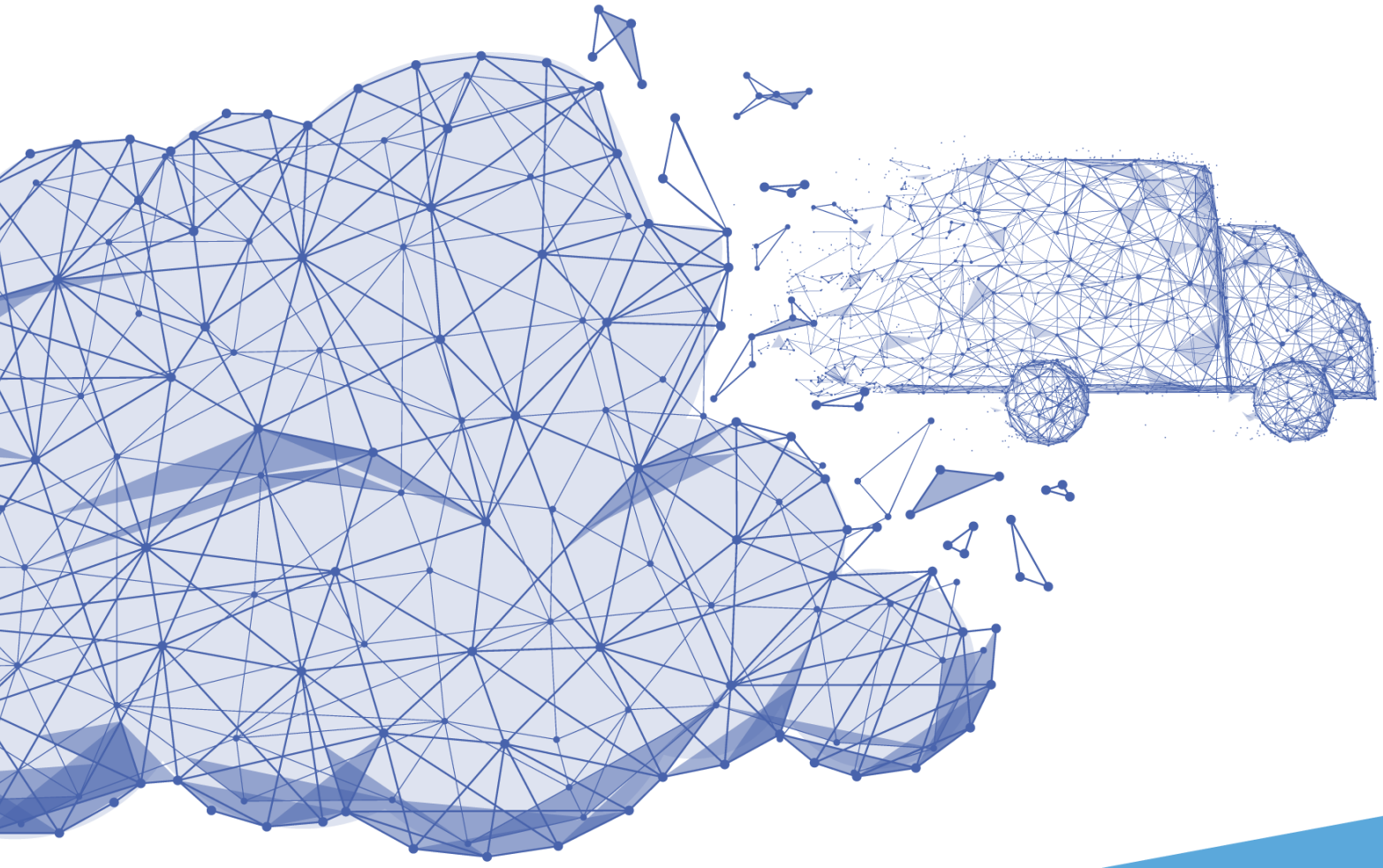


Supply Chain Management in the Cloud

Whitepaper

attila SECURITY

The Problem

For as long as organizations have worked together to move products or services from supplier to customer, sensitive business data has flowed up and down the supply chain. Today this information may be transmitted via email, eCommerce platform, application program interfaces (APIs) or through direct access to a supply chain partner's network. Data isn't the only thing that flows up and down the supply chain. So does risk. A security breach at a supplier or customer is a threat to every member of the supply chain.

