AZURE SECURITY REVIEW

As enterprises adopt cloud-based platforms, the number of high-profile data breaches continues to increase. Too many of the world's well-recognized brands are dealing with the aftermath of these disturbing events. Organizations must consider cybersecurity risks to cloud resources just as they would in an on-premises environment—including how they approach privileged access management.

IDENTIFY AND MITIGATE CLOUD VULNERABILITIES

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce the risk of sensitive information exposures.

To help enhance our clients' cloud security posture in Microsoft® Azure®, Sirius offers an Azure Security Review that maps policies to cloud standards. We ensure that your policies are aligned to industry standards or measure your progress to them. If you have existing policies that need review, we can work with your teams to identify current state and recommend a course of action.

Gold Microsoft Partner

Microsoft

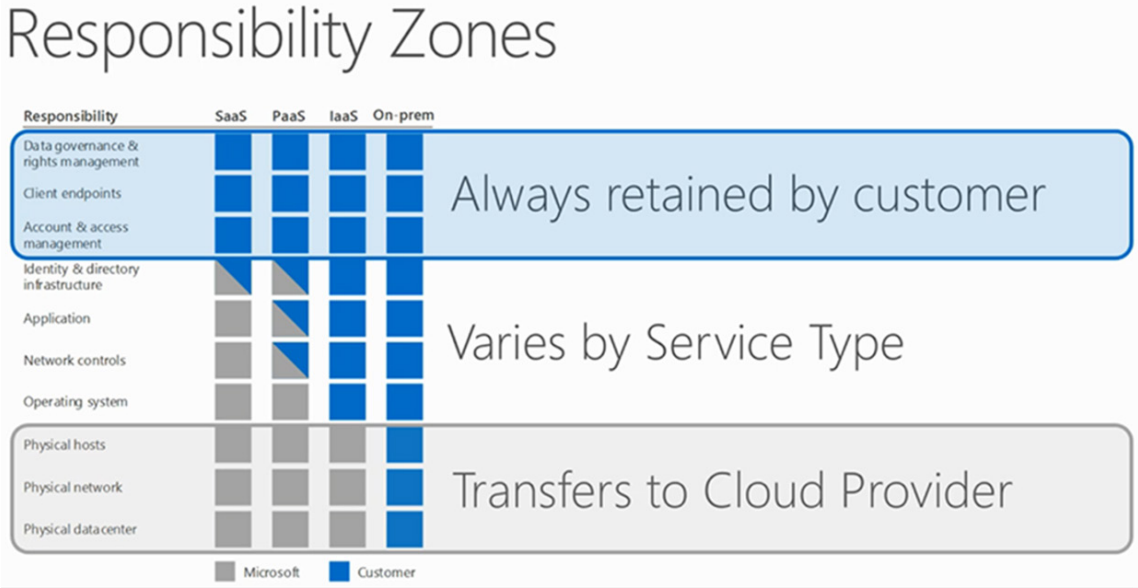
DEDICATED TEAMS OF AZURE, CLOUD AND SECURITY EXPERTS

Sirius will help you advance your security and optimize your overall IT risk management strategy to help protect your data, intellectual property and brand. Sirius offers leading-edge technology solutions, expert implementation and advisory services, and managed security services as well as customized testing in our state-of-the-art Technology Enablement Centers.

With a dedicated Microsoft Azure practice consisting of certified cloud consultants and technologists, Sirius applies engaging, practical and proven methodologies to ensure that clients achieve their cloud goals. Our team of cloud experts can also provide clients a full-service life cycle of cloud offerings from plan and design to operational transition.

SHARED RESPONSIBILITY MODEL

Security is a multilayered subject in every public cloud, including Azure. When analyzing security for an environment hosted in Azure, the following responsibilities matrix is taken into account.



THE SIRIUS APPROACH TO CLOUD SECURITY

As part of our Azure Security Review, we work with your team to uncover where security threats could compromise your environment. Our methodology is based on past client experiences and comprises seven design principles for cloud security:

- **Implement a strong identity foundation:** Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your Azure resources. Centralize identity management and aim to eliminate reliance on long-term static credentials.
- **Enable traceability:** Monitor, alert and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
- **Apply security at all layers:** Apply a defense-in-depth approach with multiple security controls to all layers. For example: edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code.
- **Automate security best practices:** Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
- **Protect data in transit and at rest:** Classify your data into sensitivity levels and use mechanisms such as encryption, tokenization and access control where appropriate.
- **Keep people away from data:** Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling, modification and human error.
- **Prepare for security events:** Prepare for an incident by having incident management and investigation policy and processes that align to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation and recovery.

For more information, please contact your Sirius client executive, visit siriuscom.com, or call 800-460-1237.

SIRIUS