

Built-in security enablement on Microsoft's Trusted Cloud



Microsoft® solutions run critical services and applications in almost every business around the world. Providing secure products that meet or exceed industry or government compliance is Microsoft's top priority. Companies can confidently leverage Microsoft's Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and supporting services knowing that Microsoft built them with a trusted security-by-design approach.

Microsoft partners with Coalfire – a leading cybersecurity advisory firm – on security and compliance initiatives, including validations, certifications, and authorizations. Coalfire's work helps Microsoft provide secure, compliant services to customers. Additionally, Coalfire proactively helps advise and educate Microsoft partners, customers, and prospects on leveraging Microsoft security and compliance investments and increasing their security posture.

MICROSOFT SECURITY IN THE CLOUD

With Microsoft security enablement built into Microsoft software, customers no longer need to question cloud security. Microsoft is also developing security tools to help customers increase their own security postures. Microsoft's shared responsibility means customers can only leverage Microsoft to a point – through control inheritance – before they must implement their own security programs to ensure their businesses meet security and compliance requirements.

MICROSOFT AZURE SHARED RESPONSIBILITY

RESPONSIBILITY	ON-PREM	IAAS	PAAS	SAAS
Data classification and accountability	Cloud customer	Cloud customer	Cloud customer	Cloud customer
Client and endpoint protection	Cloud customer	Cloud customer	Cloud customer	Cloud customer / Cloud provider
Identity and access management	Cloud customer	Cloud customer	Cloud customer / Cloud provider	Cloud customer / Cloud provider
Application level controls	Cloud customer	Cloud customer	Cloud customer / Cloud provider	Cloud provider
Network controls	Cloud customer	Cloud customer / Cloud provider	Cloud provider	Cloud provider
Host infrastructure	Cloud customer	Cloud customer / Cloud provider	Cloud provider	Cloud provider
Physical security	Cloud customer	Cloud provider	Cloud provider	Cloud provider

Legend: ■ Cloud customer, ■ Cloud provider

LEVERAGE MICROSOFT'S SECURITY INVESTMENTS

Businesses looking to migrate or build new applications in the cloud can leverage Microsoft's work in PCI DSS, HIPAA/HITRUST, ISO, SOC, Department of Defense (DoD), FedRAMP, and penetration testing for their own initiatives. Microsoft's efforts to protect the cloud enable customers to focus on securing the data they put into the cloud for their business needs.

With its architectural understanding of Microsoft's IaaS, SaaS, and PaaS environments; broad security; and regulatory compliance, Coalfire develops and provides reference architectures for Microsoft partners in a variety of industries. Referenceable architectures can help ensure that migration or deployment on Microsoft's platforms meets industry or multi-industry compliance best practices and efficiently enable customers to run in a secure, compliant manner.

EVALUATING MICROSOFT'S SECURITY POSTURE

Since 2010, Coalfire has provided Microsoft with advisory or assessment services to meet government compliance standards or industry requirements.

Microsoft product/service	Services performed by Coalfire
Azure®	PCI DSS assessment; PCI advisory; ISO 9001, 20000-1, 27001, 27017, 27018 certification; HITRUST CSF certification; GDPR assessment; technical evaluation white paper; NERC services; cyber engineering (security architecture)
Azure Germany	PCI assessment; ISO 9001, 20000-1, 27001, 27017, 27018 certification
Azure Government	PCI DSS assessment; ISO 9001, 20000-1, 27001, 27017, 27018 certification
Cloud and Enterprise (became part of Azure)	PCI DSS assessment; ISO 9001, 20000-1, 27001, 27017, 27018 certification
Cloud-in-a-box	FedRAMP pre-assessment
Commerce Engineering Operations	PCI DSS gap analysis, assessment, and scans
Endpoint protection/client security (EP/CS)	Technical evaluation white paper
Health Agent	HIPAA assessment
Intune (consumed by Azure)	FedRAMP pre-assessment, HIPAA assessment, SOC2 gap assessment
Microsoft Commerce	ISO 27001 and 27018 internal audits
Microsoft DataGrid	ISO 27001 internal audit
Microsoft Dynamics® (consumed by Azure)	FedRAMP advisory and supporting documentation development (2017), FedRAMP assessment (2018), PCI DSS assessment

Microsoft product/service	Services performed by Coalfire
Microsoft Next Generation Privacy (NGP)	ISO 27001 and 27018 internal audits
Microsoft Office 365®	FedRAMP assessment, FedRAMP advisory and supporting documentation development (2015), PCI DSS assessment, HITRUST assessment, IRS 1075 review, DoD SRG assessment
Microsoft retail stores	PCI assessment
Order Management (phased out)	PCI DSS gap analysis, assessment, and scans
Skype®	PCI DSS gap analysis and assessment
Windows® 10	Penetration testing
Windows Server®	Technical evaluation white paper

SECURITY BY DESIGN

The Coalfire Engineering Team can design, build, and optimize compliant and secure-by-design Microsoft reference architectures to the following standards:

U.S. public sector: FISMA, FedRAMP, Criminal Justice Information Services (CJIS), IRS 1075, NERC CIP, and DFARS/NIST SP 800-171

Financial: Federal Financial Institutions Examination Council (FFIEC); PCI DSS; SOC; and ISO 9001, 20000-1, 27001, 27017, 27018

Healthcare: HIPAA; HITRUST; SOC 2 Type 1/2; and ISO 9001, 20000-1, 27001, 27017, 27018

Retail and Technology: PCI DSS; SOC; and ISO 9001, 20000-1, 27001, 27017, 27018

About Microsoft

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more. www.microsoft.com

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com



For more information about Coalfire, visit Coalfire.com, or to speak to an expert about your organization's security needs, visit Coalfire.com/contact.