Cloud Security: A Necessary Component in Digital Transition Planning

Published May 7, 2021

Team8
Global venture group

Cloud Security

Buoyed by tailwinds from the pandemic and remote work, cloud adoption is on the rise, and enterprise cloud migrations are expanding from fringe applications and experiments to business-critical initiatives. As such, security capabilities are evolving to allow enterprises to reap the benefits of moving to the cloud while retaining control over their security posture, data protection programs and application integrity.

Drivers

2020 will go down as a pivotal year for cloud adoption as businesses sought to cut costs, retain flexibility and throttle demand due to dislocation caused by the pandemic. In fact, cloud security is the number one investment area for 2021, according to the Team8 2021 CISO Survey, followed by security automation and identity and access management. In retrospect, we expect that 2020 will be remembered not only as the year when **cloud became the default**, but also when the dynamics governing enterprise networks and workload deployments changed forever. In a world where **containers**1 offer the capability to combine hybrid, multi-cloud and on-premise computing and storage strategies, security tools and techniques will need to evolve to reduce **complexity** created by a multitude of new offerings within and beyond the enterprise perimeter. For example, workloads moving between different cloud environments to optimize for speed, scalability, cost and compliance have created a new “shared responsibility” model between the enterprise and its different cloud providers. If not managed properly, this model could open the door for threat actors to identify and leverage misconfigurations as a way to gain access.

Impact

Cloud is becoming so complex it should be perceived as an operating system. Many of today’s security solutions are just modern-day equivalents of endpoint security and other on-premise techniques that had limited effectiveness. Attacks are not only still happening, they are being amplified by the pervasiveness, speed and connectedness of the cloud. Instead of applying legacy solutions to the cloud, organizations need security solutions that are architected for the cloud, combining control and integrity with scalability and agility.

Solutions

Cloud workload protection platform (CWPP), cloud security posture management (CSPM), container security, cloud infrastructure entitlement management, cloud access security broker (CASB), extended detection and response (XDR).

Perspectives:

- **Defender's Perspective** – The next big thing with regard to cloud security is automated remediation. Most cloud vulnerabilities can be automatically fixed rather than fixing them one by one, by hand. When you describe things with code, they can be easily applied to multiple instances. This characteristic offers an opportunity to automatically remediate these vulnerabilities as opposed to waiting for DevOps to do it." – Jonathan Jaffe, CISO, Lemonade
- **Team8's Attacker Perspective** – The complexity of an environment usually plays into the hands of the attacker, and it would be hard to find infrastructure more complex than the modern cloud. It is a mesh of services, identities, logs, networking, compute and storage. For attackers, it's the Wild West.

When moving to the cloud, many enterprises lose the visibility, understanding and control they had when their infrastructure was on-premise. This is a new playground for attackers, especially since they have plenty of opportunities for target practice on cloud networks.

In our next blog post, we will cover the Security of Things. The full series can be accessed here.

Authors who have contributed to this blog post:

Bob Blakey, Operating Partner at Team8.

1A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

Important Risks Related to this Article

The views expressed in this blog post are those of Team8. Any reference to "we" should be considered the view of Team8 and not necessarily those of WisdomTree Asset Management.

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity and fintech. Leveraging an in-house, multidisciplinary team of company builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to outline big problems, ideate solutions and help accelerate success through technology, market fit and talent acquisition. For further information, visit www.team8.vc.

This material is prepared by WisdomTree and its affiliates and is not intended to be relied upon as a forecast, research or investment advice, and is not a recommendation, offer or solicitation to buy or sell any securities or to adopt any investment strategy. The opinions expressed are as of the date of production and may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources. As such, no warranty of accuracy or reliability is given and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by WisdomTree, nor any affiliate, nor any of their officers, employees or agents. Reliance upon information in this material is at the sole discretion of the reader. ***Past performance is not a reliable indicator of future performance.***