Superior security with cloud infrastructure

How Microsoft Azure can strengthen Utilities' security approach

Executive summary

Cloud technologies provide recognized opportunities for businesses, yet perceived security concerns have slowed their adoption in the Utilities sector. That is beginning to change. Early adopters are migrating both operational and control data to the cloud because cloud providers have progressed security to meet even the most stringent requirements like those for Utilities. Microsoft is leading the way among providers with a robust and trusted cloud, Microsoft Azure.

This paper explores the security features of Microsoft Azure and how they can help protect Utilities' critical information. With Azure, a Utilities company maintains complete ownership and control of data and can pick which security features to enable. Azure incorporates advanced security measures and maintains compliance with many industry regulations, including ISO/IEC 27018, to protect critical information in the Utilities industry.

Azure's security features work together to provide logical isolation, making Azure just as secure, and often more secure, than on-premises deployments. With a variety of encryption methods complementing its compute, storage and networking isolation, Azure segregates workloads and automatically prevents unauthorized access. Microsoft's advanced malware solutions protect data against the latest threats, and incident response teams are available 24x7. With Microsoft Azure, Utilities can rest assured that critical information is accessible and secure.

Table of contents

The cloud offers substantial benefits to Utilities 2

These benefits have long felt out of reach because of concerns about cloud 2

- With highly sensitive data, Utilities can't adopt technologies that pose heightened security risks 2
- Cloud concerns typically fall into three main categories 2

With Microsoft, cloud concerns should no longer hinder your cloud adoption 3

- Security: Microsoft has a host of security solutions to help protect your data 3
- Compliance: Microsoft Azure maintains compliance with a broad range of industry standards 7
- Sovereignty: Microsoft supports sovereignty requirements better than any other cloud provider 7
- Hybrid deployment: The Microsoft cloud is designed to integrate with on-premises solutions 7

Mimic your physical air gap with logical isolation in the cloud 7

- Compute isolation 8
- Storage isolation 8
- Networking isolation 9

Going forward: Microsoft continues to invest in cloud security, privacy, transparency and compliance 10

Get started with Microsoft Azure 11

- For more information 11

Microsoft

The cloud offers substantial benefits to Utilities

Cloud infrastructure brings significant opportunities to businesses, including cheaper storage, faster computing and greater scale. These advancements can be especially beneficial to Utilities looking to replace aging infrastructure, meet ever-changing industry regulations and streamline operations. For example, the cloud offers:

- **Increased flexibility.** With the emergence of more sustainable energy technologies and IoT solutions, Utilities can use the cloud to integrate a variety of technologies and workloads. They also have the opportunity to centralize asset monitoring and improve real-time communications across organizations.
- **Big data capabilities.** Smart meters and new online tools are creating a lot more data that must be stored, compiled and correlated. The cloud offers inexpensive storage options and can handle a wide variety of data types from multiple sources around the globe.
- **Advanced analytics.** Storing all of the data will not add value unless the data can be turned into insight. Utilities can use advanced analytics capabilities to monitor asset health and enable predictive maintenance, streamlining operations and lowering operating costs. Powerful cloud-based analytics tools can also assist with load balancing and demand forecasting to optimize grid efficiency.

Overall, cloud technologies offer faster and more cost effective ways of performing the tasks that Utilities already do. It can help ensure consistent, reliable operation of the electric power grid.

These benefits have long felt out of reach because of concerns about cloud

Many Utilities have been unable to take advantage of these benefits due to perceptions that cloud environments cannot provide the level of security needed. Storing data outside of a company's own on-premises servers and infrastructure creates the impression that it no longer has control over its data. It must rely on the cloud provider to make sure that data is available to employees and protected against the latest threats. Whatever benefits the cloud offered, it was not worth putting critical information—and company reputations—at risk.

With highly sensitive data, Utilities can't adopt technologies that pose heightened security risks

Many companies must maintain a certain amount of confidential information, whether customer data, billing data, or private company IP. Unlike other industries, however, Utilities must maintain the strictest security across the majority of their data. A compromise in billing data could put customer credit card numbers and bank accounts at risk. Unauthorized access into real-time smart meter readings could help determine whether or not customers are at home, leaving their property vulnerable.

Even more crucial are the infrastructure control and supervisory control and data acquisition (SCADA) systems. A compromise or attack on these systems could destroy valuable and critical infrastructure and shut down power to large geographic areas. This sort of disaster could take a long time and significant investments to repair.

