Data Protection for Cisco Integrated System for Microsoft Azure Stack

Certain data cannot move to a public cloud

Information is the ultimate competitive advantage. In 2018, many countries had laws enacted that specified the locality of consumer data. As a result, companies can be held liable if this data enters the public domain. Therefore, despite the best efforts of Microsoft Azure to put security measures in place, the need for low-cost onsite data protection for consumer data housed on an Azure Stack system is a topic of concern for customers seeking to implement Cisco's Azure Stack solution.

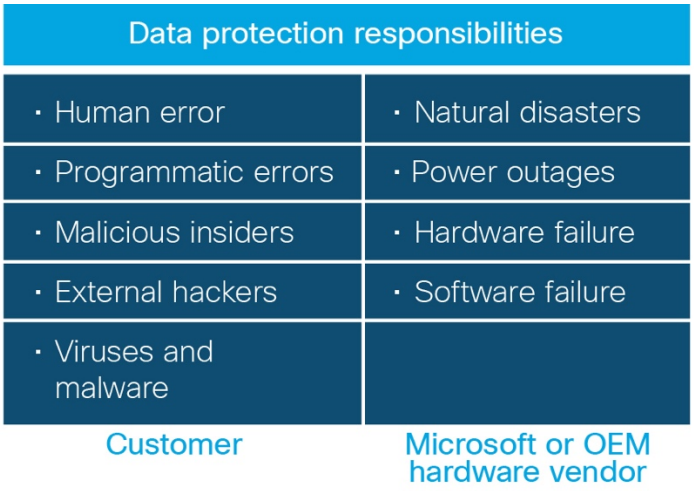
Data protection responsibilities

Enterprise IT is being transformed as cloud providers mature. Cloud providers are now offering computing, storage, and application services with exceptional elasticity, scale, resiliency, and availability on a consumption-based economic model. However, the choice between public cloud and on-premises infrastructure is not a binary one. As some workloads shift to the cloud, enterprises are also seeking to transform their internal data centers and services into offerings that provide cloud-like scale, flexibility, resiliency, and operational methods, with similar positive economic outcomes. To this end, architects are augmenting or replacing traditional, proprietary, and single-purpose IT infrastructure and applications with software-defined services, distributed processing, big data applications, and hyperconverged architectures.

The Cisco® Integrated System for Microsoft® Azure Stack enables your organization to access the development tools, data repositories, and related Azure services needed to reinvent your applications and gain new information from your secured data. Azure Stack provides the same APIs and user interface as the Azure public cloud. An integrated system enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations related to data location and accessibility. Cisco's infrastructure provides the main automation benefits of the Cisco Unified Computing System™ (Cisco UCS®) with leading Cisco Nexus® Family networking and data security technology, while helping ensure the highest-performing design to meet your future hybrid cloud growth requirements. Azure Stack opens the door to new hybrid cloud possibilities. When you use the Cisco Integrated System for Microsoft Azure Stack, you gain high-performance networking and industry-leading versatility for virtualized environments with Cisco Unified Fabric. You also automate infrastructure management with Cisco UCS Manager and help ensure consistency with policy-based management.

Data protection is essential for business continuity, protecting against human error, data corruption, ransomware, etc. Figure 1 shows the data protection responsibilities for an Azure Stack environment.

Figure 1. Azure Stack data protection responsibilities



Your IT department can set policies and purchase security tools, applications, and services to try to stop or limit the impact of malicious insiders, external hackers, and viruses and malware. Backup generators can keep the lights on should a power outage occur. In fact, all of these investments should be made and maintained regardless of the IT infrastructure on which your data resides or your organization's cloud strategy.

Earthquakes, tornados, hurricanes, and other natural disasters are typically addressed by planning and testing the capability of remote locations to keep your operations going. Although relatively few organizations experience these disasters, some industries require a plan to be in place and systems tested. Human and programmatic errors are far more difficult to prevent.

