C-Suite & Board Members

Cybersecurity Risk: A Board's-Eye View

A Strategic Guide to Protect and Grow Your Business

PORTSYS®

August 1, 2020

In the opening chapter of this eBook, we provided a Board's-eye view of the five critical questions you need to ask in order to fully assess your security posture. This week, our strategic guide looks at the advantages and disadvantages of the three flavors of Zero Trust.

THE 3 FLAVORS OF ZERO TRUST

When you look at the Zero Trust landscape, it's easy to get confused. This leads to several challenges for your IT team – increasing security sprawl, aggravated end users, and corporate resource constraints, to name just a few.

Zero Trust is a popular term and everyone seems to be jumping on the bandwagon. There were more than 90 companies at RSA this year alone boasting of their Zero Trust capabilities – up from 60 in 2019.

There are many benefits to the different solutions, but hopefully what follows will help you sort through some of the hype and confusion in the industry. To fully weigh the benefits and drawbacks of the different approaches, it may be helpful to first group the current Zero Trust solutions into these three buckets:

IDENTITY-FOCUSED

These credentials-based solutions are typically easy to deploy. They are designed to shore up your organization's identities so you can prove who a person is when accessing resources.

Organizations can strengthen identity through Multi-Factor Authentication, biometrics, passwordless authentication, constraints delegation that limits access of a delegation machine or account to specific services while impersonating a user, or other methods.

It's important to remember that identity alone is not security. Identity is just a single factor that can be used to help secure access.

When organizations do add tools to strengthen identity, the process changes often spur much more support needs, such as help desk calls and password resets. And even then, the identity may not apply to all access. For instance, if you haven't focused on reducing the complexity in your environment, you can't always add Multi-Factor Authentication to all your resources.

Why isn't a username and password enough? Around half of all end users use the same passwords for their personal and work accounts, and compromised passwords account for more than 80% of hacking-related breaches.[1]

Credentials-based identity is not security. It is simply identity, and while confirming an identity is helpful, it is not all you need for good security.

1. Helpnet Security, The Password Reuse Problem Is a Ticking Time Bomb, November 12, 2019

Advantage:
Typically easy to deploy.

Disadvantage:
May not significantly change the organization's security posture.

DATA-FOCUSED

Again, this is a viable concept, whereby an organization focuses on controlling access to the data itself, rather than worrying about applications or access control. If you protect the data, so the thinking goes, you're protecting the most valuable assets of a company.

Ideally, in this environment, those assets are being controlled and managed with an appropriate audit trail (potentially down to the file level) and permissions being granted – for both user access and application access. A data-focused approach usually is relatively transparent to the end user, since it occurs behind the scenes.

A data-focused approach has its merits – for instance, it can help protect you against ransomware attacks and the exfiltration of data. So overall, this gives you a stronger security position than just an identity-focused approach.

The problem is that many data-centric Zero Trust solutions lose focus when it comes to controlling access. You frequently hear some vendors say it doesn't matter if a hacker gets inside, because all the data is protected. But that's not true. If a hacker gets inside your organization, there are many things they can still do as they move laterally across your network – even if the data is protected.

Another issue is that even with a data-focused approach it doesn't address the issue of open ports that hackers seek out with port-scanning bots. If hackers gain access to your infrastructure through an open port and have valid credentials obtained through phishing or brute force attacks, a data-focused approach will recognize them as legitimate users and grant access – without taking into account the context of that access, such as where they are coming in from, what device they are on, if that device has current anti-virus and registry certificates, and other critical factors. They can then have carte blanche to your resources.

The even bigger challenge here is your ability to implement a data-focused Zero Trust approach in a timely fashion. It is a very significant endeavor – one that can take years for you to deploy, since it requires a fundamental re-architecting of your infrastructure. The potentially significant pains of such a rip-and-replace approach keeps many organizations from realizing the security goals of their Zero Trust strategy for years.

Yes, by itself a data-focused approach to Zero Trust provides a good deterrence. However, if it is done in a vacuum, without controlling for factors surrounding the context of access, organizations still end up with just a partial solution. And that partial solution comes at a very big price from an implementation perspective. The potentially significant pains of such a rip-and-replace approach keeps many organizations from realizing the security goals of their Zero Trust strategy for years.

Advantage:
Strong protection over data resources (assuming credentials aren't stolen).

Disadvantages:
Very significant effort to implement.
May lose focus on controlling access.

ACCESS-FOCUSED

The concept here is to control access to all your resources – regardless of where they reside – through a consistent, easy-to-use interface. There are significant advantages to this design. A Zero Trust Access approach, when it's done right, brings together access control for your organization into a central solution, strengthens your security, and allows your business to embrace digital transformation to gain a competitive advantage.

All resources can be protected through a properly designed Zero Trust Access solution, wherever they happen to be. And your organization is no longer subject to the restrictions of the cloud provider for managing access – YOU are back in control of your infrastructure.

Now, your local and cloud security policies can be made consistent. For example, you could have the same Multi-Factor Authentication for all local and cloud resources. You can more easily migrate between your local datacenter and cloud hosting, because the impact on your end users is negligible. They won't know that the workload moved from your on-premise server to the cloud last night.

One of the major advantages of a Zero Trust Access approach is the potential ease of deployment. A properly designed Zero Trust Access product can be implemented alongside your existing infrastructure without the requirement to make changes to your existing systems. This means you can deploy the Zero Trust Access solution while you continue to do business normally, and then migrate users to the new solution over time at your own pace in the way that makes the most sense to you.

Advantages:
Ease of deployment.
Strength of security.

Disadvantage:
Requires some change in user behavior for internal users in particular (no more jumping straight on the network). However, when properly implemented, Zero Trust Access actually makes end users' lives easier while strengthening security. More on that in the next section.

As you have read in this chapter, there are significant differences among the three flavors of Zero Trust. In our next chapter, we will dive deeper into how a Zero Trust Access approach makes life significantly easier for end users, allows your IT team to focus on more strategic initiatives that help grow the business, and saves your organization money.

CHECK OUT THESE ADDITIONAL RESOURCES ON ZERO TRUST ACCESS

Check out these additional resources to learn more about the advantages of an access-based approach to Zero Trust, and how Total Access Control from PortSys delivers simpler, stronger and more unified security for leading organizations around the world:

White Paper	What to Look For in a Zero Trust Solution in 2020
Webinar	IT Security Is Broken: Can Zero Trust Access Fix It?
Blog	Making the Business Case for Zero Trust Access
Infographic	Zero Trust Access: Today's IT Security Falls Short
Video	Total Access Control: Zero Trust Access
Case Study	TAC's Zero Trust Access Helps UK County Council Improve Productivity, Gain Granular Access Control
Case Study	Oklahoma Municipal Power Authority Energizes Team's Secure Remote Access with TAC
Case Study	Total Access Control Provides Zero Trust Application Access for Financial Services Firm
Case Study	ZS Solves Office 365 Security Issue with PortSys TAC
Case Study	Risk-based Security for Any Device and Application
Solution Brief	Total Access Control for Managed Service Providers

To set up a demo on how Total Access Control from PortSys can help your organization to create a more comprehensive, integrated and fortified architecture:

Call: +1 781-996-4900 in North America

+44 208 196 2420 in Europe, the Middle East, or Africa

Email: Sales@PortSys.com

Web: Contact Us

TotalAccessControl™

PORTSYS®