelerate post-incident forensic investigation while decreasing incident response time.
2. **Limit access to data on BYOD devices and enforce other access control policies as needed.**
   While deploying custom applications on Azure provides the fundamental benefit of letting employees access critical resources from anywhere, at any time, using any device. It also introduces security risks because sensitive data could be exposed after downloading to an unmanaged or unsecure BYOD device. CASBs provide contextual access controls that enforce distinct access policies for custom applications based on whether the device is managed or unmanaged, if the IP is blacklisted or safe, or whether the traffic originates from a trusted or untrusted location. CASBs can also force additional authentication steps if predefined risk conditions are met.
3. **Detect insider/external threats and compromised accounts.**
   Given the ubiquity of compromised accounts, insider threats, and privileged user threats, CASBs provide threat protection to custom applications hosted in the cloud. CASBs not only analyze anomalous activities within a custom application, but also correlate activities across all custom and SaaS applications to sift through the noise and identify true threats. CASBs can create an alert when, for example, an internal employee downloads a large amount of data onto a personal device right before taking a position at a competitor company, or when a privileged user performs unwarranted permissions escalation. They can also detect external threats such as when a third party attempts to log in to an account using compromised credentials.

4. **Enforce data loss prevention.**
   Controlling the upload and sharing of sensitive data is one of the common use cases for a CASB. Highly regulated industries such as financial services, healthcare, and government, who want to take advantage of the benefits of cloud computing while staying compliant with internal and external policies turn to CASBs for their cloud data loss prevention requirements. The recommended platform approach to cloud data loss prevention (DLP) ensures that the same policies that protect data in SaaS and on-premises applications can be used to protect data in custom applications hosted on Azure. CASBs provide multiple remediation options when a policy violation occurs, including blocking the upload, coaching the user, or notifying an administrator.

5. **Encrypt data uploaded to custom applications.**
   Enterprises looking for an additional layer of security can use a CASB to encrypt data in custom applications using their own encryption keys. Using enterprise-owned encryption keys ensures that the IaaS provider cannot decrypt and view the data. Aside from strengthening the security of the custom application, storing data encrypted has another benefit. Numerous regional and industry-specific laws, including HIPAA-HITECH, require organizations to notify customers whose data has been compromised in a breach. However, if that data has been made indecipherable with encryption, organizations are exempt from the breach notification requirement.

> "Moving applications, data and workloads to the cloud exposes enterprises to new threats and risks. At the same time, the adoption of cloud allows organizations to transform their business. This is why we are on a mission to make cloud the most secure environment for business, and the introduction of our Azure security solution is an important step to fulfilling this mission for our customers."
>
> —Rajiv Gupta, Senior VP of the Cloud Business Unit, McAfee

Learn More About McAfee Skyhigh Security Cloud for Azure

Our Azure security solution is a comprehensive monitoring, auditing, and remediation solution for your Azure environment and custom applications.

Visita us at **www.mcafee.com**.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com