POINT OF VIEW

Why Digital Acceleration Needs a Secure Cloud Network

Executive Summary

Organizations large and small have adopted digital transformation initiatives to enable them to deliver business growth and meet organizational objectives. In the last couple of years, however, organizations have accelerated their digital investments in order to address challenges caused by the global pandemic. IT teams were forced to move many applications to the cloud faster than originally planned. These rapid changes increased cybersecurity risks, imposing a heavy burden on infrastructure teams, including networking and security operations.

On the other hand, digital acceleration has provided CIOs and CISOs a great opportunity to utilize virtualization and cloud to drive better scale and performance for business-critical applications by leveraging hybrid-cloud and multi-cloud environments. By combining the scale and availability of cloud provider platforms with existing investments in virtual data centers, organizations plan to overcome challenges and achieve better business results.

Organizations are continuing to invest heavily in cloud Infrastructure-as-a-Service. $82B cloud system infrastructure services spend in 2021, projected to grow by 30% to $107B in 2022.[1]

With moving to public clouds and modernizing data centers at the heart of this transformation, care and attention must be given to adopting appropriate network security solutions to secure the organization's digital acceleration objectives without increasing risk and exposure.

Digital Acceleration: The Journey to Cloud Starts With the Cloud Network

Organizations pursuing digital acceleration have various strategies and are at different stages with their cloud adoption and applications journey. In many cases, organizations are lifting and shifting virtualized application workloads from their virtual data centers into the cloud, while some are refactoring applications to integrate with cloud provider services, and a few are actually architecting applications to be cloud native. Regardless of where they are in their journey, all of them have major concerns about their applications and data security.

For most organizations, securing this application journey to the cloud begins with securing the network that connects their users, branches, and data centers to the cloud. As a next step, they focus on securing the cloud network that connects to cloud provider services and workloads in the public cloud and hybrid cloud. Organizations at an advanced level of cloud maturity then move on to securing the networks that connect their application infrastructure in a multi-cloud deployment. Getting the cloud network ready for deploying applications causes plenty of challenges, including setting up a robust cloud perimeter for every network setup by various types of users, implementing advanced security for compliance, and streamlining their network and security operations without being run over by runaway cloud costs.

Cloud Network Security Challenges and Trends

Because cloud transformation plans and application journeys vary across organizations, network security challenges differ depending on the maturity of the cloud deployment. There are, however, some fundamental challenges that are the same across organizations. Here are some key challenges faced by organizations deploying applications into public and private clouds:

- **Internet-based inbound threats**

  Inbound traffic can come into a cloud network over the internet from external users, such as customers, partners, and suppliers. Remote workers are also another source of this inbound traffic. A variety of threat actors utilize effective techniques to exploit known vulnerabilities to infiltrate the cloud network and launch attacks or drop payloads with malware or ransomware that may impact organizations negatively and even damage their brand and reputation.

- **Uncontrolled outbound communications**

  This type of communication from a cloud deployment happens when outbound web traffic attempts to connect to low-reputation sources (based on the domain or hostname). These connections could be established by malicious spyware or malware trying to exfiltrate sensitive data or connect to an external command-and-control server. On the other hand, the traffic could originate from developer workloads contacting developer tools like GitHub, or it could be application workloads contacting outside servers for software updates.

- **Lateral movement of threats**

  In the cloud and virtualized data centers, there is typically no control or protection put in place to inspect the traffic flowing between different virtual networks or between workloads in the same virtual network. This leaves room for malicious internal actors to introduce threats that can quickly propagate through the virtual data center or in the cloud. Another important threat vector to consider is the software supply chain and open-source software, which may have been compromised. Developers inadvertently use these resources, thereby introducing external threats that can also propagate laterally and launch catastrophic attacks.

- **Limited bandwidth for secure connectivity into the cloud**

  As organizations accelerate their use of cloud services, they onboard traffic at many locations, including HQ, on-premises data centers, branches, and remote locations. In many of these cases, they may use virtual private network (VPN) technology to connect to the cloud. Organizations have an option to use cloud-provider VPN gateways. Still, most of these gateways do not offer the bandwidth performance needed to deliver the best application experiences to users across different locations.

- **Fragmented management and policy infrastructure**

  When organizations start using more than one cloud provider, and may even continue to use their virtual data center or private cloud, then their operations teams are burdened with many new environments. They have to manage different consoles and set up different policies across these diverse platforms. This leads to a higher cost of training and may leave security gaps among the various environments.

