White paper
Cisco public

Best Practices in Securing a Multicloud World

Actions to take now to protect data, applications, and workloads

We live in a multicloud world. A world where a multitude of offerings from Cloud Service Providers (CSPs) give us the potential to agilely respond to business opportunities and challenges at a moment's notice. With application and infrastructure services deployed across public, private, and hybrid clouds, it is easier than ever before to add new services and rapidly increase capacity during periods of peak demand. In a multicloud world, it is easier to access, build, store, and host the data, applications, services, and infrastructure that run our businesses.

In recent studies, 84 percent of business leaders surveyed reported using multiple clouds to address their business needs. Yet a third of respondents had a mature cloud strategy. Complicating this is the shortage of cybersecurity talent. Why does this matter?

In a multicloud world, everything changes. While it's easier to deploy new IT services, we may lose visibility and control unless we make changes to the way we manage security. The security tools and processes that we've used in our networks and data centers will not work in public clouds. We lose visibility into the behavior of users, the disposition of data, and the network. The cloud services we consume may be delivered on several different platforms. Yet we must still protect privacy and data, and detect and respond to threats across all of our clouds. We need the same visibility and discovery for cloud applications and workloads that we can get on the network behind our firewalls. To accomplish this, it's critical to adapt our security processes, technologies, and knowledge.

Businesses face another challenge: the security risks introduced by shadow IT. Business units are constantly looking for greater speed and agility. To achieve it, they may bypass their IT departments and buy application and infrastructure services directly from CSPs. When this happens, the business unit personnel may not know how to evaluate whether a provider has adequate security capabilities, or, if the provider does, how to configure and manage these. This accentuates the tension between IT and business units and exposes the business to unnecessary risks.

What can we do to address these challenges? How do we help ensure that we are meeting our organization's business, audit, and compliance requirements in a multicloud world?

To do so, we need:

- A complementary, coordinated approach to security across networks, endpoints, and the cloud that assesses risks across multiple cloud environments
- Tools designed to provide visibility, analytics, control, and responsiveness in a multicloud environment
- Knowledge of what our CSPs provide and what they don't provide, so we can protect, react, and respond, no matter where our data, applications, and workloads reside

Other essential elements include:

- Repeatable policies and procedures that adhere to our business, audit, and compliance requirements and are tailored to our current and desired future states of cloud security
- Cybersecurity talent that understands how to think through multicloud security

We need to obtain the level of control in a multicloud environment that we have with our on-premises infrastructure. That means helping to ensure the cloud controls and technologies we adopt will give us the visibility and protection our business requires.

Software-as-a-Service (SaaS) applications and hybrid workloads on Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) clouds are widely used in multicloud environments. Let's look at some specific issues and best practices for each of these types of public cloud services.

The best practices are grouped into five categories:

- **Discover** the unsanctioned SaaS applications or IaaS and PaaS workloads deployed
- **Assess** our cloud service providers' security capabilities and whether our data, applications, and workloads have the right controls, policies, and processes in place
- **Create** a cloud strategy and roadmap
- **Define and communicate** policies, processes, and technologies to our people
- **Detect and respond** to threats from across our multicloud environment

Security best practices for SaaS applications

SaaS application usage is frequently a blind spot for organizations. Attackers can compromise cloud identities, gain access to information stored in the cloud through excessive file shares and public data exposures, and create malicious applications that connect to users' cloud identities by exploiting the Open Authorization (OAuth) protocol.

At the same time, email is still a leading attack vector. Billions of emails are sent daily and lots of business is done over email. Migration to a cloud-based solution reduces the burden of management and deployment on IT, but it also leaves businesses vulnerable due to the loss of visibility and control over the security of their solutions.

Here are the best practices for dealing with these SaaS challenges:

1. Discover

The first step is to discover what cloud apps users access on the network. We need to understand application and vendor information, usage data, and risk evaluations.

2. Assess

Once we understand what SaaS applications we have and would like to adopt, we need to ask:

- How do we meet our business, audit, and compliance requirements?
  - What are the regulatory requirements we need to meet? (For example, these may include Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), or General Data Protection Regulation (GDPR))
  - What are our business and audit requirements?
  - Given these requirements, which applications I should use in the cloud?
  - Will these applications be used in a country that limits data storage to that country?
  - Can the SaaS vendor meet these requirements?
- What does third party intelligence reveal about the security of the SaaS provider?
- Does the SaaS provider:
  - Have the right security controls and processes in place?
  - Offer the right protection across our data?
  - Make it possible for us to conduct our own security verification, such as penetration testing of the application and network layer?
- For each SaaS application, does the provider offer the ability to:
  - Connect the application to the identify management platform using single sign-on?
  - Implement multifactor authentication selectively? (For instance, we may wish to require that certain groups use two-factor authentication because they have access to sensitive data.)
  - Generate telemetry that allows us to audit every action in the application, such as uploading, deleting, giving or removing access, and user login and logout?
  - Encrypt data using standard encryption practices?
  - Determine where data is stored?

3. Create

We can reap more benefits from our SaaS application services investments above by applying our learning to our desired future state. Two ways to do this are to:

- Create a services catalog that includes the security profile of the approved SaaS applications that we currently have and defines the security criteria for adding new ones.
- Develop a strategy and roadmap that considers privacy, security, compliance, and business requirements across our multicloud landscape.