Because of the sensitivity of Utilities data, concerns about using cloud technologies have been widespread. Until recently, perceived limitations of cloud security have caused Utilities to err on the side of caution and keep data on premises.

Cloud concerns typically fall into three main categories

By working with various Utilities customers, Microsoft has noticed that concerns typically fall into three main categories:

1. **Security**. With large volumes of sensitive data, unauthorized access could impact customers, companies, and governments alike. If cloud solutions fail to implement the strictest security standards, an attack could

compromise critical infrastructure and SCADA data with disastrous results. Utilities want to ensure that they can safely use cloud-based applications without increasing vulnerability to attacks.

2. **Sovereignty**. Regional and national regulations specify how and where data must be used and stored. If a cloud solution prevents a company from maintaining full control over their data, they cannot adhere to these regulations.
3. **Compliance**. Customer, industry, and government regulations also impact how Utilities store and use information. Cloud providers that fail to meet these regulation requirements put at risk the compliance of the Utilities company.

With Microsoft, cloud concerns should no longer hinder your cloud adoption

Thanks to a company-wide focus on security, Microsoft Azure is just as safe—if not safer—than your on-premises setups. Microsoft can address any of the above concerns with the Microsoft Azure trusted cloud platform – security, sovereignty, and compliance. Microsoft also integrates with your on-premises investments to get started faster and retain maximum control. Azure can help you maintain secure, reliable operation of the electric power system.

Security: Microsoft has a host of security solutions to help protect your data

Microsoft Azure is designed as a multi-tenant cloud environment that leverages virtualization technologies to provide scale and resource utilization as well as full data separation and isolation. Microsoft provides robust security options and continues to invest in the latest technologies. Azure security measures focus on 4 key areas:

Managing and controlling identity and user access

Protect against unauthorized access with **identity and access management**

Provide specific levels of access for individual users, for example, ensuring service technicians cannot access customer billing information and preventing accounting teams from interfering with infrastructure controls. And stop anyone outside of your organization from accessing company information.

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud-based directory and identity management service. It provides authentication, authorization and access control for your users, groups and objects. With Azure AD, your users receive single sign-on (SSO) access, so they can use a single set of credentials to sign into thousands of cloud SaaS applications regardless of where they are hosted.

Azure AD can be used as a standalone cloud directory for your organization or as an integrated solution with your existing on-premises Active Directory. It offers robust authentication methods, using primary and secondary secret keys for each account. It also enables such features as Multi-factor Authentication (MFA), AD Domain Services and Active Directory B2C to protect your information and provide streamlined user experiences. Azure AD Premium offers advanced reporting and identity management in the cloud.

With the tools offered by Azure AD, you can ensure that your employees can access the information they need at anytime from anywhere. Through the same methods, you can also prevent unauthorized access to your data and applications. Protect your grids and other infrastructure from compromise with enhanced visibility into, and control over, information and application access within your organization.

Control app usage across your organization with **cloud application security**

See which employees are using cloud apps and regulate the information they share within those apps. Microsoft Cloud App Security is a new service from Microsoft that provides IT visibility, control and security over cloud applications at a level similar to on-premises. With this cloud access security broker (CASB) solution, you can get the benefits of cloud applications with increased insight into user activity, detection of anomalous behavior and compromised accounts, and improved protection over critical company data. This solution works with popular cloud applications, including Box, Dropbox, ServiceNow, Salesforce and Office 365.

Ensure technicians can access information safely with **secure remote access**

When service technicians need to access smart meter data on site, provide secure ways for them to access that information. Microsoft Azure not only protects information in storage; it also provides safeguards to prevent exploits and maintain data confidentiality and integrity while in transit. Built-in cryptographic technology enables you to encrypt communications within and between deployments, between Azure regions and from Azure to on-premises datacenters. If you grant a Microsoft administrator access to your virtual machines through remote desktop sessions, remote Windows PowerShell or the Azure Management Portal, their transmissions are always encrypted.

To securely extend your on-premises datacenter to the cloud, Azure provides both site-to-site VPN and point-to-site VPN capabilities as well as dedicated links with ExpressRoute. ExpressRoute creates private connections between Azure and on-premises datacenters; connections do not traverse public internet and offer more reliability, faster speeds, lower latencies and higher security than typical internet-based links.