Data protection—no matter where your data resides—is a real concern, including in Microsoft Azure Stack. While Microsoft supports the Azure Stack software and Cisco supports the hardware components, it is up to you to protect your data in Azure Stack.

Cisco Integrated System for Azure Stack solution overview

The Cisco Integrated System for Microsoft Azure Stack solution enables your organization to access the development tools, data repositories, and related Azure services needed to reinvent your applications and gain new information from your secured data. Azure Stack provides the same APIs and user interface as the Azure public cloud. The integrated system enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations related to data location and accessibility. Cisco's infrastructure provides the main automation benefits of Cisco UCS with leading Cisco Nexus Family networking and data security technology, while helping ensure the highest-performing design to meet your future hybrid cloud growth requirements.

The solution offers the following benefits

- **Design by Cisco:** All major system components are designed, developed, and manufactured by Cisco, which simplifies system management, provides for single-source support, and helps avoid unforeseen product roadmap issues.
- **Leading system performance:** The latest Intel® Xeon® Scalable processors, up to 1536 GB of memory on the server, Non-Volatile Memory Express (NVMe) standard storage cache, and an optional solid state disk (SSD) are part of the package.
- **Firm data center standards:** Maintain your IT organization's data center standards for Cisco Nexus switching and system racks by installing all system components in your racks and using your networking team's existing expertise.
- **Freedom to choose:** Purchase Azure services from any vendor.
- **Proven tools:** Cisco UCS Central Software and Cisco Nexus hardware enable easy management of multiple locations or regions from a single screen on your desktop.

Industry trends and challenges and targeted Azure Stack use cases

The solution addresses some of today's main industry trends and challenges (Figure 2):

Regulatory limits on data location

In an effort to safeguard consumer data, many governments have enacted strong statutes that define exactly what type of data can move to the cloud and what type of data must remain confined to your data center.

In May 2018, 28 European countries begin enforcing the Global Data Protection Regulation (GDPR), which governs the locality of consumer data and establishes specific data-management job functions that must be addressed by each company doing business in those countries. Companies in violation can be fined up to 4 percent of their global annual turnover. This regulation also governs any non-European company that transacts any business with the 28 nations. Thus, the impact of GDPR is felt globally.

Many individual countries and local government bodies are also enacting similar legislation that will affect a company's ability to move data to and from any public cloud. IT departments must be mindful of these new data limits to avoid public ill will should consumer data enter the public domain.

Data sovereignty

Vertical industry sectors such as financial, medical, and government organizations face ethical issues and potential public outcry should their customers' data enter the public realm. Exposed credit card data can cause an immediate negative impact on a company's finances, and the news is filled with examples. Imagine a healthcare company's embarrassment should patients' medical histories become publicly available. Even worse, the safety of a nation could be jeopardized if a secure government database were compromised. The question is, though: How can you manipulate data that cannot leave your data center?

Customization: Enable existing traditional applications for the cloud

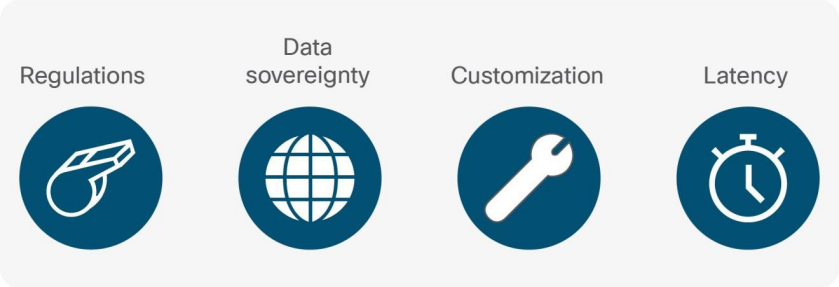
Many organizations still run applications that were developed years ago, before smartphones, tablets, and various remote data collection capabilities became available. In addition, as businesses expand into new markets, the challenge of localizing these applications for language, exchange rate, and traffic patterns is a constant worry.

