

**Topic:** Guard customers’ organizations against external threats

**Solution:** Security is a critical pillar for cloud

Your nonprofit customers can have always up-to-date security that keeps their organizations running. They don’t need to worry about compromising business-critical application data and files across on-premise servers and the cloud.

With Microsoft Azure, your customers will be able to:

* **Guard their organization against external threats and breaches**, using built-in security features across on-premise and cloud deployments.
* **Keep their organization up and running no matter what**, with full backup and recovery to the cloud. No extra steps or redundant processes are required.
* **Make it easy for employees and volunteers to access their apps and devices with a single sign-on**,extending local user identities and permissions to the cloud.
* **Benefit from Microsoft security**, which has the largest portfolio ofsecurity and compliance certifications—more than any other cloud provider.

Provide these benefits to you customers with the top four security features in Azure.

1. **Identity and access management (IAM)**: Defend against malicious login attempts and safeguard credentials with risk-based access controls, identity protection tools, and strong authentication options — without disrupting productivity.
2. **Multi-factor Authentication:** Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication.
3. **Azure Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. If an outage occurs at your primary site, you fail over to secondary location, and access apps from there.
4. **Backup service**: The [Azure Backup](https://docs.microsoft.com/azure/backup/) service keeps your data safe and recoverable by backing it up to Azure.

Customers don’t see the importance to migrating? Show them the cost of doing nothing.

* **Increased risk:** End of support means the end of ongoing security updates. It may put your customers’ organization at increased risk if they are running applications and data on unsupported software.
* **Financial loss:** A breach could mean significant financial loss and damage organizations’ reputations.
* **Non-compliant with regulations:** Updating means you can help nonprofit customers meet data protection mandates for regulations and laws like HIPAA, HITECH, FERPA, and COPPA.

All these factors contribute to a better security landscape for your customers. Talk to your customers and explain how migrating the Azure cloud increase their security footprint and protects their business.