Mitigating supply chain risk has become even more complex in recent years, because data now nearly always flows through, or is stored in, one or more public or private clouds. Moving data to or through the cloud exposes it to a new set of unique security risks. A security breach at one of the supply chain members' cloud provider is a risk to every member of the supply chain. This ripple effect even impacts organizations that don't have data in the cloud - simply by association they are at risk too. In essence, the security perimeter of every company is now in the cloud.

One of the things that makes the cloud unique is the concept of *shared security responsibility*. When a company contracts for cloud services, it's a shared responsibility of both the cloud service provider and the company to secure the data. So, even if the cloud provider's security is bulletproof, company data may still be at risk, depending on the company's security capability. Compounding matters, hackers tend to focus on the most lucrative targets. And there's nothing more lucrative than penetrating a cloud provider. A successful attack on a cloud provider doesn't yield data from one company, it can yield data from hundreds or thousands of companies.

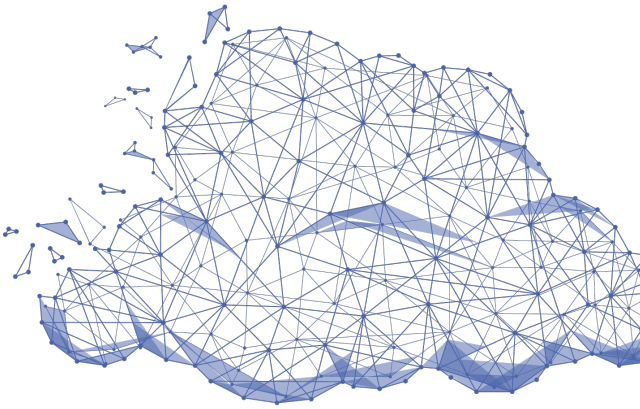
As members of a supply chain, companies need to understand the unique risks associated with doing business in the cloud and then adopt strategies to mitigate those risks. Some of the more impactful risks include unauthorized use, insecure interfaces, multi-tenancy and multi-cloud risks. There's also the risk from "Shadow IT" and Bring Your Own Cloud (BYOC).

"There's nothing more lucrative than a successful attack on a cloud provider."

Unauthorized Use

One of the risks inherent in the cloud is unauthorized use of cloud assets. This can occur either intentionally or unintentionally. In the first scenario, consider that public cloud providers such as Amazon or Microsoft do little vetting of their customers—usually anyone with an email address and a credit card can sign up. This makes it easy for malicious actors to gain access to the cloud, which is the first step in unauthorized use.

The second scenario, unintentional unauthorized use, often involves company employees. With bring-your-own cloud (BYOC), employees are allowed to use public or private third-party cloud services to perform their job. Unfortunately, employees may use unauthorized or untested cloud services. They may or may not follow security policies. And to complicate matters, IT departments are frequently unaware of the extent to which employees are downloading apps or using cloud services. According to cloud service provider Trapp Technology, nearly half of cloud services in use in organizations today are commissioned without the involvement of the IT department.



Insecure Interfaces

Another risk associated with the cloud is insecure interfaces. APIs enable a computer at one company to talk to a computer at another company without human intervention, and APIs are responsible for automating almost all intercompany transactions today. Every computer communicates with the cloud through an API, and in this manner, APIs expose clouds to the world.

While APIs make communication convenient, they also leave it vulnerable. APIs require keys, which aren't always adequately secured. APIs often use clear-text authentication for transmission of content. However, without adequate security, the authorization may be compromised. The bottom line is that a perfectly secure standalone system can be made insecure by placing it in the cloud with access via an API. This means a single vulnerable API deployed by a member of a supply chain puts everyone at risk.

Insufficient Access Management

Access management is a method for granting authorized users the right to use a service, while preventing access to non-authorized users. This usually involves a username and password. Insufficient access management leaves clouds vulnerable.