Such applications reside within your data center and cannot be hosted on a public cloud. This lack of cloud capability also prevents these applications from being co-licensed by third parties, eliminating a potential new revenue stream. If you could redesign these applications to incorporate new data input devices rapidly and use development tools and data stores, what positive impact might this have on your income?

Connectivity issues: Latency

Some data center solutions and applications run in environments that are completely or intermittently disconnected from the Internet. Mining, offshore drilling, and shipping operations are examples of environments in which a constant connection to the Internet is not possible. Many government and other highly secure data centers do not permit any connection to the outside world, and often any equipment going into the data center, even a laptop, cannot be removed for any reason. Temporary "data centers" supporting the Olympic Games, auto races, music concerts, and other large events often must process data while operating offline. How can Azure services be accessible when the Internet itself is inaccessible?

Figure 2. Examples of IT trends affecting hybrid cloud use



> "Microsoft and Cisco are proven innovators and trusted technology partners, giving customers the confidence that their IT environments can be supported and secure."
>
> **Mike Neil**
> **Corporate Vice President, Enterprise Cloud Group**
> **Microsoft**

Table 1 summarizes some common use cases for the Cisco and Microsoft solution.

Table 1. Use cases: Industry examples

Industry	Use cases
Financial	• Credit card details becoming public knowledge • Brokerage information exposed, affecting consumer confidence
Medical	• Patient history exposure, leading to public embarrassment and potential lawsuits
U.S. government	• Secured data centers disconnected from Internet • Tax records released to public domain • National security compromised • International embarrassment from leaked data
Shipping	• Disconnection from Internet
Offshore drilling	• Disconnection from Internet
Indian reservations, GDPR, and country regulations	• Helping ensure that you can clearly define the location and movement of all customer-specific data
Mining	• Disconnection from Internet
All	• Cloud-enabling traditional applications to incorporate new data input capabilities, and localizing applications by geographic region • Loss of potential revenue stream from relicensing of applications located on Azure Marketplace • Adhering to GDPR regulations in 28 European counties

Cisco Integrated System for Microsoft Azure Stack

The Cisco solution starts with rack-optimized Cisco UCS C240 M5 Rack Servers. These models house two Intel Xeon Scalable processors, up to 1.5 terabytes (TB) of memory, and up to 96 TB of storage. You can select from 14 different processors, provided that each server is configured with exactly the same processors, memory, and storage. The servers drive the Azure Stack software and house all of the virtual machines and data.

Each server is connected to two third-generation fabric interconnects, which house the Cisco UCS Manager software. The use of two fabric interconnects means that there is no single point of failure in the architecture. These fabric interconnects are connected to two Cisco Nexus 9000 Series Switches to enable connectivity to the data center's border switches. Each switch and fabric

interconnect maintains a copy of the other's configuration to help enable easy replacement should replacement be required. Each server is configured with NVMe cache storage and 40 Gigabit Ethernet, which is managed by a Cisco Nexus 2000 Series Fabric Extender. The unified fabric that connects the system enables 40 Gigabit Ethernet traffic, which is a clear benefit as the system configuration grows over time.

Azure Stack installation services managed by Cisco Advanced Services are included (a typical installation takes only 3 days) within the solution configuration. We place the system components in your system rack, as we support your choice of system racks. You can configure any node increment from four up to the limit supported by Azure Stack.

Unique to Cisco is the capability to add server nodes to installed systems without the need for any professional services. You can purchase nodes when you want at the most affordable prices and have them in your data center either boxed and stored or in the system rack ready to be installed as your needs dictate. When you need another server, simply place the server in the rack, cable it, and power it on. Cisco UCS Manger will autodiscover the system node, assign the Azure Stack service profile to the server, and integrate it into the Cisco UCS cluster. This process typically requires only approximately 45 minutes. Then simply access the Azure Stack Admin Portal, select Scale Unit and Add-Node, and enter the server's address. Azure Stack will then copy the infrastructure files to the new server and integrate the server into the cluster. The cluster will then begin to rebalance the workloads. Within approximately 90 minutes, the new node is ready to process data: only 2.5 hours from the time you open the box containing your new server.

