protiviti®
Global Business Consulting

Cloud Shepherd for Microsoft Azure

Building security in Azure through codified preventative and reactive controls

Many organizations have reached the initial maturity stage of building cloud security platforms. Some organizations have deployed and operationalized detective controls, for example, a Cloud Security Posture Management (CSPM) solution, while others are in the process of adopting detective controls. Oftentimes, these controls are not being deployed effectively, which leaves security with visibility only and no automated remediation being utilized.

Protiviti's Cloud Shepherd for Azure Security Posture Management is designed to strengthen the security posture of your Microsoft Azure Accounts through the implementation of automated preventative and reactive controls and receive polices immediately.

Without Cloud Shepherd for Azure

- Detective controls
- Backlog build-up
- Increased security risks
- Difficulty maintaining DIY Preventative and Reactive controls

VS

With Cloud Shepherd for Azure

- Effective Detective, Preventative, and Reactive controls
- Automatic policy enforcement
- Consistency and standardization
- Immediate results

Steps to implement Cloud Shepherd for Azure

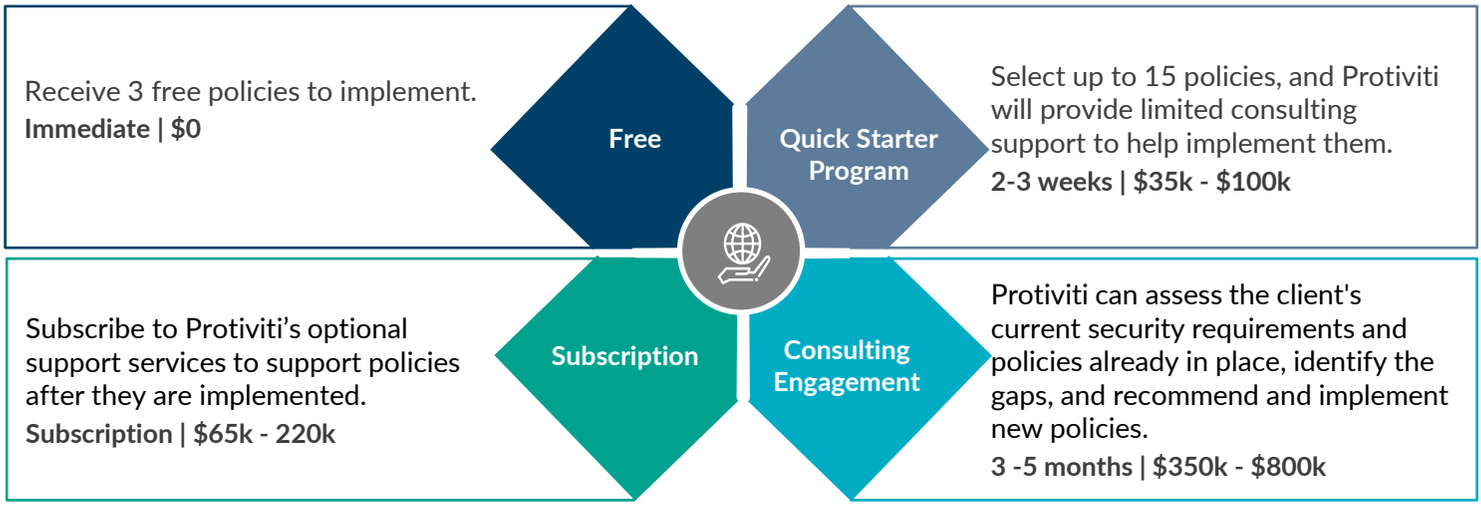
1. Review current security requirements and controls in place
2. Update security requirements and select and test preventative and reactive controls
3. Implement preventative and reactive controls

Real World Example

	Security Requirement	Detective Control	Preventative Control	Reactive Control
Before	My home must be secured from intruders.	Cameras monitor who is around my home.	Manual locks are on doors, and I must remember to lock them.	I call 911 once I get home if I noticed an intruder broke in.
After		Cameras monitor who is around my home.	Smart locks are on doors, and they automatically lock.	Alarm system calls 911 if it is not turned off.

INNOVATE. TRANSFORM. SUCCEED.

Cloud Shepherd for Azure Pricing Tiers & Use Cases



Example Use Cases

Public Network Access

Security Requirement	Preventative Control	Description
Public network access should be disabled for SQL Server.	Configure Azure SQL Server to disable public network access.	Enforces Azure SQL servers are created with public network access disabled to ensure that they can only be accessed via a private endpoint, which will help improve overall security posture.

Storage Encryption

Security Requirement	Preventative Control	Description
Enable 'Infrastructure Encryption' must be enabled for each storage account.	Storage accounts should have infrastructure encryption	Enforces that storage accounts are created with infrastructure encryption providing double encryption, which will help reduce risk of potential security attack.

Soft Delete

Security Requirement	Reactive Control	Description
Storage accounts shall have soft delete enabled.	Ensure soft delete is enabled for Azure Storage	Enforces that soft delete is implemented when storage accounts are created, which protects storage accounts from accidental deletes or overwrites by maintaining the deleted data in the system for a specified period.

Protiviti.com/Microsoft

MicrosoftSolutions@Protiviti.com

TCblog.Protiviti.com

Microsoft Solutions Partner

Microsoft Cloud

protiviti®

Global Business Consulting