Just as with unauthorized use, insufficient access management can occur in two ways. The first scenario is through an inadequate credentials policy that doesn't require strong passwords or frequent updating. The second scenario is through a risk known as Shadow IT. Shadow IT refers to “rogue” IT systems, or those that were built and deployed without explicit approval by the organization. Since activities that are outside of the control of the IT department are also outside the IT department's policies, even if a company's password policy is sufficient, Shadow IT within that company can threaten the entire supply chain.

Multi-Tenancy Issues

Perhaps the greatest risk to cloud services is multi-tenancy. Cloud services are cost effective because they share resources among customers including hardware, software and databases. This sharing of resources is referred to as *multi-tenancy*. But this sharing also makes the resources vulnerable. For example, a single database can be shared by hundreds of customers at once, which means their data is essentially comingled in the same data structure. With multi-tenancy, security threats that would otherwise be isolated to one organization, can leave multiple organizations exposed. Here are just a few examples: the credentials an employee at the cloud provider may get compromised, a database administrator may accidently grant someone access to the wrong organization’s network, a hacker may break the encryption of one organization in a multi-tenant database. Multi-tenancy puts unaffiliated organizations in close digital proximity to each other. It's a risk inherent to the cloud which means it's a risk inherent to the supply chain.

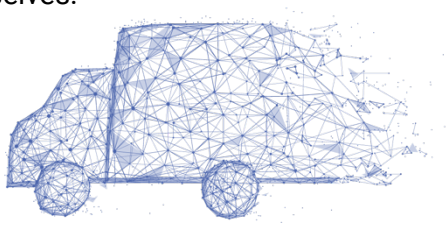
Multi-cloud Issues

Multi-cloud architecture is the result of a company procuring cloud services from more than one cloud service provider. Companies do this to take advantage of best-of-breed services and to add system redundancy. Cloud diversification is a large and growing trend. According to a survey by Forrester Consulting, 86% of global organizations with 1,000 employees or more have adopted a multi-cloud strategy.

Securing services from more than one cloud provider comes with its own set of security challenges. Multi-cloud security risks stem from several factors. First, configuration and deployment of various clouds is unique, which can pose some problems. Organizations don't always have staff with multi-cloud experience, which may leave these systems vulnerable. Also, companies don't always invest in all the tools required to ensure the clouds are compatible. In addition, multi-clouds generally means more APIs, which translates to more entry points for hackers. When taken in the context of the supply chain, the security risks associated with multi-cloud architectures are just like every other security risk: the ripple effect applies.

Protection from the Supply Chain

Because of the unique risks associated with the cloud, a supply chain is never 100% secure. The data moving back and forth between an organization and various members of its supply chain must be protected to the greatest extent possible and cloud service providers simply cannot be relied upon to provide that protection – it must come from the supply chain members themselves.



Organizations are encouraged to lock-down access to all endpoints, thereby reducing the attack surface. Another recommendation is to mandate use of a virtual private network (VPN) for all communications - both within the supply chain and externally. VPNs turn a public network into a private network by establishing a secure point-to-point "tunnel" through the cloud. VPNs encrypt the data, filter internet and data traffic and deny unsolicited data requests.

To take advantage of VPN technology, it's important to ensure the following key points:

1. Insist that supply chain members use a VPN for all communications and to lock down all IP-enabled devices.
2. Ensure that the selected VPN solution may be securely deployed in a public cloud, a private cloud and on-premises.
3. Select a VPN with robust encryption, preferably one that is CSfC (Commercial Solutions for Classified) certified. This means that the VPN is certified for the transmission of classified data.

Moving data up and down the supply chain comes with risks and these risks are amplified when parts of the supply chain reside in the cloud. By selecting and mandating the use of an enterprise-grade IT security solution throughout the supply chain, members can enjoy the benefits of the cloud - flexibility, scalability, efficiency and reduced IT costs - without the associated increased cyber risks.

About Attila Security

Attila is a cybersecurity company focused on providing services that identify, control and defend against cyber threats across physical, virtual and cloud technologies. Attila has been named among the Cybersecurity 500 index of industry leaders, and has been recognized as an industry leader for its revolutionary and innovative technological advancements in completely portable, government grade, IP security as well as their suite of cloud and virtual servers. For more information, visit **www.attilasec.com** or call 410.849.9472.

attila SECURITY

attilasec.com