Cisco Cloud Security Solutions

Q. Why is cloud security important?
A. Cloud computing changes the way information and services are provided and consumed. Faster, more responsive, and more efficient use of resources leads to better business performance and competitiveness, allowing organizations to achieve their business goals at an accelerated pace. At the same time, cloud computing introduces new security risks and concerns around technology and business processes. To succeed with cloud computing, organizations must address cloud security concerns.

Q. Can you share some examples of customer cloud security concerns?
A. Here are three typical categories of security issues related to cloud computing.

1) Existing security vulnerabilities that are amplified by cloud technology. XML-based communications, for example, are known to be prone to attacks. Recently, researchers have demonstrated cloud security issues using an XML signature wrapping attack technique.

2) New technology challenges. Multitenancy is a good example. Instead of having a physically dedicated infrastructure for each customer, cloud service providers use technologies such as virtualization to pool computing and storage resources together to deliver more efficient services. Many customers have concerns about the security and privacy of data in such shared environments.

3) Ownership and responsibilities. Cloud computing brings an increase in shared responsibilities and, in some cases, gray areas. For example, if there is a data breach in the cloud, whose responsibility is it? The cloud service provider or the data owner?

Q. How do we approach cloud security?
A. Cloud security needs to be addressed at both the technology and business levels. Organizations need to include security in their overall cloud computing planning process and make it an integral part of organizational governance and culture. When deciding what to move to the cloud, customers should assess their business goals and architectural requirements, and build security into the cloud architecture so that it is pervasive and robust. Once a cloud security solution has been implemented, accountability and improvement processes are critical to keep up with changing threats and evolving technologies.

Q. What are the architectural considerations for cloud security?
A. A cloud security solution needs to meet and support the following architectural requirements.

1) Logical separation. Security controls need to be implemented to secure logical entities, which can include both physical and virtual infrastructure components.

2) Policy consistency. It is critical to have a cloud security policy design that can be enforced consistently in both physical and virtual environments.

3) Automation. In a cloud computing environment where resources are shared dynamically, there are two security requirements: Cloud security needs to support an automated environment where resources such as virtual machines (VMs) may move around, and cloud security itself needs to be provisioned through an automated process.

4) Authentication and access control. With the “anytime, anywhere” availability of cloud services, security policies are needed to validate user credentials and authorize their cloud services.
5) Scalability and performance. A cloud computing implementation will need to securely support large workloads and the underlying infrastructure, such as high-density VMs. Firewall and IPS services, for instance, must be able to scale so that they do not become the bottleneck.

Q. What do Cisco® Cloud Security solutions help us achieve?
A. The Cisco SecureX framework enables consistent cloud-based security policies and enforcement, up-to-date threat intelligence, greater scalability, and improved performance, helping to remove barriers so that customers can achieve the economies of scale and efficiency of cloud computing.

Q. What is the Cisco SecureX framework?
A. **Cisco SecureX** is a context-aware approach to security that includes context-aware policy and enforcement, using the network as the architectural foundation. Cisco SecureX enables:

- Greater alignment of security policies with business needs
- Integrated global intelligence
- Simplified security and policy delivery
- Consistent security enforcement throughout the organization

Customers can use the Cisco SecureX framework to increase visibility into their networks, strengthen their policy controls, and improve IT efficiency.

Q. What is Cisco Security Intelligence Operations?
A. **Cisco Security Intelligence Operations** (SIO) is a cloud-based security service that delivers global threat information, reputation-based services, and sophisticated analysis to provide stronger protection with faster response times.

Q. What cloud security solution capabilities does Cisco provide?
A. There are three sets of solution offerings in the Cisco Cloud Security solution portfolio: Secure Cloud Infrastructure, Cloud Security Services, and Secure Cloud Access & Communications.

1) Secure Cloud Infrastructure solutions include high-end firewall, VPN, and IPS solutions, as well as the Cisco Virtual Security Gateway and Cisco ASA 1000V Cloud Firewall.

2) Cloud Security Services include Cisco SIO services, Cisco IronPort® Cloud Email Security, and Cisco ScanSafe Cloud Web Security.

3) Secure Cloud Access & Communications solutions include Cisco AnyConnect™, Cisco TrustSec®, and the Cisco SaaS Access Control solution.

Q. How do Cisco Cloud Security solutions address customers’ security concerns?
A. Cisco Cloud Security solutions provide customers with context-aware security policy controls and enforcement so that they can address their specific concerns effectively. Context-aware security identifies users and other related information to make dynamic and intelligent network access, control, and threat protection decisions. For example, a critical SaaS revocation capability enables secure access to cloud-based SaaS applications. SaaS users are authenticated at a central location within the SaaS cloud subscriber organization. After successful authentication, Security Assertion Markup Language (SAML) is used to authorize access to SAML-enabled SaaS applications.

Q. How do Cisco Cloud Security solutions help meet architectural requirements?
A. Many architectural considerations are built into Cisco Cloud Security solutions. For instance, logical control is fully supported via **Cisco Virtual Security Gateway** zone-based security policy controls, and multitenant edge
security is enabled by the Cisco ASA 1000V Cloud Firewall. The Cisco ASA 5585-X Adaptive Security Appliance provides industry-leading MultiScale™ performance, enabling rapid connections per second, an abundance of concurrent sessions, accelerated throughput, and multiple security services for exceptional flexibility. In a virtual environment, these capabilities are equally well supported by the Cisco Virtual Security Gateway which supports high VM density. Furthermore, the Cisco Virtual Security Gateway includes the vPath steering mechanism with enhanced “fast path offload” performance.

Q. What cloud security recommendations do you have for cloud service providers?

A. Cloud service providers can greatly improve their business results by focusing on the following areas:

- Promoting transparency and awareness to address customer security concerns
- Maintaining a strong security posture
- Offering robust security services in the overall cloud service portfolio
- Using the various cloud security and architectural considerations discussed here to deliver cloud security

Q. What cloud security recommendations do you have for private and hybrid cloud practitioners?

A. Private and hybrid cloud practitioners can help accelerate the adoption of a cloud computing solution by concentrating on the following areas:

- Incorporating cloud security into corporate governance
- Building security into cloud architecture
- Specifying cloud security accountability and establishing review cycle to ensure improvements
- Using the various cloud security and architectural considerations discussed here to implement cloud security

Q. What cloud security recommendations do you have for general cloud customers?

A. General cloud customers can help achieve cloud strategy success by putting their efforts in the following areas:

- Including security risk management as part of their overall cloud strategy
- Collaborating with cloud service providers to understand each other’s rights and responsibilities
- Sharing best practices with the community
- Using the various cloud security and architectural considerations discussed here to engage cloud service providers

Q. What is unique about Cisco Cloud Security solutions?

A. Cisco Cloud Security solutions are based on the Cisco SecureX framework, an approach that provides context-aware policy and enforcement to gain deeper visibility, stronger controls, and better IT efficiency. Cisco SIO adds global visibility and threat intelligence to the Cisco Cloud Security solution portfolio. Cisco has the unique ability to integrate cloud security with networking and data center technology to meet the scalability and performance requirements of cloud computing, and provides a rich set of security solution deployment options that cover physical appliances, switch service modules, virtual appliances, and cloud-based security services to meet different customer needs.
Q. Where can I find more information about Cisco cloud security solutions?
A. Please visit the Cisco SecureX website and Cisco Cloud Security solutions website for further information.