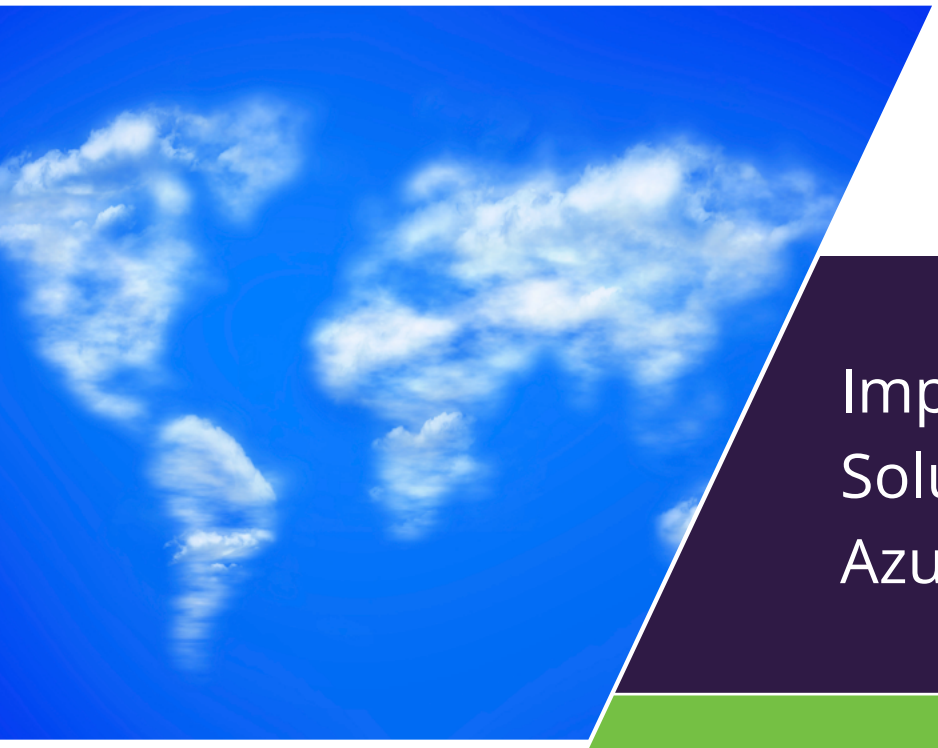
IMPERVA



Imperva SecureSphere Solutions for Microsoft Azure

DATASHEET

Benefits

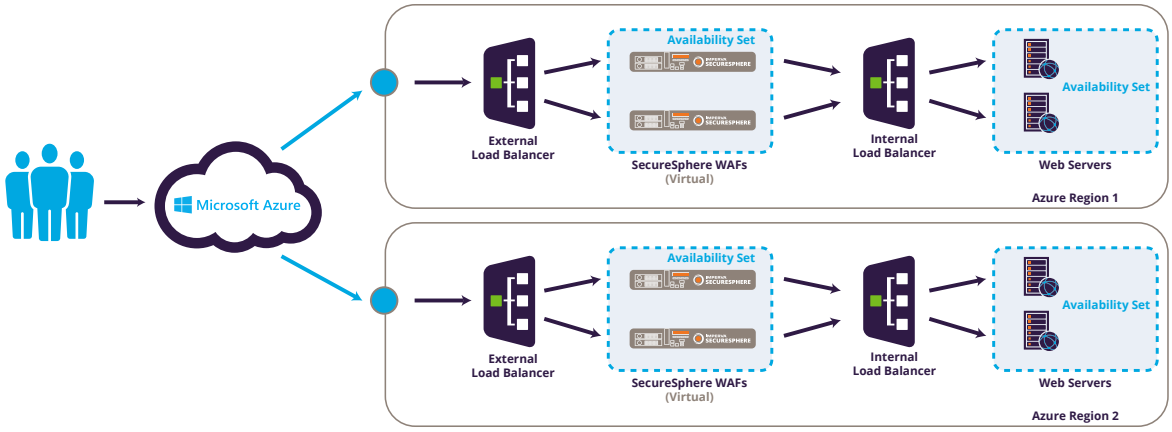
- Protects applications on Azure with enterprise-class web application firewall
- Streamlines deployments and extends scalability by leveraging native features in Azure
- Virtually patches website vulnerabilities to eliminate time-consuming emergency code fixes

Protect Web Applications and Data on Microsoft Cloud

Microsoft Azure enables organizations to deploy mission-critical applications to the cloud that scale with your business, and avoid the time and expense of building an on-premise data center. If your organization plans to move applications to the cloud, you need to move your application security and compliance solutions to the cloud too. Otherwise, you are exposed to web attacks and data theft and failed PCI audits. Moreover, the cost savings you hoped to realize from cloud computing will evaporate – replaced by expensive data breach investigation, downtime, and lawsuits.

Imperva SecureSphere Web Application Firewall (WAF) extends all of the security and management capabilities of the world's most trusted web application firewall to the Microsoft Azure. SecureSphere WAF virtual machine images are available on Azure Marketplace for customers with a "bring your own licensing model" (BYOL). This enables customers to quickly spin-up or spin-down SecureSphere WAF instances as your application traffic grows or shrinks.

SecureSphere data audit and protection solutions monitor and protect your sensitive data in the Azure cloud with the same market-leading audit and security capabilities as the on-premise solution. The hybrid Azure cloud and on-premise deployment model ensure a comprehensive coverage and uniform policy enforcement across your evolving database, file and Big Data environment.



Imperva SecureSphere WAF for Azure can protect applications hosted in multiple availability sets to maximize uptime, and provide better user experience to customers in every corner of the globe.

SecureSphere WAF analyzes all user access to your critical web applications hosted on Microsoft Azure and protects your applications and data from cyber attacks. It dynamically learns your applications' "normal" behavior and correlates this with Imperva ThreatRadar – a globally crowd-sourced threat intelligence service, to deliver superior protection for your web applications.

The industry-leading SecureSphere WAF prevents advanced web application attacks that slip through traditional perimeter defenses and provide the following key customer benefits and differentiators.

- Dynamic Application Profiling: patented technology that adapts the WAF security controls with any changes to the web applications and simplifies on-going maintenance.
- Deep Threat Intelligence: Imperva ThreatRadar real-time threat intelligence is crowd-sourced from Imperva customers worldwide and curated by the research team in Imperva Application Defense Center.
- Granular Correlation Policies: distinguishes attacks with incredible accuracy and the lowest false positive rate in the industry, by correlating multiple attributes delivered through WAF core functionality and ThreatRadar threat intelligence.
- Virtual Patching: proactively protects vulnerable web applications from being attacked, by virtually patching the attack paths in the WAF using scan data from industry leading vulnerability scanners.
- Customizable Reports: enables customers to quickly assess application security posture and demonstrate compliance for PCI, HIPAA, SOX, and other regulatory standards.

IMPERVA SECURESPHERE

SecureSphere for Azure Models

PERFORMANCE	MV1000	MV2500	MVM150
Supported SecureSphere Products	Web Application Firewall	Web Application Firewall	MX Management Server
HTTP Throughput	Up to 100 Mbps	Up to 500 Mbps	N/A
MINIMUM REQUIREMENTS FOR EACH SECURESPHERE FOR AZURE INSTANCE			
Minimum Azure Instance	A2 for HTTP only A3 for HTTPS	A3/D3 for HTTP only D3v2/D4 for HTTPS	A3 Standard