With Secure Remote Access, you can ensure that data is transmitted securely to and from all endpoints in your business. Connect your cloud deployments to any on-premises systems with secure VPNs, and maintain compliance with the latest industry standards. Ensure that your employees can access the information they need quickly and securely.

Encrypting communications and operations processes

Protect sensitive customer information with **data access control and encryption**

With customer billing and payment methods now available online, protect your customer's personal information at rest and in transit with advanced encryption. Azure provides multiple capabilities for protecting data in transit and at rest, including encryption for data, files, applications, services, communications and drives. You have the option to encrypt information before placing it in Azure as well as storing keys in your on-premises datacenters. Neither the storage service nor the applications ever see these keys. Keys are unique to each tenant; even Microsoft Azure support technicians can only gain access with explicit permission that is automatically revoked after the completion of the engagement. Azure Key Vault increases your security over keys and passwords, helping you create and import encryption keys in minutes.

Azure StorSimple encrypts data via a 128-bit public/private key pair prior to uploading it to Azure Storage. Azure supports and uses numerous encryption mechanisms, including SSL/TLS, IPsec and AES, depending

on the data types, containers and transports. Microsoft also offers BitLocker Drive Encryption and Always Encrypted to provide additional protection for sensitive data.

With this advanced encryption, you can add an extra layer of security to your data no matter where it is stored. While Azure uses other security measures to prevent unauthorized access, this encryption ensures that data is accessible only to those with the right encryption credentials. For example, even if the physical hardware on which data is stored were compromised, the information inside would still be inaccessible.

Securing networks

Keep your critical infrastructure isolated with **virtualization**

Add extra layers of protection by running critical infrastructure workloads in separate virtual machines from the rest of your company data. In Microsoft Azure, virtual machines do not have access to the physical host server. This virtualization of physical resources leads to a clear separation between guest OS and hypervisor, resulting in additional security separation between the two. Azure's Hypervisor passes all hardware access requests from guest VMs to the host for processing, preventing users from obtaining raw read/write/execute access to the system and mitigating the risk of sharing system resources.

This virtualization is central to Azure's security capabilities. Even with multiple accounts sharing the same physical storage location, virtualization prevents a compromise in another business from infecting the physical hardware and, in turn, your data. Your customer billing information remains separate from your asset monitoring, which all stay separate from your load analysis. If an email opens an attachment that compromises your marketing workload, you can ensure that the rest of your infrastructure—customer data, billing information and SCADA data—remains safe in their respective virtual machines.

Protect your employees by safeguarding all traffic with **virtual networks and firewalls**

Segregate your networks just as you would on premises to prevent corporate traffic from interfering with SCADA traffic. The distributed and virtual networks in Azure help ensure that your private network traffic is logically isolated from traffic on other Azure Virtual Networks. Virtual Local Area Networks (VLANs) are used to separate customer traffic from the rest of the Azure network. Access to the Azure network from outside is restricted through load balancers, and network traffic to and from VMs must pass through the Hypervisor virtual switch, which filters traffic and segregates VMs from other tenants.

This step ensures that communication into, out of, and between your networks remains secure. Your network is separate from other networks which lowers the amount of traffic your virtual machine encounters, reducing the possibility of attacks. Your VM gets its own address space that is completely invisible to VMs outside of your deployment unless you configure it to be public facing. Even communications between your own VMs can be configured to ensure a compromised computer or a rogue employee cannot access critical infrastructure.

Managing threats

Address threats quickly with **logging and monitoring**

Gain visibility into potential threats already inside your networks to prevent damage to grid infrastructure. Azure provides authenticated logging of security-relevant events that generate an audit trail, including system information and security event logs in Azure infrastructure VMs and Azure AD. Azure security administrators monitor activity such as changes in DHCP or DNS server IP addresses; attempted access to ports, protocols or IP addresses that are blocked by design; changes in security policy or firewall settings; account or group creation; unexpected processes or driver installation.

Azure stores these logs in a database from which alerts about suspicious events are sent directly to a Microsoft administrator. The administrator can access and analyze these logs (only the logs, not your actual data), which are retained for a set period of time depending on account configuration. You determine if or how administrators can access logs associated with your account. The storage accounts for logs are protected from direct administrator access to help prevent against log tampering.

Azure Security Center is another robust tool that helps you prevent, detect and respond to threats quickly and effectively. It provides increased visibility into and control over the security of all your Azure resources, so you can better understand your current security steps and implement changes from a centralized location. The Security Center makes it easy to define policies, integrate new solutions and configure security alerts.

