BUSINESS BRIEF

Zero Trust

Secure your network by managing trust

Plus, best practices for getting started

The Zero Trust Journey

Myth: It's just the latest unrealistic trend

Reality: Zero Trust is not a trend, but arose out of necessity, and will not go away. Highly publicized breaches (e.g., Google and 35+ other technology companies being compromised as part of Operation Aurora) gave rise to the notion that existing security measures are not enough, and a more comprehensive approach to security is required to defend against all forms of threats.

Myth: It's unattainable.

Reality: Many organizations are shying away from Zero Trust because they don't know where to start, or don't think they can achieve it, predominantly because they don't have the resources, or have a pre-existing mixed batch of technologies. Zero Trust, however, is not an end-state. It's a process that involves making changes and upgrades that improve security each time, and incorporating this process is definitely attainable.

Myth: You have to start from scratch.

Reality: It isn't necessary to 'have a starting point'; you can work with your existing processes, investments and infrastructure.

Myth: It must be done all at once.

Reality: In fact, it's smarter to focus on your business-critical functions and data first.

Myth: Zero Trust…isn't it bad to not trust my people?

Reality: Zero Trust doesn't have to do with not trusting your people; it's about reducing the implicit trust extended to anyone (or anything) that has access to resources on your network. To look at it another way, Zero Trust helps to ensure that the right people are accessing the right systems.

Business is built on trust, right? And trust underpins most of our societal norms, our financial system, our day-to-day interactions…and much of our technology.

Times have changed — especially when it comes to securing your network. The 'implicit trust' we extended within our networks is used against us, via attacks that could expose critical data or bring the network down – and they are coming from every angle. In fact, Zero Trust as a strategy came about as a reaction to large scale attacks where the need to combat attacks from both from outside and within your network perimeters, was identified.

So as a network security best practice…you can't *implicitly* trust anyone or anything trying to connect to your network or systems.

Why Zero Trust — and Why Now?

Traditionally, we set up our network and gave any device on the network open access to everything inside of the perimeter walls of the Local Area Network. Telecommuting and remote work has further pushed us to enable LAN access to remote employees. Now that the gig economy has landed, we're granting access to freelancers and contractors who are performing a variety of tasks. Sometimes consultants, partners and investors even get a peek.

To complicate matters even more, various people across departments are granting access to areas of the network as personnel and roles change.

Too many organizations don't know who is accessing what and when — and any device, account or person could be up to no good. It makes perfect sense: People using devices that have access to storage systems and applications constantly interact with critical data, and any one of their devices and accounts can be targeted and used to compromise the organization as a whole.

In addition, if your organization is like most, you have inherited a legacy of IT and security infrastructure and configurations that conflates devices, users, networks, identities, access and permissions to the point that they're described as flat networks, meaning anyone in the enterprise has or can easily gain access to other users' information, data or applications. This is a veritable paradise for threat actors – compromising what may be seemed as an unimportant device or identity in a network often provides ease of privilege escalation and access to the entire network. And many of today's most highly publicized breaches involve these types of acts.

Zero Trust is a strategy for understanding, managing — and most importantly, decreasing — *implicit* trust in your computing environment. It provides a target framework to address complexity introduced by enterprises that are increasingly embracing mobility, cloud and web-facing applications and services.

In the most basic terms, it means you have zero trust for any person, device or identity that's accessing the network, until you take some steps to verify that the person, device and their associated identity belongs there. Once verified, is also means opening the least amount of access necessary to perform a task…and providing continual monitoring and verification that nothing 'has gone off the rails' – in other words, that your security measures (and your security stack as a whole) are functioning as intended. If it isn't the case, the ability to quickly detect, respond and shut down threats is also a central to Zero Trust.

Zero Trust also has a flip side: you are also enabling trust, helping to ensure that the right people — the people who deserve your trust and have validated themselves — have the right access to the right resources at the right time, while keeping your most critical assets safe.

Zero Trust Is a Journey, Not a Destination

First things first, a magic bullet doesn't exist. You won't find a single solution that will get you to Zero Trust. Instead, think of Zero Trust as a journey, always changing and requiring consistent monitoring. It is an ongoing process, but you're going to be markedly more secure with each step.

You just have to start.

As you plan, and begin to embark on your Zero Trust journey, follow these best practices.