4. Define and communicate

Once we have verified that our SaaS providers meet our security standards, we need to define the security policies and processes that will help us protect, detect and respond. We need to:

- Incorporate cloud security tools into our processes that help us discover unsanctioned applications and provide ongoing applications visibility to on and off-network cloud activity.
- Train our security operations team on our new tools, policies, and procedures, so they can incorporate these into their ongoing operations.
- Educate our users about their role in protecting the business from online attackers.

5. Detect and respond

Finally, and most importantly, we need to monitor cloud application activities, detect threats, and respond quickly to contain and remediate these. To do this we need to:

- Incorporate and monitor the telemetry generated from our SaaS applications into our malware protection solutions and processes.
- Identify ways to keep cloud productivity apps, especially email, safe. Email is the number one attack vector.
- Adopt a security solution that protects and secures cloud-based email.

Now that we have identified the best practices for securing SaaS applications, let's look at hybrid workloads on IaaS platforms.

Five security best practices for data and workloads on public IaaS and PaaS platforms

Organizations often have little visibility into and control over their use of the cloud. Just as with the adoption of SaaS applications, many organizations are moving data and workloads onto public clouds, taking advantage of Amazon Web Services (AWS), Microsoft Azure, and other IaaS and PaaS platforms. Some of the moves are unsanctioned and made by employees who don't understand their business' security and compliance requirements.

Consequently, organizations may not know how to leverage the security options offered by CSPs. While public cloud providers are beginning to add more security options, they don't offer the same security visibility and detection as an organization's on-premises network that is protected by the full traditional security stack. Attackers take advantage of these vulnerabilities to compromise access to public cloud services. That way, they can steal workloads and use public cloud instances as command and control to serve up malware or merely destroy data.

How do we address these challenges and securely take advantage of IaaS and PaaS on public clouds? The best practices are similar to those for SaaS applications. We need to:

1. **Discover** the network flows with IaaS and PaaS public clouds.
2. **Assess** the security profile of our CSPs and determine whether they can:
   - Deliver the security needed to protect our data and workloads.
   - Meet our business, audit, and compliance requirements.
   - Provide the telemetry needed for us to monitor, analyze, and detect threats.
3. **Create** a cloud strategy and a security architecture roadmap that will help us address gaps and achieve our desire future state across our multicloud landscape.
4. **Define and communicate** our new cloud policies, processes, and technologies for protecting our data and workloads as they move to, from, and within IaaS and PaaS clouds, and:
   - Verify that the Security Operations Center (SOC) can:
     - Track workload movements and determine what's good and bad.
     - Monitor and manage threats during periods of peak demand. (For example, what's happens when an application spins up and uses 1,000 servers to meet demand?)
   - Train our Security Operations team.
   - Educate our employees.
5. **Detect and respond** to threats to our data and workloads hosted on our now more secure IaaS and PaaS public cloud environments.

How Cisco protects your multicloud world

Cisco takes a complementary, coordinated approach to security across networks, endpoints, and the cloud. This framework is critical because of the interconnected nature of these three elements and the clear detection benefits that result from a holistic approach. An effective cloud security strategy must incorporate inputs from the network and endpoints to help assess risk across multiple cloud instances. Cisco recognizes the complexity of a multicloud environment and extends security to, for, and from the cloud. This results in consistent, comprehensive security architecture that allows you to extend your security posture to the cloud with confidence.

For organizations who want strategic advice, knowledgeable implementation of Cisco solutions, or expert help designing and managing their multicloud environments, Cisco offers a full range of advisory, implementation, and managed security services. For example, these services can help organizations:

- Address their business, audit, and compliance requirements.
- Assess and identify the security gaps with the public cloud services currently being used.
- Identify the new security policies and procedures needed.
- Evaluate whether technologies being considered will satisfy the organization's cloud security needs.
- Develop a customized cloud security strategy and roadmap.
- Accelerate implementation of Cisco cloud security solutions.
- Manage detection and response.

Cisco cloud security offerings now include the most complete shadow IT solution in the market, stronger email threat protection for cloud-hosted email, and a deeper level of security visibility and control for public cloud infrastructure.

These new capabilities add to the Cisco cloud security portfolio for comprehensive, industry-leading cloud security that helps organizations move forward with confidence in a multicloud era.

Cisco can help you:

Get a grip on shadow IT

Take advantage of consistent app visibility and discovery for apps at the office behind the firewall, now extended to include cloud and SaaS apps both at the office and off the premises.

Protect productivity apps

Keep cloud productivity apps like email safer than ever.

Improve visibility

Get real-time security visibility, insights, and control over workloads in the cloud

Block malware

Stop malware before it reaches your network or endpoints so you can reduce the time spent remediating infections.

Extend user protection

Protect users anywhere they go, and anywhere they access the Internet. Protect users, data, and apps in the cloud against compromised accounts, malware, and data breaches.

Keep users productive

Help enable secure cloud use by improving security with no impact on end-user productivity.

Let's get started

The Cisco® Cloud Security Assessment Service can help meet your privacy, security, compliance, and business requirements in your multicloud environment. We will help you improve network visibility, identify risks, and speed cloud adoption while improving security.

Visit our Security Services page to connect with our advisors and protect your business today.

Why Cisco?

The Cisco security architecture integrates security across the network, endpoints, cloud, and email for a more effective security posture that sees a threat once and protects against it everywhere. With an architecture consisting of services and products designed to fit and work together, we stop more threats, respond faster, lower costs, and deliver automation for a force-multiplier effect for IT teams. Our services and solutions are delivered by highly trained, experienced security experts who are focused on your business and understand your challenges and objectives.