A Unified Zero Trust Platform Integrated with the Enterprise Security Ecosystem

Zero trust security as defined by NIST special publication 800-207 and the CISA Zero Trust Maturity Model has become a recognized a best practice by both industry analysts and enterprise risk and security practitioners, because it reduces the blast radius of ransomware and malware attacks, and it reduces the attack surface available to the adversary.

Two key areas which are identified as crucial domains on which to exert zero trust best practices are network microsegmentation and secure user access. In zero trust microsegmentation, endpoints, 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. Zero trust network access (ZTNA) supports encrypted IPsec tunnelling for remote users and asserts user access policies to microsegments. By their nature, a platform approach which unifies the management and execution of these two areas, network microsegmentation and secure user access, is a natural fit. A unified zero trust platform approach allows centralized administration of these two core zero trust security practices.

Centralized management of these two domains in a unified platform is crucial. Otherwise, if separate point solutions are used, an onerous burden would be placed on those responsible for executing zero trust security; they would need to manually maintain coherence between polices separately enforced for microsegment communications inside the enterprise environment, vs. microsegment access policies for remote users. A unified platform allows for a holistic approach to zero trust policy definition and enforcement, so that no inadvertent vulnerabilities are allowed.

However, such a unified zero trust platform must also coexist with the enterprise ecosystem. It must support integration with other best-of-breed tools present in the security landscape, such as identity management and single sign-on.

Open application programming interfaces (API) must allow seamless integration of those third-party tools with the zero trust platform's microsegmentation and zero trust network access (ZTNA) functions.

To support a holistic approach to zero trust security, these APIs should include the following functionality to integrate with the organization's security ecosystem:

- Integration to receive user attributes from the identity management system (IdM and IAM) to control access to the microsegments. These may be on-premise systems or cloud deployed identity management such as Azure Active Directory.

- Integration to receive data from the inventory of network assets in the configuration management database (CMDB) system. Conversely, if the CMDB is inaccurate or out-of-date, the network assets reported by the zero trust platform's microsegmentation system agents could be used to rectify the CMDB.
- Integration to send data to the security event and incident management (SEIM) system. The microsegmentation platform can identify traffic which is out-of-policy, which can be alerted to the SEIM system.
- Integration to receive quarantine alerts from the security orchestration, automation, and response (SOAR) system, so that the microsegmentation platform can be used to enforce the quarantine as part of the response to a compromise. Using the unified zero trust platform, network assets have been tagged, microsegments have been defined, and communications polices have been established. The microsegmentation enforcement points controlled by the ZT platform can enforce quarantine alerts from the SOAR system.
- APIs should be well documented and based on common standards (such as ReST) so organizations' IT teams will have the skill sets needed to maintain the integration of the solution. The ZT platform vendor can also support the organization with consultancy engagements to initially configure integrations, with a knowledge transfer focus to enable the internal IT team going forward.

Leaders should ensure that the zero trust technology they employ will provide a unified yet extensible platform to deliver a secure and manageable zero trust solution. Access control to network microsegments from both on-campus assets and remote users should be administered in a unified platform. This platform should integrate seamlessly with the total enterprise security ecosystem of their organization, using open-standards-based APIs. Integration capabilities of the zero trust solution should be evaluated using the criteria of completeness, ease of initial integration, and ease of maintenance of the integration.

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.**