DARKReading

Autonomous Security Is Essential if the Edge Is to Scale Properly

Service demands at the network edge mean customers need to get cost, performance, and security right.

By Harley Stowell 7/7/2021

No one wants to own and operate technology anymore. Companies want to deliver and operate high-value services at the edge and endpoint. This huge and profitable market for endpoint services is waiting for us at the intersection of hyperscale cloud and hyperscale networks, but on the network side, we need to get cost, performance, and security right at scale.

Secure, dynamic networks with cloud access are the fundamental building blocks of the edge services market. We must recognize that they are going to occur at extreme scale, far more frequently than even cloud or edge compute instances. Connections will come and go all the time, and security will require constant assurance and policy updates.

Secure SD-WAN might be limited to large enterprises today, but it will ultimately connect every small and midsize business office and underpin every Industrial Internet of Things (IIoT) implementation, multiaccess edge computing, and "smart cities" service as well. So we're talking about tens of millions of connections in just a few years, and hundreds of millions before 2030.

The emerging problem in front of us is how to deliver secure dynamic networking at this extreme scale while meeting the economic and security requirements of the various tiers of service. For instance, SD-WAN for large enterprises has a price point that allows for manual life-cycle operations, but secure networking for small and midsize business and the IIoT do not. Security policy operations are manually arbitrated in the enterprise market today, but such manual operations will never work at the future scales we're talking about. Finally, enterprise networks are relatively static, but the fully connected, smart-everything world ahead of us will feature highly dynamic, zero-trust networks at extreme scale. The upshot: For secure networking to function at the scale and price we need, it must become autonomous.

When you unpack the nature of cloud-delivered secure endpoint services, you immediately discover the common limiting factor for cost, security, scale, and reliability: people. Right now, secure network operations are manually arbitrated. For example, deployment of a single secure SD-WAN endpoint takes five to nine worker-hours. Certainly, automation exists, but it is siloed by technology domain and we are relying on people to determine, preserve, and implement service intent across the domains. Because of this, swivel-chair operations are the norm for alignment of security applications, security policy, underlay, overlay, and cloud resources, and they are required every time fulfillment, assurance, healing, optimization, policy updates, or maintenance operations are executed.

This is obviously untenable, and totally inappropriate for the scale of the emerging edge services market. In fact, the industry will struggle to even take the next logical step — secure networking for SMB — without a significant move toward autonomous service operations that can economically provide the required scale, security, reliability required. A failure on this front will simply prevent the edge services economy from taking off.

The first step is always admitting that you have a problem — and we do. And that problem is cross-domain service operations. There are lots of good automation platforms within the various technology domains, but very little that connects them together into end-to-end services. Today that job is being left to people, and that is what we must fix.

To achieve the scale, performance, and security we require, we actually need secure network services that self-operate — like robots in an Amazon warehouse. Each service has its own goals and service level agreement, but is aware of the other services, sharing common resources, operating under policy-based control and organized in an intelligent, prioritized hierarchy.

This sort of service-first approach to autonomous operations embodies five key characteristics:

- Durable expression of service identity
- Top-down implementation of identity across abstracted technology domains
- Closed-loop continuous operations
- Distributed management and distributed control
- Cost and scale engineering

This is the way forward. Autonomous service operations will give us the cost and scale we need, and the speed required to keep our networks secure. We've gone as far as we can building from the bottom up. Technology improvements within domains are useful, but they can't solve the cross-domain operations challenge. It's time for us to work top-down — starting with intelligent services and building toward the resources.

It's a big change, but service-first autonomous operations is the only way to unlock the edge services future and to keep it well secured.