User-based Zero Trust Microsegmentation

Increasingly, today's enterprise networks must be configured to accommodate a new paradigm in business, that of remote work. Formerly, user access to network resources was defined by the brick-and-mortar location, the subnet, the building, the floor, or other physical location attributes. Security was largely based on perimeter defense strategies, such as firewalls and anti-virus, and users and assets inside the perimeter were assumed to be trusted. The few numbers of remote users were granted access through virtual private networks (VPN), but after securely tunneling into the enterprise network they too were assumed to be trusted.

In the zero-trust security approach, assets and users are not trusted by default based on their location, e.g., inside the enterprise network or intranet. All access is granted on a "least privilege needed" basis. Servers and applications are grouped into granular logical groups called microsegments with polices that restrict access to them from users and from other microsegments. These policies, while allowing valid traffic to pass, prevent the propagation of malware or ransomware that has slipped through the perimeter firewall defenses. This has important security benefits for protecting enterprise networks, such as reducing the blast radius of any ransomware or malware attack that penetrated the perimeter and minimizing the attack surface available to the adversary. That is why zero trust as defined in NIST special publication 800-207 is becoming a well-accepted best practice.

Zero trust security also fits in very well with the new "work anywhere" enterprise landscape. All users can be considered remote, even if they happen to be sitting in the office at a particular time. Access permissions are associated with the person, wherever they are working, not to the building, floor, or subnet. This "all users are remote" approach is appealing for both technical and business reasons: simplicity of a unified deployment and cost savings on the former "brick and mortar" type network infrastructure. But there are factors that must be considered before an enterprise would make this fundamental change.

There must be a high level of assurance that there would be no loss of connectivity or business disruption in the new zero trust network access and user-based microsegmentation system. The new paradigm will not be acceptable if service calls are increased inordinately.

Since all users are to be considered remote, the scalability of the solution must support secure access

and microsegmentation policy for a significant number of concurrent users. Traditional VPN servers would not be an optimal strategy to support secure access at this "work anywhere" kind of scale. The elasticity and scalability needed for this type of landscape makes Software-as-a-Service a natural technical fit, since it obviates the need for hardware capacity planning and OS configuration.

The ideal solution would use a unified platform to secure workloads and give users appropriate access. It would allow an incremental deployment of user-based microsegmentation, minimizing implementation risk. It would allow traffic policies to be authored in natural language, and then delivered to different policy enforcement points in the specific rules format needed for a diverse topology that may include data center servers, cloud workloads, virtual machines, containerized microservices, and operational technology/internet-of-things devices. It would make changes automatically when user-context changes, such as, changes in business responsibilities, e.g., which project am I working on now, or which client am I servicing? It could also change permissions based on the health of the access device, i.e., is it free from known threats, is its operating system patched and up to date?

User-based microsegmentation can bring significant security benefits in protecting against modern cyber threats and simplify the delivery of business application capabilities to a "work anywhere" or hybrid workforce.

Simplifying Your Journey to Zero-Trust Architecture

ColorTokens is a leader in delivering innovative and award-winning zero-trust cyber security technology solutions such as network micro-segmentation, endpoint hardening and whitelisting, cloud and container security, and zero-trust network access. ColorTokens is a US corporation headquartered in Silicon Valley, and has approximately 400 employees world-wide, with offices in the United States, the United Kingdom, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please visit **colortokens.com.**