The biggest cloud security challenges are around consistency, permissions, and scale. Security teams have the additional challenge of supporting a hybrid or multi-cloud environment. Organizations require an effective way to manage security across environments with consistency of processes and policies. This has been challenging as teams work to define security best practices to workloads and cloud service providers (CSPs).

It's important to follow industry-defined security best practices to improve our security posture and compliance risk. To support this, organizations need to ensure their cybersecurity team has the processes and tools necessary for cloud security requirements. This also includes implementing role-based access control (RBAC) for Kubernetes environments, automated vulnerability management, and monitoring Kubernetes clusters for misconfigurations/vulnerabilities.

Lack of visibility into public cloud infrastructure hosting our cloud-native applications impacts our security posture. It has been challenging for security teams to support the move to cloud services and to worry about underlying infrastructure or maintenance. At the same time, they need to support their applications in on-premises environments. This makes it challenging for security teams to support the move to cloud services and to worry about underlying infrastructure or maintenance.

Lack of clarity on the shared responsibility security model impacts our security operations complex and time-consuming. The security staff has to aggregate results from multiple tools in use for asset inventory.

Organizations report an elevated information security risk due to cross-environmental complexity and processes. Problems arise when they need to accurately track and report on effective security measures to stakeholders.

The Cisco Cloud Protection Suite delivers a modern application security approach with end-to-end security for hybrid and multi-cloud application environments. From bare-metal to cloud-native infrastructure, the suite provides customers with holistic application security, safeguarding workloads across environments, both on-prem and in the cloud.

It is critical for hybrid and multi-cloud environments for organizations to have a comprehensive solution that can manage security across environments. The Cisco Cloud Protection Suite provides organizations with the tools necessary to maintain security consistency across environments, ensuring a secure and efficient cloud experience.

Moving from Multiple, Siloed Tools to a Higher-efficacy Solution

The biggest cloud security challenges are around consistency, permissions, and scale. Security teams have the additional challenge of supporting a hybrid or multi-cloud environment. Organizations require an effective way to manage security across environments with consistency of processes and policies. This has been challenging as teams work to define security best practices to workloads and cloud service providers (CSPs).

It’s important to follow industry-defined security best practices to improve our security posture and compliance risk. To support this, organizations need to ensure their cybersecurity team has the processes and tools necessary for cloud security requirements. This also includes implementing role-based access control (RBAC) for Kubernetes environments, automated vulnerability management, and monitoring Kubernetes clusters for misconfigurations/vulnerabilities.

Lack of visibility into public cloud infrastructure hosting our cloud-native applications impacts our security posture. It has been challenging for security teams to support the move to cloud services and to worry about underlying infrastructure or maintenance. At the same time, they need to support their applications in on-premises environments. This makes it challenging for security teams to support the move to cloud services and to worry about underlying infrastructure or maintenance.

Lack of clarity on the shared responsibility security model impacts our security operations complex and time-consuming. The security staff has to aggregate results from multiple tools in use for asset inventory.

Organizations report an elevated information security risk due to cross-environmental complexity and processes. Problems arise when they need to accurately track and report on effective security measures to stakeholders.

The Cisco Cloud Protection Suite delivers a modern application security approach with end-to-end security for hybrid and multi-cloud application environments. From bare-metal to cloud-native infrastructure, the suite provides customers with holistic application security, safeguarding workloads across environments, both on-prem and in the cloud.