Applying AGILE concepts to a Zero Trust Microsegmentation Implementation

As IT architectures continue to evolve and cloud infrastructure and containers take up ever more substantial roles, the traditional perimeter security model is insufficient. Organizations must now focus on ensuring only authorized east-west traffic are permitted while detecting and preventing propagation of malwares across multiple data center systems and cloud assets. Zero trust microsegmentation allows organizations to protect against malicious lateral movement between systems even as they embrace dynamic cloud environments and container technology.

A successful zero trust microsegmentation project must consider several factors for success, for example:

- IT environments are more complex than ever, comprised of multiple technologies, applications, and systems, and have several stakeholder groups.
- Interconnectivity between systems is not well understood, making it difficult to craft least-privilege policies that are appropriate for the individual systems.
- Moving from a default/allow posture to a stricter one of default/deny carries with it risk, and the consequences if done incorrectly can disrupt business processes.
- Gaining alignment between numerous IT/IS managers and administrators with potentially competing organizational priorities creates a time-consuming challenge because each team requires reconfiguring multiple pieces of hardware like routers, firewalls, and NACs.
- Effective project management is essential as it includes gathering requirements, creating schedules and execution plans, as well as establishing outage windows, and countless other tasks.

Addressing these challenges using traditional network-based segmentation techniques and classical “waterfall” project management approaches has proven to be lengthy and expensive, often with little to show after significant effort.

AGILE Enables Collaborative Process for Implementing Microsegmentation

Implementation of microsegmentation begins with visualization of the users, servers, VMs, containers and external internet connections in the enterprise landscape. Then the assets are assigned tags which are used to define appropriate microsegments and to create traffic policies that allow the normal business processes of the enterprise while prohibiting unauthorized lateral movement of data or malicious programs. This requires a collaborative process between the IT security team that is charged with delivering the zero trust microsegmentation project, and the application team which has the domain knowledge needed for creation of the right microsegments and the appropriate traffic policies. This collaborative effort is where the AGILE methodology can be brought to bear.

> The ability to independently segment individual environments, systems, applications, users, etc. enables the project to be managed using iterative sprints.

By leveraging the asset & traffic visualization user interface, the teams can work together to create policies and then test them iteratively using observe/enforce modes to ensure that the enterprise business processes are supported while enforcing the least-privilege-needed discipline to protect critical systems and data. The ability to independently segment individual environments, systems, applications, users, etc. enables the project to be managed using iterative sprints.

Select a Solution With an AGILE-based Implementation approach

- A SaaS-based, cloud-delivered solution that can be deployed in less than one traditional 2-week sprint and requires no ongoing maintenance or support.
- Includes a real-time visual map of users, applications and networks that delivers actionable information about the environment and aids in policy design and verification.
- Allows for flexible, unlimited tagging for the reconfiguration of microsegments as necessary. For example, the first sprint may segment a sensitive production environment from the rest of the infrastructure, then in subsequent sprints, this segment may be decomposed into even smaller microsegments representing individual applications.
- Uses host-based software firewalls as policy enforcement points rather than hardware firewalls allowing more flexibility to iteratively implement and test enforcement.
- Incorporates a policy engine and definition capabilities that allow for a "guardrail" approach to the creation and deployment of policies, with full access between microsegments initially, then narrowing the guardrails over multiple sprints as confidence increases by monitoring traffic flows and observing user and system behaviors.

Finally, select a solution that supports a broad range of systems, from legacy Windows systems in a local facility, to microservices running in a cloud-based Kubernetes environment.

Conclusion

Traditional approaches to implementing network-based segmentation can be costly, time consuming and resource intensive. By leveraging a unified zero trust platform and an iterative, collaborative, AGILE methodology, ColorTokens makes it possible to implement zero trust microsegmentation quickly and effectively. This allows organizations to protect critical systems by limiting the lateral movement of malware or ransomware, reducing the 'blast radius' of an attack. Organizations that take advantage of these technologies and methods can speed the time to completion, improve their networked environment, strengthen their security posture, and provide visibility of their entire network while keeping operational costs low.

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically. With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **colortokens.com.**