#1. Define Strategies to Monitor and Secure Your Environment
Taking a security stance is also about ensuring that your stance has not been compromised. That involves a well-implemented security process, with threat detection and response as its centerpiece. Adopting a data-centric security model is important, to ensure you have the information you need to quickly identify problems and resolve them quickly. But the focus can't be just on external threats. You need to be monitoring north-south as well as east-west traffic.

Beyond that, you can't fix it and forget it. You also need to *continuously monitor your solutions* and security measures to ensure that they are working as intended and to pinpoint weaknesses.

#2. Understand Where the Highly Critical Data Resides
You must know what data is most important for you to protect and start there.

It requires a shift to data-centric security, where you build layered defenses from the data outwards, with data access controls at the storage layer that enforce strong authentication for the data; for example, allowing only certain users from certain locations to access it.

So, as a first step, take inventory of what is in your environment so that you can create a smaller perimeter — that you can realistically monitor — around your critical data and applications. From there, you can ensure you have deployed the right tools and established the right policies to protect your crown jewels.

The harsh reality is that you can't always protect your entire network, so focus first on what matters most first.

#3. Know Where Implicit Trust Exists
Before you take another step, know exactly where you have granted open access to employees, contractors and third parties. Implicit trust exists typically in one or more of these areas, so it's a good place to start your evaluation:

- VPN connectivity
- LAN/network core
- Specific network segments (or lack thereof)
- Authentication and directory services (active directory)
- Service accounts
- Single-factor authentication

This step is critical because once you know which areas are most vulnerable, you can prioritize your efforts.

#4. Establish Who and What Should Have Access to the Network
Employees are hired, fired, promoted, moved off-site — roles continuously change, as does access to various parts of the network. It is critical to know what every stakeholder's role is and what access each role requires at any point in time.

You need to understand and manage these roles, and you need to revisit them on a regular basis to ensure you are removing and updating permissions as needed. The process requires consistent upkeep because roles change from year to year and even month to month.

That isn't possible without a holistic view of your network, gained only through pervasive visibility not just into the network, but into the people using the resources, devices and network.

#5. Adopt a Zero Trust Strategy
The Zero Trust strategy — that you must verify everyone and everything trying to access your network — must be at the core of your IT strategy. That means looking at existing and new solutions through a 'Zero Trust lens' and prioritizing purchases and changes based on those goals.

Going forward, evaluate each product not just by the direct problem it solves, but how it supports your Zero Trust efforts.

#6. Start Small — and Tackle One Thing at a Time
Guess what. You can back into the process. You don't need to scrap everything and start over. In fact, it's highly likely that you already have most of the technologies needed to secure your network. Once you know where the crown jewels reside, you can segment your network and focus on those critical areas first.

It makes the overall process less overwhelming — and more doable.

The key however is to continue to look at your overall security posture through that Zero Trust POV. You need to assess how all your tools work together — and that requires intelligence behind each security tool.

#7. Gain More Visibility into Encrypted Traffic
More and more traffic is encrypted, which is traffic you can't see. If you can't see it, you have no way of knowing if threats are lurking within it. You simply cannot secure what you cannot see, and you cannot analyze what's hidden.

You need the ability to inspect and facilitate analysis on the massive amount of encrypted traffic traversing your network, while conforming to any regulations you must adhere to. The challenge is that most organizations struggle to keep up with decryption – they often have no plan on how to tackle it.

Adopting a centralized approach to decryption allows you to offload decryption to prevent straining network tools and test new upgrades on the fly without disrupting operations.

It's Time to Start Your Zero Trust Journey

As both the number and sophistication of attacks increase, so does the pressure to protect your network — but you can't fight with blinders on. Network visibility is essential to your success.

Contact Gigamon today to learn how we can help you take the first step in your Zero Trust journey. Or better yet, let us show you ways to get started: request a demo today.

Bassam Khan
VP of Product and Technical Marketing, Gigamon

Bassam Khan serves as Gigamon Vice President of Product and Technical Marketing Engineering, responsible for positioning and promoting the company's products and solutions, as well as corporate and go-to-market strategy. Bassam brings a strong track record of more than 20 years managing products and marketing for security, cloud and collaboration technology companies. Prior to Gigamon, he held executive positions at ControlUp, AppSense, PostPath (acquired by Cisco), Cloudmark and Portal Software. Bassam holds degrees from Carnegie-Mellon University and Boston University.