Cyolo

A CISOs Guide to Meeting Critical Business Demands While Securing the Organization

Chapter 1 - Challenges with the current threat landscape

The COVID pandemic has significantly boosted an increase in remote working, especially from home networks. The perimeter has collapsed. In addition to needing to secure the office and hybrid networks, CISOs must work within tighter budgets, and meet the demands of all the different stakeholders within the organization.

As a result of these ever-evolving challenges, the Zero Trust (ZT) model is being widely pursued as a solution to the challenges at hand.

NIST defines ZT as an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

The business alignment and investment optimization of the ZT model is precisely what we're going to explore in this paper. In the following three chapters we will define what ZT is, how it can benefit key departments in your organization, and where to begin implementing a ZT security model in your company.

Chapter 2 – The impact of security breaches on organizations

Regardless of your job role or department, ZT has real measurable benefits for all. There is an upward trend of data breaches which result in data loss, intellectual property losses, reputation damage, high ransomware payments, customer lawsuits and possible criminal charges against business owners. Unfortunately, the threats are getting more sophisticated and frequent so your business needs to prepare now so you are in a better position to defend against these growing threats.

A proper ZT implementation provides organizations with the intel and tools to do their jobs more effectively. Prior to ZT, visibility was extremely lacking in the entire digital domain.

The benefits of ZT cannot be overstated for every department and person in an organization. At the end of the day, it comes down to managing risk and ZT allows you to manage this risk better than ever before.

In the next chapter we will provide some guidance on how your organization can prepare to defend against current and future threats effectively.

Chapter 3 – The Next Generation of Secure Connectivity

The main tenant of ZT is VISIBILITY, which is very different than the previous model, which presumed that everything behind the firewall is safe. ZT is a shift in mindset where every request is expected to carry a degree of risk and must be VERIFIED explicitly.

There are 4 principles which govern the ZT model:

1

Verify Explicitly
Authenticate and authorize based on all attributes available. This includes user identity, location, device health, workloads, asset controls and so on. In addition, ZT wants to leverage role-based, attribute-based and / or policy-based access controls (R/A/PBAC). A true two factor mechanism must be included in the equation (something you have and know). It is vital that your MFA be provided “out-of-band”. This implies being delivered separately from that of which you are protecting. Skepticism from a technological and human perspective is essential.

2

Least Privileged Access
Only grant the minimum level of access needed to perform the task or action at hand. This can be managed using just-in-time and just-enough-access (JIT / JEA) controls & tools, risk based adaptive policies and data protection to secure your data. Access should also be timed and scheduled where appropriate. These controls should be validated and enforced per request.

3

The Perimeter Has Collapsed
There is a concept in CyberSecurity called “minimizing blast radius”, which is to limit the damage that can occur from a breach. This can be done by limiting the lateral movement of an attacker through network segmentation. In this process you will restrict access by users, devices, apps and more. This is a form of isolation and to move from one segment to another requires verification and validation (policy enforcement). Each “hop” across a segment would meet a “digital gatekeeper” whose job is to validate the ticket so to speak.

4

Continuous Diagnostics
An ounce of detection is worth a pound of prevention. This is accomplished by leveraging various modules that contend with data ingestion such as log and netflow analysis, etc. At all times the attributes are collected and verified based on your policies and business demand.

Chapter 4 - How to Implement ZT Effectively

To implement ZT effectively you will need to assess your current domain's compliance and maturity level. You should aim to have 5 lenses of FCAPS. These stand for fault, configuration, accounting, performance and security. Apply these lenses to each "exposed" layer of the OSI model.

Assessment

You need visibility into all devices in your domain; you must also have an understanding of your risk profile. There are a number of tools on the market which can assist you in this process. Please reach out to us for a consultation and let us help you get started.

Identities

You may have heard this a lot lately... the perimeter has collapsed. Remote or home workers are now likely to be out of the organization's control.

The reason identity is our first component is because every request for access comes from a user or device. It is critical that you verify these requests across your entire digital domain. You do this by implementing a strong authentication policy. This authentication and explicit verification should happen as requests enter a segment. For user authentication it is strongly advised to employ a minimum of a 3-factor challenge.

Devices

You MUST have visibility into every device that is connected to your digital domain. Again, this comes back to the paradigm of "you can't defend your organization blindly". You must have the ability to block devices which are not approved to be connected to your domain. Implement alerts that warn you about unexpected devices that get detected. This detection should be real-time and you can leverage tools such as Cyolo.

Applications

Application monitoring and protection has been neglected in the past. ZT gives us new datasets to facilitate root cause, attribution, authentication, etc. ZT ensures appropriate permissions when working inside applications using gate access based on real-time analytics plus monitor and control user actions.

Data

The collapsed perimeter requires us to move to a data-driven protection model. We recommend you implement the following controls for your data:

- Use intelligence to label, classify and categorize data.
- Encrypt and restrict access based on identity and policies
- Data should be encrypted while at rest, in use or in motion
- Access to data should never be open ended. Requests and data access should expire when no longer needed.
- Continuous monitoring for unusual or "out-of -norm" access and behavior

Infrastructure

It is imperative to deploy a framework which gives you telemetry and real-time reporting for attacks, anomalies and governance violations across the organization. These concepts such as an Extended Detection and Response (XDR) or Comprehensive Governance Model (CGM) provides a holistic view of both the control and data-plane. This is accomplished via strong access controls which can ingest, detect and block offenders based on risk evaluation through a trust algorithm.

Network

To stress this again; just because an asset is on your internal network does NOT mean that it is trustworthy. All assets should be considered a potential risk.

Make certain you encrypt all internal communications in transit and in motion. Limit access by policies and use segmentation to restrict lateral movement. Employ real-time threat detection which continuously monitors and scans all devices on the network "hunting" for threats.

In Conclusion

A framework and shift of mindset and security culture only works when it moves from the realm of research and ideas and into real-world application and delivers measurable results. ZT has been evolving and there are many tools and guides which can assist you in transforming your organization.

We hope that this ZT introduction inspires and encourages you to start down the path on becoming a formidable defender against malicious actors.

At Cyolo we have created a number of guides and products which can help you in your journey. If you would like a free consultation please contact us at: info@cyolo.io.

About Cyolo

Cyolo is the leading zero trust security provider for organizations that require fast and secure connectivity. By securely connecting all users from anywhere without requiring a VPN, Cyolo enables employees to focus on their work and your business to grow. Cyolo provides advanced user management features, real-time recording abilities and an easy to use UI. Cyolo can also integrate with your VPNs, if needed.

Cyolo takes minutes to implement and is compatible with any network topology and identity infrastructure. In addition, Cyolo does not have access to the organizational data. Not only does this ensure true privacy and security, it also improves performance as a better user experience.

Request a demo to learn more: info.cyolo.io/demo-request.