By providing visibility into these events, Azure reduces the risk of threats in your environment. It notices when, where and how people request access and can help make sure that no one gains access illegitimately. If one of your accounts exhibits unusual behavior, administrators can address it before it causes problems to the rest of your business data.

Rest assured that your operations are protected with **threat mitigation**

Address attacks quickly before they remove infrastructure safety controls and take assets offline. As the threat landscape continues to evolve, Microsoft is investing heavily to address cybercrime. On average, attackers remain undetected in a network for +200 days, and a data breach costs a company $3.5 million. Azure Antimalware is enabled by default on all infrastructure servers and can be enabled within your own VMs. Microsoft maintains continuous monitoring across servers, networks and applications to detect threats and prevent exploits, notifying administrators automatically of anomalous behaviors.

Microsoft uses "Red-Teaming" to conduct regular penetration testing to improve cloud security controls and processes. Azure's integrated deployment systems manage the distribution and installation of security patches across the cloud platform to ensure consistent policy updates. Azure also offers the option to deploy 3rd-party security solutions within your subscriptions to add extra layers of protection.

Microsoft has invested in a new Cyber Defense Operations Center to address the latest threats. Staffed with teams 24×7, the center has direct access to thousands of security professionals, data analysts, engineers, developers, program managers and operations specialists throughout Microsoft to ensure rapid response and resolution to security threats. Informed by decades of experience working with the industry to fight threats on a global scale, the center maintains critical connections with industry security partners, governments and enterprise customers, engaging Microsoft's Digital Crimes Unit when law enforcement needs arise.

The security controls and risk management processes Microsoft has in place to secure its cloud infrastructure reduce the likelihood of incidents. But, in the event an incident occurs, the Security Incident Management (SIM) team within the Microsoft Online Security Services & Compliance (OSSC) team is ready 24x7 to respond.

Microsoft is actively addressing threats to keep your data safe. Advanced malware scanning and alerts in real time can help prevent hackers from accessing confidential IP and customer information within the cloud. Azure also helps protect against attacks that could cause outages and infrastructure downtime.

Compliance: Microsoft Azure maintains compliance with a broad range of industry standards

Microsoft Azure meets 34 international and industry-specific compliances standards. It aligns to the US Federal Risk and Authorization Management Program (FedRAMP) specifications for government agencies, and FedRAMP certifies that Azure meets the National Institute of Standards and Technology (NIST) 800-53 controls standard.

Microsoft has incorporated ISO/IEC 27018 controls for the protection of personally identifiable information (PII) in the public cloud and is verified by third parties. Microsoft was the first major cloud provider to incorporate the ISO/IEC 27018 code of practice. With the PII protection, Utilities can confidently store and manage smart meter data, customer data and billing information on the Azure platform.

Sovereignty: Microsoft supports sovereignty requirements better than any other cloud provider

Microsoft Azure is a global platform, available in 140 countries and supporting 10 languages and 24 currencies. With physical datacenters already online in 22 geographic locations, and more coming online regularly, Microsoft enables you to control where your data is stored. Storage of data can be restricted to a single geography, region or country to comply with any national or regional regulations you may face.

To limit the number of geographic storage locations while still realizing the value of data redundancy, Microsoft also offers hybrid deployment options. By duplicating your data in the cloud and on your own servers, you can adhere to regulations while meeting the Utilities' Disaster Recovery mandate of ensuring your data is always available.

Hybrid deployment: The Microsoft cloud is designed to integrate with on-premises solutions

Microsoft Azure hybrid deployments enable you to migrate some workloads to the cloud while running others in your on-premises servers. You can start with a single scenario to realize benefits right away and transition as much or as little to the cloud as you need. Migrate supply chain information or create custom web portals to share up-to-date information with your customers in intuitive ways.

Hybrid deployments also enable you to move workloads around as your business needs evolve. For example, if a storm requires rapid expansion of staff, or access to control centers is temporarily compromised, secure remote access via the hybrid deployment can be enabled. With a hybrid solution from Azure, you can run analysis across all workloads simultaneously as if all data were stored in the same location.

Mimic your physical air gap with logical isolation in the cloud

Public clouds offer a multi-tenant approach to data storage, meaning that your data may be stored on the same physical infrastructure as the data from other accounts. Even though the physical infrastructure is the same, Microsoft Azure maintains the same level of protection as physical isolation with a feature known as logical isolation. Azure core infrastructure and virtualization technologies are designed with stringent controls to meet strict data separation requirements, meaning that your data just as separated as traditional air gap approaches.

