SILVERFORT

Q&A on Identity-Based Zero Trust

Following our webinar series on "Why Identity is a Crucial Component of Zero Trust Security", we sat down with guest speaker Dr. Chase Cunningham, for this one-on-one, exclusive interview.

With Forrester Analyst
Dr. Chase Cunningham

FORRESTER®

1 What, in your opinion, is the role of identity in Zero Trust security?

Identity is the "mechanism" around which the gears of the cyber security machine revolve. Everything in the Zero Trust space in truth is dependent on security and managing identity at scale. Whether that is a machine ID, a human username, or some other form of identity all ZT is contingent on the security of the identity.

2 What would be the benefits of having unified IAM visibility and control for the implementation of Zero Trust security?

It is difficult, if not impossible to manage identity at scale without an automation capability. We have so many forms of authentication and identity for the modern enterprise that not having an ability to control and maintain positive command of those assets introduces risk and will lead to a compromise. A loss of visibility and automation constitutes a critical point of failure in a Zero Trust strategically enabled enterprise.

3 What is the importance of risk analysis and adaptive polices in Zero Trust security?

Policies in the modern enterprise must be fluid and must be dynamic in nature. The days of having a static never changing rule set for enterprise offerings has gone the way of the dinosaur. Risk is introduced by a lack of cognizance and control and by the introduction of unmanaged assets and identities. It is imperative that any organization that is moving towards Zero Trust must embrace dynamic policy controls and malleability to better reduce risk and overall friction of control for both users and administrators.

4 Should service accounts and machine-to-machine access be included in Zero Trust security initiatives? If so, what are the barriers to achieve that today?

Yes, to be frank. Any access request or identity should be part of the risk calculation and should be part of a Zero Trust based approach. Often the issue we see here is that the scale and diversity of the many different items that must be controlled, monitored, and secured is too large to deal with. To solve that issue I suggest organization leverage automated offerings that help to address that issue.

5 What are the challenges of implementing Zero Trust in the cloud, for both cloud-native and migrated assets?

The cloud by its very nature is meant to be a dynamic amorphous virtual infrastructure that is always going to be difficult to solve for. When you add in the growth and sprawl of cloud assets, identities, and resources it becomes even more complex. The only way that any organization can hope to handle that space is by using solutions that empower diverse control capabilities and use the cloud as a potential control plane, not just another housing for data and applications.

Be sure to watch our webinar series on the Place of identity in Zero Trust Security, featuring guest speaker Dr. Chase Cunningham

info@silverfort.com
www.Silverfort.com

US
(+1) 646 893 7857
43 Westland Avenue,
Boston, MA, USA

Israel
(+972) 77 202 4900
30 Haarbaa St, 26th Floor,
Tel Aviv, Israel

Gartner COOL VENDOR 2019