Guardicore

CISO INSIGHTS

Segmentation and Zero Trust Security: A Primer for CISOs

Zero Trust Security is moving into the mainstream. And segmentation is a foundational component to reduce risk and prevent data breaches.

The perfect storm of digital transformation, agile DevOps and a stark increase in the number of high-profile data breaches has challenged the status quo in IT security and prompted security leaders to explore new strategies to better secure digital assets for organizations of any size. The old premise of keeping the bad guys out and letting the good guys in via bigger walls at the perimeter has proven it is no longer a sustainable strategy for success. The new rule is that internal traffic that used to be trusted can no longer be.

> *Zero Trust mandates that enterprises create microperimeters of control around their sensitive data assets to gain visibility into how they use data across their ecosystem.*
>
> — Forrester, Five Steps To A Zero Trust Network, October 2018

What is Zero Trust Security?

Initially introduced by Forrester in 2010, the concept of Zero Trust security is not new. Zero Trust security proposes a fundamentally different model than what Forrester calls the “moat and castle” strategy that ignores threats and compromised assets inside the castle. It assumes that every user, device, system or connection is already compromised (by default) whether they are inside or outside of the network.

Zero Trust is not a technology, and it is not a product. There are no silver bullets in achieving a Zero Trust security posture. It is a strategic, architectural approach to network security enabled by technology. Simply put, it provides CISOs and other security leaders with a more rigorous security posture for today’s world of escalating risk.

Where Does Segmentation Fit Within Zero Trust Security?

A Zero Trust architecture abolishes the idea of a trusted network inside a defined corporate perimeter. At the core of Zero Trust is the application of “microperimeters” of control around sensitive data assets. The idea here is to reduce the attack surface and prevent lateral movement. The goal is that when — not if — a breach occurs, an intruder can't easily access other systems or sensitive data by moving laterally. Organizations can reduce the attack surface of critical systems and prevent the exfiltration of sensitive data by applying segmentation or micro-segmentation for fine-grained access control.

Says Forrester in the The Forrester Tech Tide: Zero Trust Threat Prevention, Q3 2018, “security pros use microsegmentation technologies to limit the ability of malicious attackers to move across data centers and cloud deployments” by creating “secure zones in hybrid environments down to the workload level without requiring a hardware appliance.”

A New Approach to Segmentation: Software-Defined Microsegmentation

Most organizations have implemented network segmentation using traditional network security tools such as internal firewalls, VLANs and ACLs. However, with today's dynamic and hybrid data center environments, these traditional approaches are no longer effective as they are slow to adapt to the pace of change, and policy management is increasingly more expensive and complex.

Software-defined segmentation offers a new, more agile approach to isolate and segment networks and applications that is faster and easier to manage than internal firewalls and VLANs. It is more flexible across on premises and hybrid cloud environments and enables more rapid implementation of a Zero Trust Security model to protect your most critical applications and data.

How Does Guardicore Help?

Guardicore provides a single product that enables rapid deployment and easy ongoing management of segmentation and micro-segmentation policies in any environment. This enables your team to move more rapidly to a Zero Trust security posture, while also reducing the cost and complexity of ongoing policy management. It also gives your team the ability to consistently enforce segmentation policy across any environment, whether your critical applications and workload are running on legacy systems, bare metal, hypervisors, or public cloud/IaaS.

Guardicore maps to these critical 5 steps for implementing Zero Trust security for data center networks:

Critical Capability*	How Guardicore Helps
Identify Sensitive Data and Assets	• Granular visibility simplifies the identification and classification of sensitive data and workloads.
Map The Flows Of Your Sensitive Data	• Creates a visual map of all flows to sensitive data, including classification of all assets and application dependencies.
Architect Your Zero Trust Microperimeters	• Intuitive policy wizard enables rapid definition of any type of segmentation or micro-segmentation policy.
Continuously Monitor Your Zero Trust Ecosystem With Security Analytics	• Real-time monitoring and analysis of security incidents, with SIEM integration, quickly identifies malicious activity.
Embrace Security Automation And Orchestration	• Open REST APIs and existing integrations with orchestrations simplify automation in any complex environment.

* From Forrester, Five Steps To A Zero Trust Network, October 2018

The Bottom Line

A Zero Trust approach to security is moving into the mainstream. If your organization has not yet embraced the Zero Trust security model, or you are in the early stages of implementation, Guardicore is here to help. Our distributed, software-defined approach to segmentation and micro-segmentation can accelerate your move to Zero Trust security, supporting both your current and future state data center and cloud infrastructure.

About Guardicore

Guardicore is a data center and cloud security company that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security — for any application, in any IT environment.

For more information, visit **www.guardicore.com**

Guardicore