At RSA Conference, look for ‘post-perimeter’ security to dominate

by, James Kobielus

March 5th, 2019

In the multicloud, the edge presents the weakest security link — hence the most promising target for hackers. Locally acquired, processed and stored data exposes edge devices to never-ending security intrusions. Device-based artificial intelligence thrives on that and other data, including content that is fetched from the cloud or ingested dynamically from other edge devices. […]

In the multicloud, the edge presents the weakest security link — hence the most promising target for hackers.

Locally acquired, processed and stored data exposes edge devices to never-ending security intrusions. Device-based artificial intelligence thrives on that and other data, including content that is fetched from the cloud or ingested dynamically from other edge devices. Securing all this data is going to be challenging, especially as AI-powered edge devices roam across private, public, hybrid and multicloud environments of growing complexity.

One of the hottest multicloud security topics is “post-perimeter” security, which also goes by such names as conditional access, zero-trust security, contextual access, device trust and continuous adaptive risk and trust assessment. Interest in post-perimeter security has grown as it has become clear that perimeter security — the foundation of traditional enterprise controls over information technology assets — is becoming less viable in this new environment. As devices roam freely outside on-premises environments and into public clouds, a new approach must move security capabilities closer to where data and applications live.

Essentially, this newer approach moves the software-defined security “perimeter” to wherever the requested content happens to live, be it on-premises, in public clouds or at the edges. Every node at the edge always has access to the relevant identities, credentials, permissions, context variables, code-based policies and other security assets needed to strongly authenticate and authorize access to managed resources while also ensuring confidentiality, tamper-proofing, audit trails and other security controls.

Standards-based support for post-perimeter security is a key element in Wikibon’s recently published hybrid cloud taxonomy, most notably the security, control, compliance and data planes. To support this capability, a multicloud environment needs the following infrastructures:

- **Trust infrastructure as a service**: The term “zero-trust security” is a misnomer. Post-perimeter security requires a trust infrastructure that enables strong multifactor authentication, permissioning, encryption, single sign-on and other security associated with users, devices, apps, data and other entities. Essentially, post-perimeter security depends on robust “trust but constantly verify” capabilities, which vet access requests constantly within a scalable, secure, end-to-end trust environment grounded in public key infrastructure.
- **Identity and permission management as a service**: The term “conditional access” goes to the heart of post-perimeter security. Access to requested resources is always conditioned on relevant identity, credentials, certificates, biometrics and other factors. Under this approach, access is narrowly scoped to specific content, contexts and timeframes in order to mitigate security risks. Essentially, all users are treated as “remote” for the purpose of authenticating and authorizing their access to requested resources.
- **Endpoint, device and mobility management as a service**: Post-perimeter security pushes more security functions to be enforced at endpoints. At the very least, it ensures that users are accessing cloud apps only from managed devices and possibly through secure apps. Post-perimeter security also ensures that enterprise IT can constrain users’ ability to connect their device to unsupported or risky software-as-a-service or cloud service. In this way, the approach gives users the ability to access many resources beyond the enterprise perimeter while also giving corporate IT tight control and monitoring over what they do.

For enterprise IT professionals, post-perimeter security provides the flexibility to change authentication techniques, access privileges and other controls in real time across all managed edge devices no matter where they roam in the multicloud. For example, it provides the ability to let user sessions in low-risk apps go on for a while if nothing looks anomalous, while immediately applying more stringent access and permission policies and possibly notifying security administrators if devices are accessing resources from

unfamiliar locations or engaging in troublesome behavior.

In the run-up to this week’s annual RSA Conference, there was already big industry news relevant to post-perimeter security. Last week, mobile threat defense provider Lookout Inc. announced the Post-Perimeter Security Alliance under which prominent solution providers are collaborating on strong security in a “modern, perimeter-less, cloud-delivered and privacy-focused world.” The group is building a vendor-agnostic framework for seamlessly integrating security and identity across devices, clouds and other IT platforms and tools. Its aim is to help enterprises protect their data all the way to the edge without crimping user mobility and experience.

In addition to Looker, the group’s members include leaders in cloud computing, identity and access management, mobile device management and endpoint protection. Specifically, Google Cloud, VMware Inc., BlackBerry Ltd., Okta Inc. and SentinelOne Inc. have signed on. They will discuss the effort at the Partner Pavilion and at Lookout’s booth at the RSA show, while also demonstrating how their solutions interoperate to support post-perimeter security.

Wikibon also expects these and other vendors to make product announcements at RSA Security that are relevant to post-perimeter security, perhaps leveraging machine learning and AI to power more contextually data-driven edge security decisions.

TheCUBE, SiliconANGLE’s live mobile streaming panel, will be interviewing experts on Wednesday, March 6, at the RSA Conference.

Former Wikibon analyst

James Kobielus

@jameskobielus

james.kobielus@wikibon.org