Cisco Solutions Support is also bundled with all installed solutions. Solutions Support is the highest level of Cisco support and provides onsite repair up to 24 hours a day, 7 days a week, within 4 hours. In addition, your support calls are automatically routed to a team specially trained on Azure Stack. This team can also move a support call to the Microsoft Case Exchange system to enable Microsoft support engagement as needed. With this process, human error in reentering call details is avoided. The call flow would work in reverse should you elect to contact Microsoft support initially.

> "Through our joint engineering with Microsoft, we're delivering to our customers a turnkey solution that is easy to deploy, manage, and scale that addresses the needs of both application developers and IT managers alike."
>
> **Liz Centoni**
> **Senior Vice President and General Manager**
> **Cisco**

Data protection with Commvault

When you use Cisco's infrastructure, you gain high performance networking and industry-leading versatility for virtualized environments with Cisco Unified Fabric. You also automate infrastructure management with Cisco UCS Manager and help ensure consistency with policy-based management. With the latest updates to the Commvault Data Platform, Commvault continues expanding its unique data protection capabilities to Azure Stack, including Cisco infrastructure.

What does this mean for you?

It means that no matter where your data resides, Commvault has you covered. One data protection platform protects your data regardless of whether it is on Cisco Integrated System for Azure Stack, in Azure, another public or private cloud—or wherever you need it. This approach lowers costs, providing one set of tools for your team to know and use. In addition, automated policies reduce human error and administrative costs.

Commvault uniquely provides agentless backup and recovery of your Azure Stack virtual machine and blob storage, including detailed recovery of files and folders from a simplified data management platform.

The main benefits include the following:

- **Deep integration with Azure Stack:** To provide agentless protection of the Azure Stack environment, Commvault uses the Azure Stack APIs to directly protect and recover data in Azure Stack.
- **Simplified data protection of Azure Stack:** Commvault simplifies backup and recovery for Azure Stack because you are not burdened by the need to deploy and manage agents for data protection. Simply create a service-level agreement (SLA)–based policy, and you are ready to back up data and virtual machines in your environment. Recovering virtual machines, files, and folders is just as easy.
- **Improved recovery times:** Meet more aggressive SLA demands with fast Azure Stack data recovery in a production-ready state.
- **Scalable and flexible data protection platform for your Azure Stack environment:** The Commvault Data Platform can scale as your Azure Stack environment grows.
- **Seamless, low-risk migration to Azure Stack:** Move workloads across platforms in just a few clicks: Reduce migration risk and simplify native moves to and from Azure Stack.

Commvault's capabilities appeal to service providers and enterprise customers because Commvault provides a simplified data protection strategy to meet demanding data protection requirements.

ScaleProtect™ with Cisco UCS provides a full suite of data services for protecting, indexing, securing, automating, reporting, and natively accessing data. In addition, ScaleProtect provides insight into the data, thereby creating the value that business demands.

The deployment scenarios detailed in this document enable the protection and recovery of tenant resource data on the Cisco Integrated System for Microsoft Azure Stack with ScaleProtect with Cisco UCS through the Commvault Data Platform. Commvault's components are hosted on Cisco UCS C-Series Rack Servers and S-Series Storage Servers based on predefined reference architectures. The Commvault Data Platform can be extended across heterogeneous data center environments comprising converged, traditional, and cloud infrastructures.

