Web Access Management on Azure

Many companies are strategically moving workloads to the cloud. At the same time, they are designing their development processes with increasing agility and adopting DevOps approaches in container-based environments.
As a result, application landscapes are becoming hybrid multi-cloud environments. These changes are having a huge impact on IT security infrastructure. In modern microservices architectures, containers are becoming an indispensable technological building block.

Secure Web Access Management service in hybrid cloud environments

What is Web Access Management on Azure?

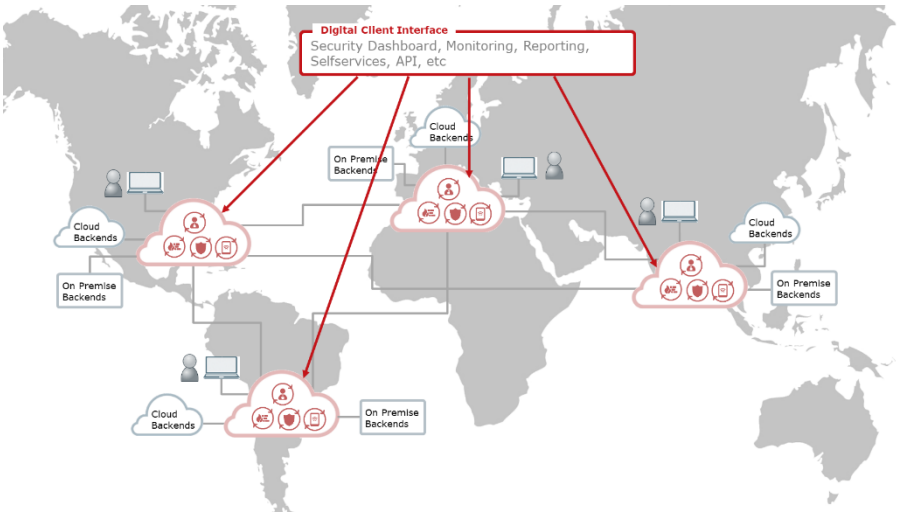
WAMoA is a modern container-based SaaS solution for OpenShift platforms in Azure and multi-cloud environments, addressing challenges in terms of security, e.g. web application protection and web access management, in hybrid setups. WAMoA helps companies provide complex applications and associated access management securely in the cloud (e.g. Azure) and on-premise. WAFs can be integrated in OpenShift as containers in any application environment.
Consistent authentication over the whole application landscape can be ensured through the use of a central IDP service such as SES ACCESS or the MS identity platform.

Your benefits with WAMoA

- **Implementation of cross-company access security guidelines** (security baseline) for all applications, regardless of application infrastructure
- **Thanks to application-centred delivery, faster releas**e cycles can be achieved (support for agile development processes and DevOps)
- **Dynamic orchestration and automation** of security layer supports dynamic and scalable applications
- **Central anomaly detection and central reporting** for hybrid environments are crucial in view of increasing cyber-security risks

With the digital customer portal (USP Connect®), the WAF can be configured and easily put into operation. The dashboard provides a comprehensive overview of the status and security information of WAF instances. Central reporting provides a user-friendly overview of security incidents.

Consolidated view of distributed infrastructure with USP Connect®



swisscom

Facts & Figures

Basic services	Container-based web application firewall in SaaS model
	- Scalable Secure Reverse Proxy with high-end WAF for complex application environments
	- Turnkey protection against OWASP Top 10 vulnerabilities
	USP Connect® as digital client interface
	- Central management of distributed instances in cloud environments (e.g. Azure and on-premise)
	- Central reporting with container-based log management
	Adherence to compliance regulations and standards such as PCI DSS 3.1 and EU GDPR
	- Authentication forwarding for identity providers
Optional services	Operational support
	Configuration support
	On-site support and professional services
Additional services with USP SES®	Access management (authentication, SSO, MFA)
	- User authentication
	- Single sign-on (incl. cross-domain)
	- Multi-factor authentication (MFA)
	- User self-service
	Federation capabilities
	- SP, IDP, IDP Broker, RP, OP
	Identity management (customer identity access management)
	- 3rd parties ID store
	- Provisioning
	- User admin and self-service

Swisscom (Switzerland) Ltd Enterprise Customers, P.O. Box,
CH-3050 Berne, Telephone 0800 800 900, www.swisscom.ch/enterprise

swisscom