An Effective Roadmap To Protect the Cloud Network

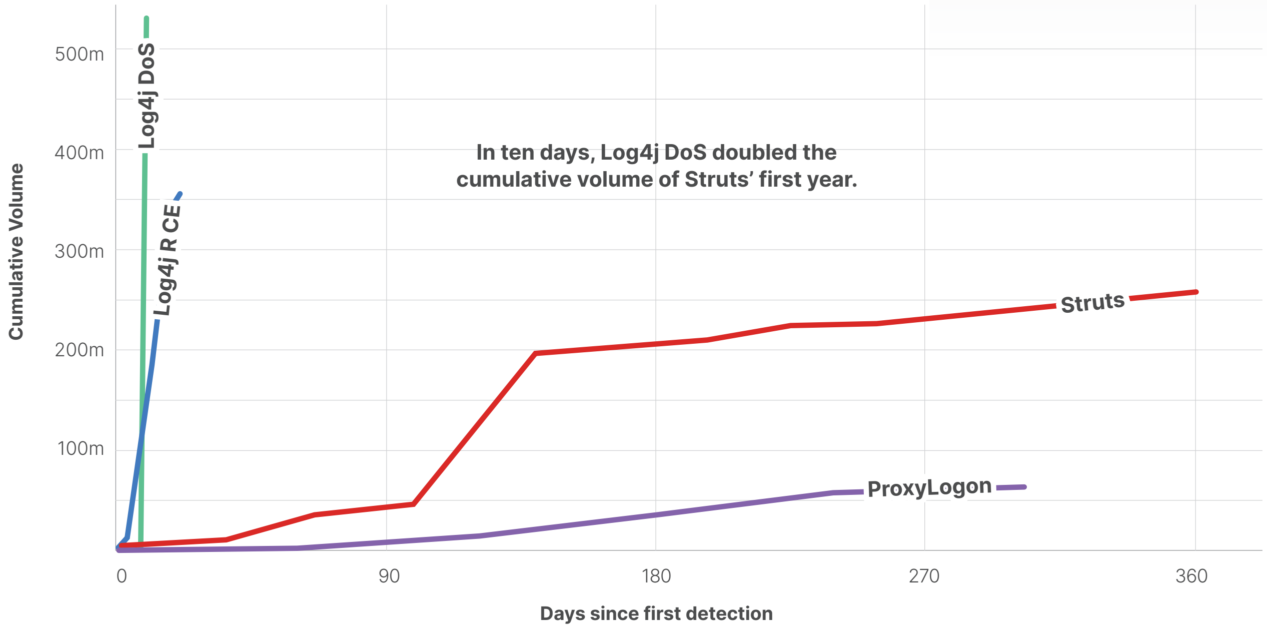
The application journey for any organization essentially lays out the evolution of their cloud transformation, which in turn drives the roadmap for rolling out their cloud network security.

It starts with the lift-and-shift phase of the application journey, which is essentially the organization's cloud migration phase. In this phase, they are **focused on providing secure connectivity** from various locations to the application workloads in the cloud.

Once the organization gets accustomed to cloud usage, they evolve to refactor and rearchitect a select set of applications or even create cloud-born applications. In this cloud expansion phase, they may expand their footprint to tens or hundreds of cloud networks. At this stage, organizations are primarily deploying robust and high-scale routing to interconnect the organization's virtual networks on any cloud provider. But they will also need to **implement a strong security perimeter** to protect the cloud networks from external and internal threats.

Next, they build and deploy cloud-native architectures or run complex IT infrastructures spanning multiple clouds. Organizations in this cloud-native or multi-cloud phase are typically implementing efficient networks to get users from tens or hundreds of locations to access their workloads in multiple clouds, and may even be connecting up application infrastructures across cloud providers by routing the traffic at their data centers or by leveraging cloud-provider or service-provider managed network services. In any case, they will need to secure the network connecting to these multiple clouds and also **secure the networks connecting across the clouds.**

Log4j Demonstrates Dramatic Speed of Exploit Organizations Face: Log4j had nearly 50x the activity volume in comparison to the well-known outbreak ProxyLogon that happened earlier in 2021. Organizations need AI- and ML-powered intrusion prevention systems (IPS), aggressive patch management strategies, and the threat intelligence visibility to reduce overall risk.



Conclusion

The answer to safely moving to the cloud for digital acceleration is reducing complexity and increasing security effectiveness with a cybersecurity mesh platform approach. A cybersecurity mesh platform benefits organizations with centralized visibility and management and automation across all solution points, allowing them to leverage intelligence sharing for faster response times. Ultimately, this reduces complexities, solves cloud cybersecurity skills and resource gaps, and increases overall security effectiveness. As such, organizations should look for solutions that integrate and support a broad, integrated, and automated cybersecurity mesh platform.

[1]. "Forecast for Worldwide Public Cloud End-User Spending," Gartner, April 21, 2021.

March 24, 2022 3:43 PM
1495202-0-0-EN