Zero Trust: A 5-Point Plan to Modernizing Secure Access

June 10, 2021

Director of Software Supply Chain Security & Emerging Cybersecurity Technologies
Aaron's collaborative leadership and drive for tangible results builds strong client relationships for providing unbiased security and business consulting. He enjoys tackling difficult problems with clients to define our desired outcomes, employing visibility to make informed decisions, and explaining security choices in business language.
Submitted by Aaron Smith on 10, Jun 2021
Zero Trust: A 5-Point Plan to Modernizing Secure Access

Virtual private networks (VPNs) are part of a traditional, outward-looking approach to security that assumes everything behind the firewall is safe. But this isn't good enough anymore.

In today's hybrid workforce environment, large percentages of employees work from home, corporate assets reside in multi-cloud environments, and attackers routinely evade defenses without being detected. All these factors make this model less effective. Organizations require a method that providers a greater security posture. Enter: Zero Trust.

Zero Trust models offer strong user identification and access policies, segmentation of data and resources, strong data security in storage and transfer, and greater security orchestration. While the benefits of Zero Trust are clear, successfully implementing it requires commitment and a clear-cut action plan.

5 steps to building an effective security approach with Zero Trust

1. Identify your sensitive data at rest and in motion

A traditional security program begins with hardware and software asset management. However, the real value resides in its data, so you need to take a data-centric approach.

Start by identifying your sensitive data at rest and in motion. If you don't know where your data is, then you won't be able to effectively manage it, so you'll need to perform data discovery. Scan your environment and network to determine where the data lives. Ultimately, you want this discovery process to become continuous.

To enable continuous discovery, create a digital pipeline by implementing continuous monitoring, continuous response, and continuous management tools.

Once you've identified your data, you need to determine who has access to it. Keep your data classification model simple. For example, customer and client information is classified or restricted, and, therefore, on a need-to-know basis. Public data is fully accessible, and everything in between is available internally.

By implementing a data classification simplification model, it will make everything easier to enforce and manage.

2. Map acceptable routes for sensitive data access and egress

Once you've identified and classified your data, determine where the data flows are. This includes both inputs and outputs.

Map where data is flowing within each workflow, paying close attention to data that's being moved manually and without authorization. Look at data moving automatically and determine if that's how you want it to move (or how it's *supposed* to move).

For instance, data should not flow out of an S3 bucket. You should also not open databases up publicly.

Make sure you understand where data flows, why it flows, and if it should flow in, who has access to it.

3. Architect Zero Trust microperimeters

The driver behind segmentation is to lower your footprint and reduce an attacker's ability to get a foothold on your system. But we can go further than that.

Set up and define microperimeters, zones, and segmentation around your sensitive data. For instance, there's no reason your email service and internet-facing workloads should be in the same zone. Furthermore, there's no reason your workloads shouldn't be segmented.

Enforce this segmentation using physical and virtual security controls. Incorporate service-oriented authorization and single sign-on (SSO) access controls and unify your authentication systems for everything from your workloads, operating system, mobile devices, and more.

Make sure you automate rule and access policy baselines, as well as audit and log all access and change controls.

4. Monitor the Zero Trust environment, in detail, with security analytics

We tend to be hands-off when it comes to monitoring. That's no longer an option.

Identify and leverage existing security analytics solutions within your organization and decide the best and most logical architecture and placement for these tools.

If you need a new solution, first determine your current and future business needs. Then, identify and work with a vendor whose security tools and analytics practices are moving in that same direction.

Zero Trust is not about passively deploying a tech-integrated walkway – it's about active management and continuous metrics. You must be active to implement your trust.

5. Embrace security automation and adaptive response

Zero Trust is possible because of automation. So, you really need to embrace security automation and adaptive response.

Implementing policy-based controls lets you be in the driver's seat because they're continuously assessing who might be trying to access data and if they have permission.

Document, assess, and test security operation center policies and procedures for their effectiveness and response. Compare policies and procedures with security analytics automation to see what can be borrowed from manual processes.

And, finally, make sure you secure the implementation of automation solutions within your environment and current solutions.

Taking a Zero Trust approach

The days of assuming that everything behind your firewall is secure are a thing of the past. You need to be just as vigilant about protecting that data and workflows from *within* your network as well.

A Zero Trust approach gives your organization the security posture it needs to feel protected in this hybrid world. And, by incorporating this five-point plan, you can be sure that your Zero Trust solution will be as effective as possible. x

Stratascale has several solutions and offerings centered around building your Zero Trust environment. Please contact us to learn more.