COLORTOKENS

SOLUTION BRIEF

Seamless Integration of Threat Intelligence and Vulnerability Data Improves Zero Trust Microsegmentation

As networks continue to grow in complexity and scale, organizations face an increasing number of challenges when it comes to securing their assets and data. By providing organizations with an effective means of isolating potential threats, reducing the attack surface, and disrupting the propagation of malware and ransomware, zero trust microsegmentation has emerged as an essential control in modern enterprise network security strategy.

While visibility of intercommunication flows in the IT infrastructure achieved by a robust zero trust microsegmentation platform is critical to understanding the current security posture, an additional aspect of this visibility is in understanding the threats and vulnerabilities associated with the environment.

Cyber threat intelligence and vulnerability data provide key additional and complementary insights when seamlessly integrated into a unified zero trust microsegmentation platform that has robust visibility, discovery, and tagging of critical systems, and can provide the earliest warning signals of potentially threatening attacks and help strengthen the environment's posture for defending against them.

“Headlights” Into the Threat Darkness

Threat intelligence information provides the “headlights” into the threat landscape, keeping the user and environment aware of what is out there, and what kinds of systems and environments are susceptible to certain attack types. Analyzing the flow of data for anomalous behaviors and notifying the security operations center when suspicious activity is detected is absolutely necessary in taking actions to address the real-time threats to the organization. This can be achieved most effectively when the microsegmentation platform not only links to or accepts third-party threat intelligence data, but in fact seamlessly integrates that data into the platform, and not bolted in as an add-on or separately licensed solution set.

For example, as a key element integrated into the microsegmentation platform, threat intelligence can detail potential risky connections to and from bad or low reputation or blacklisted IP addresses or locations. Additionally, integrated threat intelligence information shows potential risky connections coming into or going out of the datacenter, or exfiltration.

By understanding these risks directly from the platform and through the console controlling the potential exposure and micro-segmenting accordingly, the organization can increase the security resilience of its application infrastructure and speed the time to resolve from advanced security attacks. This integrated view of threats with defining zero trust security policies, inherent in a micro-segmented infrastructure, elevates microsegmentation to a new level.

Integrated Vulnerability Data Enhances Security Visibility

Like threat intelligence information, vulnerability data – when provided by feeds from third parties and seamlessly integrated into the microsegmentation platform, acts as a compensating control and adds a robust layer of protection, bolstering the security posture that microsegmentation already delivers. Vulnerability data gives an indication of security weaknesses at the operating system level, and provides visibility into which systems are unpatched, configured incorrectly or represent other potential exploitable hazards to the rest of the network. When combined seamlessly with microsegmentation, this combination can provide a clear indication of how hardened the OS is for defending against malicious inter-server communication or unauthorized lateral movement, typically invoked by ransomware attempts.

Vulnerability-enhanced microsegmentation allows for the mapping of known OS vulnerabilities to unlocked TCP ports on the assets and provides an understanding if these ports are being used to connect to other systems within the datacenter. By scanning the OS for known vulnerabilities, and mapping this to open listening ports of exposure, greater visibility of the attack surface to be reduced is achieved.

For example, a vulnerability is discovered on a particular machine, but a critical application needs to use the port that is related to that vulnerability. Just blocking it isn't enough. What vulnerability-enhanced microsegmentation does as a compensating control is limit the number of machines that are allowed to access that port with the known vulnerability behind it. That machine might be on a network with several hundred other machines, but perhaps only two machines out of those hundreds generally need to communicate with that server on that port. As a result, the zero trust microsegmentation solution reduces the attack surface from several hundred machines down to two.

> Threat intelligence information provides the "headlights" into the threat landscape, keeping the user and environment aware of what is out there...

Conclusion

In conclusion, the importance of seamlessly integrating threat intelligence information and vulnerability data in microsegmentation cannot be overstated. This type of integration offers organizations enhanced visibility into their IT infrastructure and allows them to quickly identify potential threats and vulnerabilities, as well as reduce their attack surface by limiting access to only authorized machines. By using this combination of technologies, organizations can significantly improve their security resilience and help protect against malicious cyber-attacks.

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**