DATASHEET

Imperva Solutions for Microsoft Azure

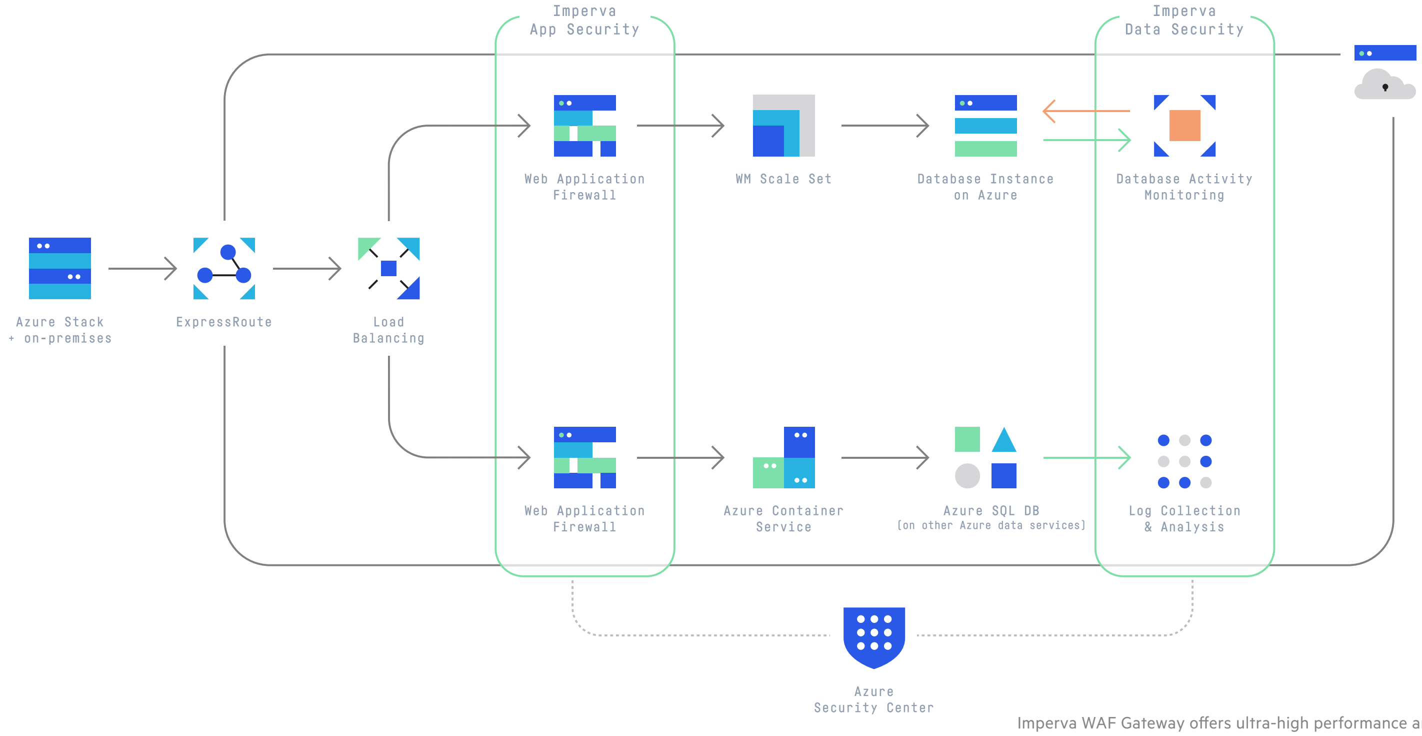
Protect applications and data on Microsoft cloud

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-premises data center. If your organization plans to move applications or data to the cloud, you need to extend your organizations current security and compliance controls to those resources. Otherwise, the cost savings you hoped to realize from cloud computing could evaporate – replaced by expensive data breach investigation, downtime, and lawsuits.

Imperva Data Security and Application Security solutions extend all of the industry leading on-premises security and risk management capabilities to Microsoft Azure. Imperva solutions are deployable as virtual machine on the Azure Infrastructure as a Service (Iaas) platform and are listed on Azure Marketplace for customers with a “bring your own licensing (BYOL) model”.

BENEFITS

- Protect applications on Azure with enterprise-class web application firewall
- Enable continuous data protection for Azure hosted databases and repositories
- Maintain consistent compliance and security risk management controls across cloud and on-premises resources



Imperva WAF Gateway offers ultra-high performance and resiliency for demanding data center environments.

Data protection for Azure

Imperva data audit and protection solutions provide standardized, real-time monitoring and protection across your sensitive data in the Azure cloud - and in on-premises enterprise resources - from the same management platform. Imperva data protection supports both Azure Infrastructure as a Service (IaaS) deployed databases, as well as Platform as a Service (PaaS) database offerings, such as AzureSQL. By supporting hybrid Azure cloud and on-premises environments, Imperva ensures enterprise-wide coverage and uniform risk management across cloud, traditional databases, file and Big Data environments through the following automated capabilities:

- Discovery and classification of sensitive data
- Database vulnerability assessment and user rights management
- Real-time detection and alerts for policy violating events across both Azure IaaS and Azure PaaS database hosts
- Automated security analytics, enhanced by machine learned role profiles, to pinpoint potential problems before they become actual compliance or security incidents.
- Notifications and reports of risky or malicious user behavior, including for privileged users, that non-database administrators can easily understand.

SUPPORT FOR AZURE SECURITY CENTER

Imperva Deployment Kit is available for customers to streamline provisioning and monitoring of multiple Imperva virtual appliances for Azure Security Center, and ensure the overall security posture of applications and data in Azure.

Application protection for Azure

Imperva 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 threat intelligence – a globally crowd-sourced service, to deliver superior protection for your web applications. The industry-leading Imperva 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: Real-time threat intelligence is crowd-sourced from Imperva customers worldwide and curated by the research team in Imperva 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 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 othe regulatory standards.
- Integration into Azure Marketplace: allows customers to quickly spin-up or spin-down WAF instances as your application traffic grows or shrinks.
- Virtually patch website vulnerabilities: to eliminate time-consuming emergency code fixes.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

imperva