Logical isolation separates virtual networks from other virtual networks and from the physical hardware on which they run. This ensures that your customer billing data remains separate from your smart meter data, which both stay completely isolated from your SCADA data. The separation from the physical hardware also means that if any system were compromised, that attack would not infect any other part of your business. If someone accessed an employee's email account, they couldn't use that access to take infrastructure offline.

Azure enforces the security principle known as the principle of least privilege, which requires that each user or application be granted the lowest clearance needed for the performance of authorized tasks. The Microsoft cloud is designed to ensure that customers and authorized administrators can use Azure efficiently and keep all information

isolated from other tenants. It accomplishes this in three main ways: compute isolation, storage isolation and networking isolation.

Compute isolation

Azure's compute platform is based on machine virtualization—meaning that all customer code executes in a Windows Server Hyper-V virtual machine. On each Azure node (or network endpoint), there is a Hypervisor that runs directly over the hardware and divides a node into a variable number of Guest Virtual Machines (VMs). Each node also has one special Root VM, which runs the Host OS. Isolation of the Root VM from the Guest VMs and the Guest VMs from one another is a key concept in Azure security architecture.

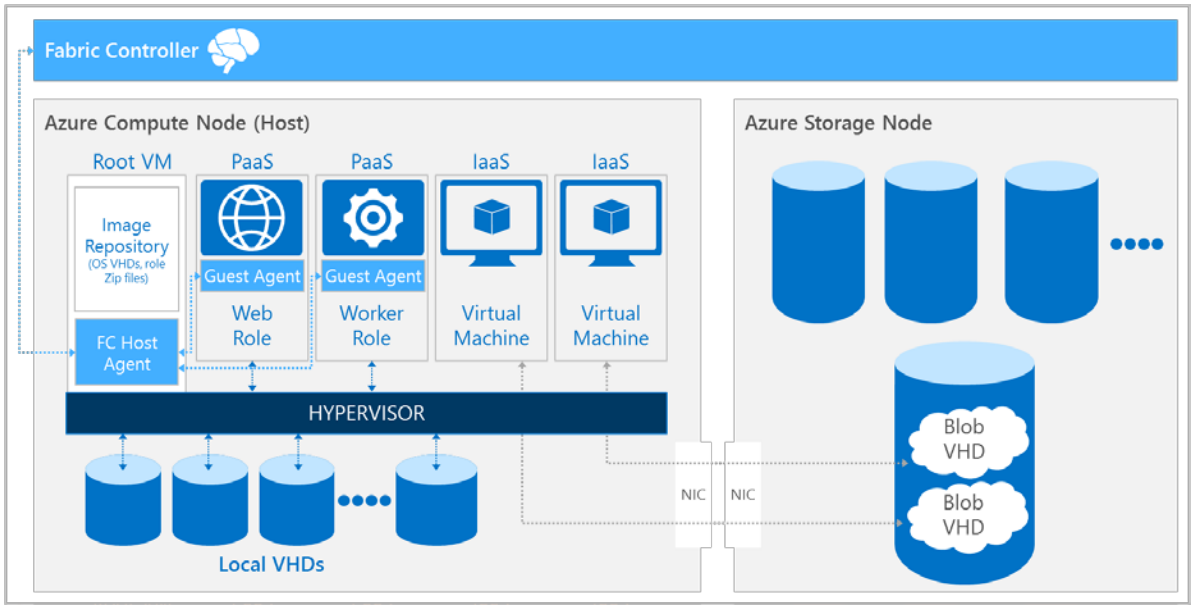

Figure 1: Azure architecture showing the isolation of the Root VM from Guest VMs and Guest VMs from one another. Compute nodes are also isolated from storage nodes for increased protection

The Fabric Controller is the brain of the Azure compute platform. The Host Agent is its proxy, integrating servers into the platform so that the Fabric Controller can deploy, monitor and manage the virtual machines that define Azure Cloud Services. Because the Fabric Controller is the central orchestrator for much of the Azure Fabric, significant controls are in place to mitigate threats, especially from potentially compromised Fabric Agents within customer applications.

By managing the isolation of the virtual machines, the Hypervisor and the Host OS provide network packet filters to help assure that untrusted virtual machines cannot generate spoofed traffic, receive traffic not addressed to them, direct traffic to protected infrastructure endpoints or send or receive inappropriate broadcast traffic (Kaufman and Venkatapathy, 2010).

