Zero Trust - Security

No matter how large or how small you are, every organization needs to take steps to safeguard its digital data. Cybercrime remains a worldwide threat, and as criminals become increasingly sophisticated, organizations in all verticals need to be prepared. A Zero Trust security model can help your organization safeguard your digital assets more effectively than classic cybersecurity models.

The Problem with the Moat & Castle Approach

Traditional cybersecurity defense models emulated the castle and moat mentality of the middle ages. Though this model was the standard for decades, many organizations find that this approach is insufficient for safeguarding data in the cloud era.

This classical approach involved multiple layers of protection where users were required to make it past tightly secured checkpoints and gateways to access digital assets. Each gateway had the ability to verify user identities, controlling access, and (theoretically) keeping unauthorized users out. However, once a user was verified, they were able to move around the internal systems with little to no resistance.

This model's main issue rested on how users were verified: users were frequently granted excessive access with inadequate identify verification or authorization. This implicit trust model meant that as long as an unauthorized user was able to sneak past the perimeter, there were little to no safeguards to prevent them from accessing almost all areas on the network. However, in addition to a lack of least privilege access, this model also suffered as the perimeter increasingly dissolved, leaving networks vulnerable as physical barriers such as locked doors and digital barriers such as firewalls fell by the wayside as the cloud rose to prominence. Credential theft, as well as credential reuse, made it difficult from a security standpoint to keep unauthorized users out.

As a response to the inadequacies of this classical approach, many organizations have switched to a Zero Trust security model.

What is Zero Trust: A Brief Primer

Zero trust, as the name suggests, assumes that the network is compromised until proven otherwise. This model moves away from the perimeter (or moat and castle) approach and allows security to take a more nuanced approach by guarding access to resources within the network (instead of just guarding the perimeter) and relying on strong authentication and authorization standards to allow or deny specific access based on user and device-specific attributes.

Basic Security Principles for All Organizations

Achieving Zero Trust is not a simple undertaking. Structured is dedicated to helping organizations improve their security posture and we see Zero Trust Architecture as one of the best ways to do that.

A Single Source of Truth

One step your organization should take is to create a single source of truth for verifying identity. In this context, identity includes not just user accounts but also systems, services, the IoT, and any other devices or network applications.

This ensures that every user, device, and application has to be verified by the criteria set out by the central security authority in your organization and allows your security team to access all data on all areas of your network.

This single source of truth approach allows organizations, in many cases, to mitigate account sprawl, password reuse, provisioning, de-provisioning (adding or removing user access), and enforce multifactor access.

Calculated Trust

Your organization should calculate trust (how much or how little you trust someone trying to access your network) and use this information to determine whether or not the potential user is granted access. Factors that should be used in this calculation include:

- Identity
- Multifactor access
- Source (who is potentially making the request)
- Destination (what is the user trying to access)
- Resource sensitivity
- Geography (where is the request coming from. If it is coming from a country or location where none of your employees live, then you know a further investigation is warranted)
- Time (is the request well outside normal business hours?)
- Access method
- System disposition

Accurate Inventory of Users & Data

Your security posture depends on a solid foundation of data. If you do not know what data you need to protect, how many users can access that data, and where that data is located, then you cannot create a robust and comprehensive security solution.

Not Everyone Needs to Be Able to Access Everything

Not every user needs to be able to access all data or all areas of the network to do their job, and overly broad access poses a security risk. Your organization needs to limit access to sensitive data and keep strict tabs on who does and doesn’t have access. If temporary access needs to be granted, you need a procedure in place to ensure that temporary access is revoked as soon as it is no longer absolutely necessary.

Multifactor Access

Multifactor access is a simple concept that allows you to add an extra layer of security easily and can take several forms. Multifactor access may involve having a user enter their username and password, at which point the program they are trying to access sends a temporary verification code to one of the users other devices (such as their smartphone). The user then authorizes the log in via their smartphone by either entering a temporary secondary password or clicking a prompt on the phone.

This approach means that an unauthorized user would need to have access to an authorized user’s smartphone as well as their username and password.

Modern Multifactor Access solutions are able to monitor user access and source, thus contributing to the calculation of trust in a way that SMS or text as a second factor is unable to do.

Logging

Logging is essential. You cannot protect what you cannot see. Modern logging solutions employ machine learning to help discern signal from noise.

Handling Access, Authorization, Encryption & Other Critical Procedures

Securing Apps & Data

Though there are a few general rules all organizations should follow when it comes to cybersecurity, how you secure your apps and data will vary from organization to organization. An assessment framework like CIS20 can help you get started, and a philosophy or architecture like Zero Trust will help you focus your efforts.

However, all organizations should start by identifying what data they have and what apps they are using, and who or what can access this data and those apps. Based on that information, you can determine which users and devices require access to which data and apps to complete their work, allowing you to limit unnecessary access.

Citrix Products & Services to Consider Leveraging

Zero trust security is a mindset, but to execute on that mindset you need high quality products. Citrix® provides solutions that you may want to consider leveraging to support your goal of achieving Zero Trust Security.

Remote Apps & Desktops

Remote apps and desktops help ensure that all data and other information are kept in the data center instead of stored across multiple user devices. This centralized approach not only lets your security team keep an eye on everything by preventing data silos but also prevents sensitive information from being stored in an unsecured manner.

Citrix ADC with SSL VPN

An ADC (application delivery controller) is a comprehensive application delivery and load balancing solution suitable for monolithic and microservices-based applications. This cloud-based product provides users with greater speed and agility, as well as operational consistency and holistic visibility on the cloud. This product not only makes it easy to move to the multi-cloud but is also able to protect your applications and APIs no matter where your employees are accessing them from.

Securing your ADC with an SSL VPN (Secure Sockets Layer Virtual Private Network) allows users to access your network via a secure web portal and provide network-level access via an SSL secured tunnel between the user and your corporate network. This solution allows users to access sensitive resources on your network in a simple yet secure way.

Citrix's ADC with SSL VPN solution can be paired with Citrix SSO (single sign-on), allowing your users to securely access business-critical applications, virtual desktops, and corporate data anywhere, anytime, making it a vital tool for organizations whose employees are currently working from home. Both of these solutions are able to integrate with many common MFA vendors and include WAF (web application firewall) and other security options.

Platforms with Built-in Security Analytics

A good security posture is built on data. Knowing precisely what is going on at any one time on your network is vital for spotting potential issues early and responding quickly to threats.

Having a robust cybersecurity solution that is tailored to meet your needs is vital for safeguarding your organization's digital assets. To help you keep unauthorized users out, our security solutions rely on only the highest-quality products and services from trusted partners like Citrix. Their solutions power business mobility by providing clients with secure, mobile workspaces that allow users to access apps, desktops, data, and communications securely and easily from any device and over any network or cloud.

Endpoint Management
Managing your endpoints is crucial for safeguarding your data, particularly as many organizations add to their ever-increasing array of user endpoints. Working with a company like Citrix that specializes in endpoint management can help you streamline the entire management process and give you a consolidated view of your device configurations and usage policies. This allows you to improve user experience for your employees while also keeping your network secure.

How can zero trust security help keep your digital assets safe? Our experienced team is here to help you find out. Let's get started.

Get started with Zero Trust Security

Visit **structured.com** to start the conversation

🖥 **structured.com**
☎ **1 (800) 881-0962**
🐦 **STRUCTUREDINC**
in **STRUCTURED-COMMUNICATION-SYSTEMS**