WHITE PAPER

CDW PEOPLE WHO GET IT™

SECURING YOUR AZURE DEPLOYMENT

Microsoft delivers robust **security** with its cloud platform, but protecting data and applications requires a commitment from enterprises as well.

EXECUTIVE SUMMARY

Many organizations find Microsoft's Azure cloud computing platform an indispensable part of their IT environment. Once they adopt Azure and other cloud computing services, security becomes an essential consideration. Organizations of all sizes are implementing these services to achieve agility, flexibility, scalability and cost savings, but worry whether adopting them jeopardizes their security posture, particularly in today's sophisticated threat environment.

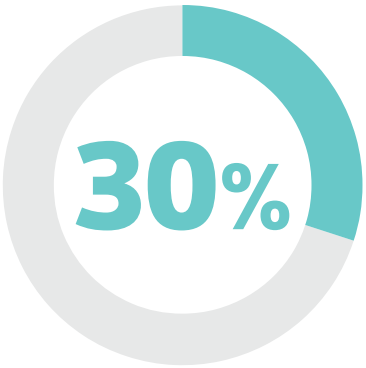
Microsoft understands these concerns and has made security a key design element of the Azure platform. Azure employs powerful encryption and access management tools, and Microsoft maintains a focus on security as the platform evolves. That being said, security in the cloud is a shared responsibility requiring commitments of time and energy from both vendors and customers. Enterprises adopting cloud computing services must implement their own security strategies to ensure that their Azure deployments adequately protect enterprise applications and data.

Why Azure Is an Essential Cloud Service

Enterprises across many different industries depend on Microsoft Azure as a critical component of their IT strategies. The flexibility, scalability and powerful technology supported by Azure allow organizations to realize the benefits of cloud computing within the framework of a comfortable and familiar technology platform. Microsoft Azure supports a broad cross-section of technologies, including numerous operating systems, programming languages, frameworks, tools, databases and devices. Microsoft built the Azure platform using many of the same Microsoft products that millions of developers and IT professionals around the world already trust for their on-premises operations.

The Azure platform provides IT professionals access to a virtually unlimited pool of computing, storage and application development resources. While on-premises environments are constrained by available hardware and require costly upgrades to boost capacity on a regular basis, Azure allows enterprises to extend or replace those environments with pooled resources shared by many different customers. This allows for reliable access to the foundational resources necessary to sustain enterprise technology environments, as well as burst capacity to meet periodic and unexpected surges in demand. Under the Azure pricing model, customers pay only for the services they need. When an enterprise requires access to computing resources on a temporary basis, it simply pays by the hour for those resources. Charges stop accumulating as soon as the customer releases the resources they've been using. In the cloud computing model, overprovisioning is a thing of the past.

Cloud services also provide customers with **rapid access to emerging technologies**. For example, Azure provides customers with on-demand access to advanced analytic services, such as machine learning and business intelligence technologies. Organizations that wish to experiment can quickly provision them and be up and running in minutes. This replaces the traditional on-premises approach that would require negotiating license agreements, designing infrastructure and ordering hardware before beginning an exploration of new technology.



The expected increase in **spending** on cloud solutions from 2013 through 2018[1]

Security Features of Azure

Microsoft recognizes that IT professionals are willing to adopt cloud computing solutions only if they are absolutely confident in the provider's ability to provide strong security measures that safeguard customer applications and data. Because of this, Microsoft invested roughly $1 billion in security during 2015 and doubled the number of security executives on its team during that same period. It focused on three key areas of Azure security: design and operational security; encryption; and identity and access management.

Design and Operational Security

As Microsoft developed the Azure service, the company adopted a revolutionary "security first" approach to the platform. Azure was designed with security in mind as a key requirement, not as an afterthought added on at the end. This approach ensures that Azure's security functionality is efficient, effective and user-friendly. Enterprises may secure the data stored in Azure with confidence that the controls were built using a defense-in-depth strategy. This approach assumes security breaches will occur and uses multiple, overlapping controls to prevent the breach of a single control from jeopardizing the security of the platform.

Microsoft also brings considerable operational security experience to the Azure platform. Azure benefits from the knowledge and oversight of Microsoft's global incident response team that works around the clock to mitigate the effects of any attack. This team can also draw on the resources of Microsoft's centers of excellence that fight digital crime, respond to security incidents and vulnerability reports, and combat malware.

Encryption

Encryption is the cornerstone technology of information security programs, and Microsoft's security-first approach to Azure integrates encryption technology for both data in transit and data at rest. Industry-standard encrypted transport protocols protect communications between user devices and

Security Testing

The best way to verify the security of cloud deployments is to test security controls regularly. In on-premises environments, security teams typically meet this objective by conducting vulnerability scanning and penetration testing. Vulnerability scans provide automated assessments of systems and services that identify known vulnerabilities, including missing patches, web application vulnerabilities and broken access controls. Penetration tests add a human touch, pointing white-hat hackers at an environment and asking them to simulate the actions that a malicious attacker would take when attempting to bypass security controls.

Organizations may choose to develop the expertise to conduct these tests internally or outsource them to an independent service provider. Independent providers bring dedicated subject matter experts and a fresh set of eyes that weren't involved in the design of the controls being evaluated.

[1]Forbes, "Roundup of Cloud Computing Forecasts and Market Estimates, 2015," January 2015

Microsoft data centers, protecting data from prying eyes. Microsoft uses this same encryption technology to protect internal communications between data centers, ensuring that customer data remains safe. Customers seeking to move large quantities of data to Azure may even opt to ship the data directly to Azure data centers on hard disks encrypted using BitLocker technology.