Storage isolation

As part of its fundamental design, Microsoft Azure separates customer VM-based computation from storage. This separation enables computation and storage to scale independently, making it easier to provide multi-tenancy and isolation. Consequently, Azure Storage runs on separate hardware with no network connectivity to Azure Compute except logically. All requests run over HTTP or HTTPS based on customer's choice.

Azure storage is allocated sparsely. This means that when a virtual disk is created, disk space is not allocated for its entire capacity. Instead, a table is created that maps addresses on the virtual disk to areas on the physical disk; that

table is initially empty. The first time a customer writes data on the virtual disk, space on the physical disk is allocated, and a pointer to it is placed in the table (Myers, 2014).

Sparse allocation helps prevent others from accessing your information. Because your data could be spread across any server, another account could not locate the data without the mapping table. Accounts can only read data that they have written, so even if your data was somehow located, it would be impossible for anyone else to access it.

When a customer deletes a blob or table entity, it will immediately get deleted from the index used to locate and access the data on the primary location. The deletion is then repeated asynchronously for the geo-replicated copy of the data. At the primary location, a customer can immediately try to access the blob or entity but will not find it in the index since Azure provides strong consistency for the delete. The customer can verify directly that the data has been deleted.

There is no possibility of one customer reading the deleted data of another customer or of an Azure administrator reading a customer's deleted data. If anyone tries to read a region on a virtual disk to which they have not yet written, physical space will not have been allocated for that region and therefore only zeroes would be returned. This ensures that your data remains secure, even after deletion.

Networking isolation

Virtual networks in Azure help ensure that each customer's private network traffic is logically isolated from traffic belonging to other customers. A customer subscription can contain multiple logically isolated private networks and can include firewall, load-balancing and network address translation.

