Guardicore

Ensure Zero Trust Coverage for Your Legacy Critical Assets with Visibility

Thinking Zero Trust? Think Zero Blind Spots

Protecting Legacy Infrastructure should be an Essential Part of Your Security Strategy

As far as security strategies go, Zero Trust is becoming too big to ignore. According to Chase Cunningham, principal analyst at Forrester, "If I have 20 calls, 17 are about Zero Trust. CISOs, CIOs and CEOs are all interested, and companies of various sizes are interested. And in three years, I think Zero Trust will be cited as one of the big-time frameworks in cyber security. Period."[1]

"..If I have **20 calls,**

17

are about Zero Trust

I think Zero Trust will be cited as one of the big-time frameworks in cyber security. Period."[1]

It's a bold statement, but the IT landscape backs it up. As modern hybrid data centers become the norm, it's harder than ever to ascertain the legitimacy of traffic, not just North-South, in and out of the data center, but East-West, within your own four walls. While historically it was enough to have perimeter security measures in place, today this checkpost approach is worryingly insufficient and some might say that firewalls are no longer relevant inside the cloud.[2] Assets do not stay contained on your network, with examples including auto scaling, containers, mesh and micro services architecture just to start.

All the while, in the background, you do not need to be a genius to launch a successful attack, as attackers are getting access to more sophisticated attack tools, leveraging advanced attack patterns, and using social engineering methods such as phishing scams and user impersonation attempts to get through your front door.[3] At this point, it's just a matter of time, some lateral movement and escalating credential usage until they make it to your most critical assets and sensitive data.

How Can Zero Trust Help?

Out of this reality, the framework of Zero Trust has been evolving since 2010, when John Kindervag proclaimed "no more chewy centers" in regards to network security. It's not enough to harden the outside, without paying attention to how to protect the critical assets within. The simple premise is that enterprises should 'never trust, always verify.' Practically speaking, this means that all access is cut off, unless expressly allowed. Thinking broadly, properly implementing this model encompasses not just users, but also devices, workloads, and data.

Micro-segmentation has become a powerful technology that can help companies adopt this Zero Trust strategy for network security, adding micro-perimeters around critical assets and customer data, and enforcing access with tight policy controls.

1. https://www.linkedin.com/pulse/what-zero-trust-why-security-experts-say-its-best-way-fitzpatrick/
2. https://www.idginsiderpro.com/article/3301354/do-you-still-need-a-firewall.html
3. https://www.calcalistech.com/ctech/articles/0,7340,L-3775934,00.html

Starting with Visibility

In order to implement micro-segmentation, one should have visibility. Without being able to visualize your entire data center (wherever it might be located or implemented), how can you be sure what needs securing, or ensure that you don't create service disruptions or bottlenecks by enforcing access policy? Without the right amount of visibility, enterprises might end up causing more work for their IT teams, rather than automating and streamlining security in a way that suits business strategy and optimizes performance.

The best security technology acts in an early and continuous way throughout, enabling DevOps teams to make quick and Agile decisions with the peace of mind that security will run smoothly in the background. To put this into place, a full view of your whole ecosystem is a foundational first step, a map that automatically includes everything from legacy systems to cloud and container technology. For the map to be truly valuable in creating security policy, it also needs to show a real-time view of all dependencies, providing essential context to your servers, applications and workloads.

A full view of your whole ecosystem is a foundational first step, a map that automatically **includes everything from legacy systems to cloud and container technology.**

This visibility also allows companies to avoid the problems caused by under or over-segmenting your network. Under-segment, and you could leave your critical assets exposed to serious risk. Over-segment, and your policy will be too tight, getting in the way of business as usual or DevOps practices and pipelines. The best approach to achieve segmentation is a phased approach, starting with low-hanging fruit that give quick time to value, and moving on to larger projects such as compliance mandates, and from there to enforcing more granular policies. All the while, with the right technology partner supporting your Zero Trust implementation, you have visibility into the changes to your architecture, and can be alerted to any problems ahead of time, before you step into enforcement mode.

It's important to realize however, that phased does not mean incomplete. Starting your Zero Trust journey with anything less than a holistic view of your entire network is a recipe for inconsistent policy and blind spots. While many micro-segmentation vendors put the emphasis on future-focused technology such as containers and microservices, it's equally important to think about your end-of-life applications and legacy architecture.

The right partner for Zero Trust adoption **will include legacy** not only in your micro-segmentation approach, but **will be able to visualize all legacy infrastructure in your map.**

Include Everything: The Importance Of Protecting Legacy Systems As Part of Your Strategy

It's easy to say, 'well, companies should modernize their old systems' but this is often easier said than done. In fact, for many organizations, the harder a system is to remove, the more likely it is to be business-critical, even if it appears to be dangerously behind the times.

Some industries like Banking, Insurance, Telecom, and Healthcare still and will continue to rely on legacy technologies that were partially modenzied. Even though the percentage of legacy servers and applications is shrinking, there are still many critical applications that are based on older Operating Systems and hardware. While the following examples are not common, one still sees legacy IBM AIX machines that process financial transactions, or Oracle DBs that run on Solaris servers performing a very specific task for a telecommunication company.

Recent research into Federal legacy systems has shown some systems that are over 5 decades old, and pose a high security risk to the Treasury, Education Department, and the Department of Health and Human Services, to name just a few.[4]

When legacy systems are this important, it's short-sighted to leave them out of your Zero Trust strategy, and impossible to launch a holistic micro-segmentation strategy without having a plan for legacy from day one. The right partner for Zero Trust adoption will include legacy not only in your micro-segmentation approach, but will be able to visualize all legacy infrastructure in your map from the start, uncovering legacy systems you might not even have been aware of, and identifying at a glance the connections and traffic you need to be aware of where it's most essential.

Balancing Security Needs of Legacy Systems with a Future-Focused Roadmap

In many cases, these legacy systems can feel like or in reality are a stumbling block that prevents organizations from achieving their business roadmap. In fact, 43% of CIOs say that their legacy infrastructure is holding them back from digital transformation.[5]

43%

of CIOs say that **their legacy infrastructure is holding them back** from digital transformation.

This means that technology that enables a Zero Trust model needs to consider and make space for infrastructure at both ends of the spectrum. It's true that in many cases, it's digital transformation that has created the need for Zero Trust, making today's modern data centers more complex and resulting in less visibility into traffic and communication flows. That means that vendors need to support the most future-focused technologies, and be ready for whatever the next big thing might be.

However, many of these same organizations have legacy needs that cannot simply be missed out or modernized. As these are often responsible for the most business-critical workloads and data, they need to be an early and continuous focus of any segmentation strategy, whether that's environment segmentation, compliance projects, or user-identity access management.

It's not enough to **harden the outside**, without paying attention to **how to protect the critical assets within.**

Legacy Technology Doesn't Need to Keep You in the Past

For enterprises attempting to handle this dichotomy, it can feel like tight security is impossible to grasp, making the move to a Zero Trust model with best practices feel even more daunting. Intelligent micro-segmentation technology is the answer, starting with broad visibility of your whole ecosystem, without ignoring your legacy needs, and moving on to airtight policy creation that moves with the workload seamlessly, regardless of the underlying platform.

Whether legacy modernization is on your roadmap or the last thing on your mind, you need security that covers you right now, in real-time. If Zero Trust is on your to-do list for 2020, get in touch to schedule a demo.

4. https://www.gao.gov/products/GAO-19-471
5. https://www.us.logicalis.com/globalassets/united-states/downloads/cio-reports/2017-cio-survey-report.pdf