Enterprises may also apply encryption to data stored in the Azure platform, protecting it against a variety of attacks. Azure offers a wide range of encryption capabilities for data at rest, including the federal government's Advanced Encryption Standard (AES), which uses 256-bit encryption keys. The use of encryption for data in transit and at rest provides customers with the confidence that their sensitive information remains safe and secure in the cloud.

Identity and Access Management

Azure Active Directory provides enterprises with a comprehensive cloud-based identity and access management solution that helps secure access to cloud applications. Users may authenticate to Azure Active Directory and then obtain tokens for use with diverse applications. Enterprises may also choose to synchronize Azure Active Directory with the Windows Server Active Directory environments that they already run on-premises, providing easy integrations between cloud and on-premises authentication infrastructures.

Azure Active Directory helps IT professionals simplify user and group management functions and integrate them tightly with security controls. It combines core directory services, advanced identity governance, security and application access management in a consolidated, trusted platform. Developers can extend Azure Active Directory using the Azure Active Directory Graph REST application programming interface and can also integrate with Facebook, Google, Windows Live ID and other identity providers using Azure Active Directory Access Control.

Data Backup and Availability

Almost every organization in existence today depends on information as a critical business asset. In this environment, protecting data from corruption and loss is one of the most important tasks facing security professionals. While cloud providers go to great lengths to protect the availability of information in their care, enterprise security teams must not only understand the correct use of those controls but also may consider the use of third-party tools as a fail-safe control against data loss.

For example, Acronis offers backup services designed to integrate with cloud service providers, including Microsoft Azure and Amazon Web Services. Organizations with on-premises data centers can use Acronis as a consolidated data backup solution that works across both physical and virtual machines on-premises and in the cloud.

To learn more about Microsoft Azure and CDW's services for it, visit CDW.com/azure.

Incorporating Azure into Your Security Environment

Microsoft's security engineers have gone to great lengths to ensure that Azure is as secure as possible, but security in the cloud remains a shared responsibility. Enterprises adopting cloud solutions must understand the security controls offered by their service providers and the details that customers must handle themselves.

One of the most important steps that organizations can take is planning out their cloud adoption strategies in advance. A cloud strategy outlines the architectural and security approach that the enterprise will use to guide the selection and implementation of cloud services. It provides an important foundation upon which the organization can build a secure cloud environment.

Account Management

Organizations often select Microsoft Azure as their cloud infrastructure provider of choice because of the advanced security features that it provides. IT professionals building a new Azure-based computing environment should pay attention to security issues from the earliest stages of account setup. In particular, leveraging Azure Active Directory for user accounts provides a centralized account management infrastructure that enhances security.

Azure Active Directory offers a flexible, role-based access control (RBAC) service that allows organizations to limit access based upon each user's specific job responsibilities. This includes the use of many built-in roles, such as owner, reader and contributor, that provide predefined security access. Enterprises seeking more granular access controls may also create custom roles that tightly limit access privileges.

One of the most important account management actions that organizations will want to take is tightly controlling access to the privileged accounts that may directly manipulate the Azure infrastructure. This type of access (such as accounts with owner, user access administrator, security manager or similar privileged roles) is particularly sensitive and should be assigned on an as-needed basis. Furthermore, enterprise security administrators should take added steps to secure these privileged accounts. For example, organizations should protect access to all privileged accounts using multifactor authentication technology that requires the use of a physical token or biometric measure in addition to a password. This prevents an attacker from gaining access to a privileged account simply by stealing a password. Finally, enterprises may enforce rules that limit access to sensitive functions based on network location.

[2]Verizon, "2016 Data Breach Investigations Report," April 2016

Network Security

Network security specialists are already familiar with the use of virtual local area networks and firewalls to segment on-premises data centers. In a cloud environment, customers do not have direct access to the network equipment required to perform segmentation, but can implement similar controls using virtualized technologies. The Windows Azure Virtual Network governs communications taking place between virtual machines in Microsoft Azure.

Virtual Network allows administrators to create separate tiers of virtual machines based on the resources they need to access and the sensitivity of information that they store, process and transmit. This technology allows enterprises to build their own virtual private data centers in the cloud, restrict access between subnets in that virtual data center, and create secure, encrypted VPN links to on-premises data centers to facilitate access to resources across environments.

Integrating Other Security Tools

Enterprises moving to the cloud should also consider implementing other important security tools. These include intrusion prevention systems, system configuration and patch management solutions, service monitoring and malware protection software. Essentially, all of the security controls that exist in on-premises environments should also exist in the cloud, run either by the service provider or the customer.

As organizations select the security tools they will adopt, they should consider the use of tools that are designed specifically to work with Microsoft Azure. For example, Trend Micro's Deep Security offers a comprehensive management approach for monitoring Azure deployments. It provides live monitoring of Azure-based workloads and also offers cloud-specific security remediation recommendations designed to bolster Azure security. Using tools that understand the cloud helps enterprises design secure cloud environments.

CDW: A Cloud Security Partner That Gets IT

CDW is ready to be your organization's cloud security partner. We provide the risk management methodologies that you need to secure data, maximize continuity of operations and put disaster recovery plans in place.

CDW's long-standing partnerships with key cloud vendors, including Microsoft, Trend Micro and Acronis, allow our experts to take a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help you achieve your security objectives in an efficient, effective manner. These phases include:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed vendor evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- 24/7 telephone support and ongoing product lifecycle support

The CDW Approach

ASSESS

Evaluate business objectives, technology environments and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services; document technical architecture, deployment plans, "measures of success," budgets and timelines.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

To learn more about CDW's cloud security solutions, contact your CDW account manager, call 800.800.4239 or visit cdw.com.

Featured Partners

Acronis | Office 365 | TREND MICRO Securing Your Journey to the Cloud

CDW PEOPLE WHO GET IT