COALFIRE

Built-in security enablement on Microsoft's Trusted Cloud

Azure

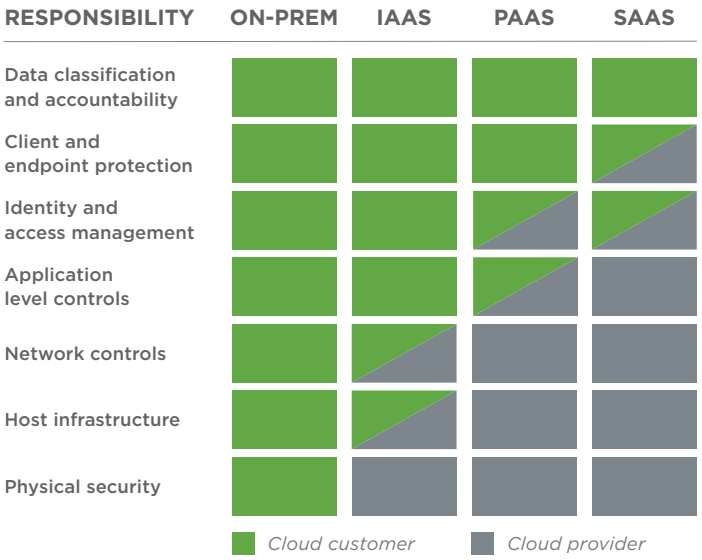
Microsoft® solutions run critical services and applications in almost every business around the world. Providing secure products that meet or exceed industry or government compliance is Microsoft's top priority. Companies can confidently leverage Microsoft's Software-as-a-Service (SaaS), Infrastructure-as-a-Service (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 clients. Additionally, Coalfire proactively helps advise and educate Microsoft partners, clients, 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, clients no longer need to question cloud security. Microsoft is also developing security tools to help clients increase their own security postures. Microsoft's shared responsibility means clients 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



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 27001 and ISO 27018, SOC, DoD, FedRAMP, and penetration testing for their own initiatives. Microsoft's efforts to protect the cloud enable clients 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 clients 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. The table provides examples of Microsoft products and services that Coalfire helped secure for regulatory compliance.

Microsoft product/service	Regulatory compliance services performed by Coalfire
Azure®	• PCI DSS assessment • PCI advisory • ISO/IEC 27017:2015 certification • HITRUST CSF Certification • Technical evaluation white paper • NERC services • Cyber engineering (security architecture)
Azure Government	PCI DSS assessment
Cloud and Enterprise	PCI DSS assessment
Cloud-in-a-box	FedRAMP pre-assessment
Endpoint protection/client security (EP/CS)	Technical evaluation white paper
Health Agent	HIPAA assessment
Intune	• FedRAMP pre-assessment • HIPAA assessment • SOC2 gap assessment
Microsoft DataGrid	ISO/IEC 27001:2013 internal audit
Microsoft Dynamics®	FedRAMP advisory, assessment, and supporting document development
Microsoft Next Generation Privacy (NGP)	ISO/IEC 27001:2013 and ISO/IEC 27018:2014 internal audits
Microsoft Office 365®	• FedRAMP advisory, assessment, and supporting document development • FISMA advisory • Controls mapping and assessment
Microsoft Worldwide Services	ISO 27001 and ISO 27018 internal audits
Order Management	PCI DSS gap analysis, assessment, and scans
Skype®	PCI DSS gap analysis and assessment
Universal Store (formerly Commerce Platform)	PCI DSS gap analysis, assessment, and scans
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 27001/2/18

Healthcare: HIPAA, HITRUST, SOC 2 Type1/2, and ISO 27001/2/18

Retail: PCI DSS, SOC, and ISO 27001/2/18

Technology: PCI DSS, SOC, and ISO 27001/2/18

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 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 more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**

COALFIRE.

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