Minimizing the Security Tools Attack Surface

By: cuculan

We believe most network professionals will agree that the smaller the attack surface the less opportunity for hackers to invade your network.

In Gartner's Top Security and Risk Management Trends for 2022 they note: "Enterprise attack surfaces are expanding. Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organizations' exposed surfaces outside of a set of controllable assets. Organizations must look beyond traditional approaches to security monitoring, detection, and response to manage a wider set of security exposures."

Today, network managers focus on strategies such as segmentation/micro-segmentation as a fundamental approach to protecting the ultimate target of the hacker i.e.: the critical data resources. Various solutions are utilized in pursuit of this goal such as VLANs, subnetting, or user trust zones with various degrees of success.

However, we believe that, in addition to focusing on the data, attack surfaces of the security tools that are employed to implement these protections also need to be minimized. The number of attack vectors of these tools needs to be the minimum required without compromising on tool effectiveness.

Today's tools come in various configurations:

- Software based security tools that are exposed to the insecurities of the operating systems they reside on
- Tools that require agents installed on the protected resources
- Tools that reach out to third party cloud-based services for configuration or authorization

- Tools that only monitor and report anomalies

The more attack vectors in the security management tools the more network management complexity and the greater the exposure to a successful cyber-attack. Can you be truly confident that your third-party service provider or security agents are themselves fully secured?

We would submit that there is a need for a security solution with the fewest possible attack vectors. The solution needs to eliminate the requirement for external authentication services or the need to install potentially insecure agents on critical systems or API's that are themselves potentially insecure. All capabilities should be fully contained and managed within a single security hardware solution including:

- Encapsulation, encryption, and communication using industry standard cryptography
- Authentication of source and destination
- Micro-segmentation
- Automated Key management
- Packet replay protection
- Failover

In other words. The security solution attack surface of the security solution is limited to the least number of attack vectors without the exposure to third party external network connectivity or invasive agents.

cuculan offers a solution that meets the above requirements for your consideration.