The main data protection and recovery use cases are listed here:

- **Protection in Microsoft Azure Stack:** Commvault provides operational recovery for active workloads and data within Microsoft Azure Stack, including the Cisco Integrated System for Microsoft Azure Stack. Commvault can provide agentless instance protection; use Commvault DASH Copy to copy data to another Azure Stack region or back to an on-premises location; and protect blob storage in Microsoft Azure Stack.
- **Migration to Microsoft Azure Stack:** Commvault orchestrates the migration of application workloads across Azure Stack instances, either at the virtual machine container level or the application level. It provides protection during the migration lifecycle while workloads are in a transition phase between an on-premises location and Azure Stack, or between the source Azure Stack scale unit and the destination Azure Stack scale unit.
- **Disaster recovery to Microsoft Azure Stack:** The Commvault Data Platform can automate the creation and replication of virtual machine replicas from a source Azure Stack scale unit to a destination Azure Stack scale unit for warm recovery.
- **Use of intelligent data agents (iDAs):** For application and data consistency, application and database plug-ins (iDAs) can be deployed within virtual machines to provide integrated application and database recovery as required.

Commvault provides the following benefits for protecting Azure Stack virtual machines:

- Native Azure Stack API integration to protect Azure Stack virtual machines
- Full virtual machine restoration for Azure Stack virtual machines
- Detailed recovery of specific files and folders in a virtual machine
- Migration from on-premises hypervisors to Azure Stack
- Disaster recovery (warm) with Live Sync to Azure Stack virtual machines

Commvault software does not require access to the Azure Stack hypervisor level. Instead, it uses representational state transfer (REST) APIs to create snapshots of each block volume. It then attaches the snapshots to a nominated proxy (VSA for Azure Stack) to read and deduplicate the blocks before writing them to ScaleProtect with Cisco UCS or cloud storage.

Data protection with Veeam

Veeam for Microsoft Azure Stack delivers hyperavailability for any application and any data in on premises and hybrid environments using Azure Stack, offering flexible backup and recovery options that enable organizations to achieve speed and agility and helping ensure protection of their data no matter where it resides.

Veeam and Cisco have collaborated to offer an integrated and preconfigured data availability solution based on Cisco UCS and Veeam technology. The Veeam Availability Solution for Cisco Azure Stack comes ready for deployment and is verified jointly by Veeam and Cisco.

The Veeam Availability Solution for Cisco UCS offers these main features:

- **Mobility of infrastructure-as-a-service (IaaS) workloads:** Veeam makes it easy to protect your public cloud workloads, enabling quick and easy restoration either on your premises or in Microsoft Azure Stack.
- **Restoration of Microsoft Azure Stack:** Restore virtual machines to Azure Stack to reduce business disruption without the need for complex configurations or hardware investments.
- **Speed, agility, and compliance:** Increase agility with data restoration, accelerate time to market by enabling development and testing environments, and help ensure compliance regardless of where data resides.

Veeam for Microsoft Azure Stack is a best-in-class solution that is an excellent fit for customers that require an advanced, enterprise-class data availability solution for their virtual environments that is simple to order, deploy, and manage and that can easily be expanded over time as the need increases. The Veeam solution uses Cisco UCS C240 and S3260 servers to deliver high-speed recovery, data-loss avoidance, and verified protection with complete visibility for applications requiring high availability and scalability. It provides fast, flexible, and reliable recovery of applications and data, bringing backup and replication together in a single solution with award-winning support.

Call to action

Can you afford to not have your vital data protected?

The Cisco Integrated System for Microsoft Azure Stack with Commvault or Veeam can enable you to back up your vital data onsite with a low-cost solution running on Cisco hardware. These data protection solutions have been fully tested on the Cisco Integrated System for Microsoft Azure Stack, and each is fully documented, in detail, for the use cases tested. With these solutions together with Cisco's automation capabilities in Cisco UCS Manager and a system design that does not expose a single point of failure, you can have the highest level of confidence that your data is fully protected. Please contact your local Cisco sales representative or valued solutions partner if you have any questions or would like a detailed proposal tailored to your data protection requirements.

For more information

For additional information, see the following:

- Cisco Integrated System for Microsoft Azure Stack (solution overview)
- Cisco Integrated System for Microsoft Azure Stack (data sheet)
- Commvault ScaleProtect with Cisco UCS (solution brief)
- Veeam Support for Microsoft Azure Stack

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-741612-00 11/18