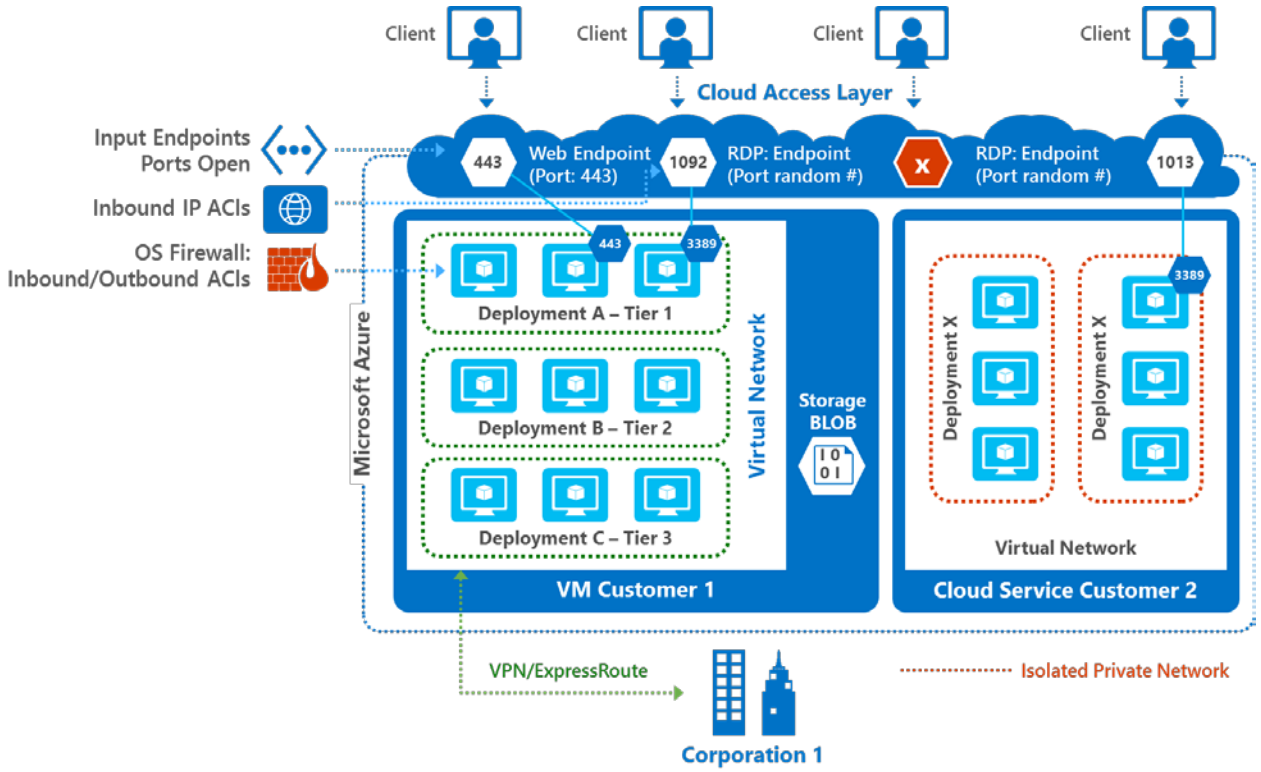

Figure 3: An example of virtual network topology

Network access to virtual machines is limited by packet filtering at the network edge, at load balancers and at the host OS level. Additionally, customers can configure their host firewalls to further limit connectivity, specifying for each listing port which connections are accepted. For each VM, the Fabric Controller composes and updates a list of

IP addresses of VMs in the same cloud service. This list of IP addresses is used by the Fabric Agent to program the packet filters to only allow intra-service or virtual network communication to those IP addresses.

Your VMs cannot send traffic to Azure's private interfaces, to other customers' VMs or to Azure infrastructure services themselves. Your VMs can only communicate with other VMs that you own or control and with Azure infrastructure service endpoints meant for public communications. When you put VMs on a virtual private network, those VMs get their own address spaces that are completely invisible, and hence, not reachable from VMs outside of your deployment or virtual network (unless configured to be visible via public IP addresses). Your environments are open only through the ports that you specify for public access; if the VM is defined to have a public IP address, then all ports are open for public access.

The cumulative effect of these restrictions is that each cloud service acts as though it were on an isolated network where VMs within the cloud service can communicate with one another, identifying one another by their source IP addresses with confidence that no other parties can impersonate their peer VMs. They can also be configured to accept incoming connections from the internet over specific ports and protocols.

Additionally, Virtual Networks provide a means for Azure VMs to act as part of a customer's on-premises network. With VNETs, you can choose the address ranges of non-globally-routable IP addresses to be assigned to your VMs so that they will not collide with addresses you use elsewhere. A cryptographically protected tunnel is established between Azure and your internal network, enabling the VM to connect to back-end resources as though it were directly on your network.

Going forward: Microsoft continues to invest in cloud security, privacy, transparency and compliance

Microsoft's portfolio of robust cloud security measures is enhanced on a regular basis. Last year, Microsoft invested over $1 billion in security, and it continues to build new security measures into its core technologies. For example, Azure Active Directory Identity Protection is a new security service that provides a consolidated view into risk events and potential vulnerabilities affecting your organization's identities. With Active Directory Advanced Threat Analytics and Azure Active Directory Identity Protection, customers can protect their environments both on premises and the cloud. For Utilities customers requiring hybrid deployments, Azure offers protection across the entire business.

> Microsoft makes security and privacy a priority at every step, from code development through incident response.

In addition to security, Microsoft also continues to invest in its trusted cloud, offering the privacy, transparency and compliance you need for your business. Microsoft ensures that you—and only you—own and control your data. You always know how your data is stored and accessed as well as how it is secured. The Azure cloud meets the requirements of many industry regulations, including ISO/IEC 27018, and Microsoft continues to achieve new datacenter certifications.

Get started with Microsoft Azure

Because of the advanced security measures and continued investments in the security space, the Azure cloud can protect your information just as well as, or better than, on-premises infrastructure. Take advantage of Microsoft's ongoing investments and expert security teams. Plus, you can leverage the power, flexibility and lower costs that only cloud services can provide.

For more information

For more information on the security features and benefits of Azure, check out these resources:

Microsoft EPG Power & Utilities: Check out the solutions Microsoft offers in the Utilities industry

Getting Started With Microsoft Azure Security: Read more about how Azure provides the security you need

Active Directory Blog: Find out more about the security advantages of Microsoft Active Directory

Azure Trust Center: Learn more about how Microsoft Azure keeps your information safe and secure

Azure Active Directory Identity Protection: Check out one of Microsoft's latest security services

Digital Crimes Unit Videos: Watch how Microsoft combats Cybercrime with the latest technology

Microsoft Security Response Center: Learn how Microsoft can identify, monitor, respond to and resolve security incidents