Zero Trust and cybersecurity with Hexnode UEM

Trust is something that has to be earned, be it in real life or in your enterprise architecture. Zero Trust is a security concept based on the principle that no device, user, or application attempting access to your architecture can be considered secure. First coined in 2010 by John Kindervag, the term Zero Trust challenges the traditional security models that are based on the assumption that everything inside an organization's network can be trusted. As such, legacy technologies such as VPN and NACs are used to verify the users outside the company network before granting access to the network. The older models assume that all users will behave responsibly and that their identities are never compromised. Zero Trust recognizes the vulnerability of this assumption. Instead of trusting anything inside or outside the organization's perimeters, everything has to be verified before being granted access. For enterprises betting everything on securing their systems, Zero Trust is an unavoidable update for cybersecurity.

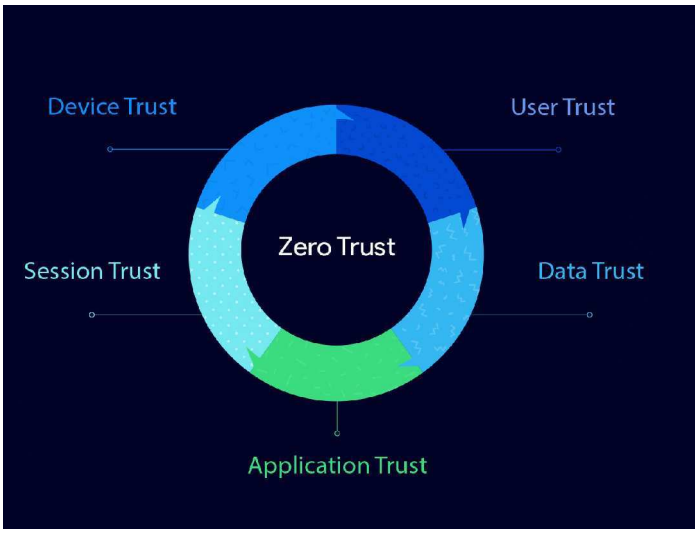
The need for Zero Trust approach in Information Security

The traditional security models operate under the convenient assumption that all cyberattacks must occur due to outside forces. However, the reality is not so convenient. According to a report from Verizon, 34 percent of all security breaches were insider attacks. In comparison to external attacks, insider threats are often guaranteed to cost the company heavier losses. So the question arises: How to secure your organization completely?

The traditional security models classify the network into perimeters and sub-perimeters using specific rules. If an attack occurs, the spread of the attack is defined by the sub-perimeters. Such an approach can be faulty since the point of infiltration may differ from the target location. With the users accessing different apps from different types of devices from various locations, a simple and dynamic security model is required to adjust to the changing needs. Amongst the new security models, the Zero Trust Model is one of the most promising ones. Zero Trust completely erases any perimeters within the organization. By verifying each and every user/device/application/location, the organization gains granular visibility for all traffic, be it internal or external.

Zero Trust Model: Never Trust, Always Verify

The success of the Zero Trust model is rooted in the transition from "trust, but verify" to "never trust, always verify" approach. So, what does implementing Zero Trust look like? There are five important components in building a basic zero trust architecture:



- **Device Trust**: An IT admin has to know about the devices that he is going to manage before trusting them. For that, you should have a detailed inventory listing all the devices owned or managed by the organization with all the relevant device details. You should also be able to monitor, manage and control the devices. This can be done by enrolling the devices in a suitable UEM solution.

  With Hexnode UEM, you can monitor and manage your mobile, desktop, and rugged devices across all platforms from a single web console. You can also configure compliance rules and ensure that you can continue trusting the devices by scheduling checks for device compliance regularly.
- **User Trust**: Depending upon just the traditional password-based user authentication has proved to be ineffective if you are serious about cybersecurity. Additional technologies like Multi-Factor Authentication (MFA) and Single Sign-On would further secure the user authentication process. Hexnode helps the IT admin to build a contextual relationship with the user. With conditional access policies and cutting-edge technology like smart card authentication, Hexnode helps you implement zero trust for users.
- Session Trust: A key component of zero trust is session trust. It means that the user has the least privilege access. The user would be able to access only those resources that are required to complete the assigned tasks. Using this principle, the access is limited for the users and minimum permissions are granted. For example, with Hexnode UEM, you would be able to maintain total control over data sharing by restricting Bluetooth, NFC, and Android Beam. Other conditions such as network restrictions and application permissions can also be defined and configured to establish session trust.
- Application Trust: Apps are used for everything in today's mobile world. It is not surprising that hackers target precious resources using fraudulent apps that trick the unsuspecting user. Helping the user to securely access any application is an important step in attaining zero trust for the organization. Hexnode allows the IT admin to modify the app permissions to regulate the exact level of control the app has over target devices. You can also create a custom app store with verified work apps to secure the application access. If any app shows suspicious behavior, you can simply remove the app with a single click from your Hexnode Web Console.

- **Data Trust**: The sole purpose of any security system is to protect the organization's data. It is of utmost importance to protect the data from any attacks or breaches and to ensure that the users are interacting with unaltered and accurate data.

Zero Trust, ZTA, and ZTNA: How do they differ?

Confusing terms? Well, let us clear the air for you.
When we say Zero Trust, it refers to the Zero Trust security model. This model moves away from the traditional implied trust based on users and network location. Zero Trust requires authentication on every transaction. The users and devices are always verified before they get access to any company resource.
Zero Trust Access (ZTA) is access control of your network. It involves knowing exactly who and what is on your network at any point of time. ZTA ensures that the admin knows who exactly is using the network – is it an employee or a guest user? It also verifies the endpoints on the network, i.e., the admin is aware of all the devices connected to the network.
Zero Trust Network Access (ZTNA) is often confused with ZTA because of its name. ZTNA, also known as Software Defined Perimeter (SDP), is actually concerned with applications. It gives users secure and brokered access to the applications. The applications can be accessed only by authorized users, where the trust has to be earned.

Zero Trust vs VPN for remote device security

VPN works on a perimeter-based model, where everything inside the private network's perimeter is trusted implicitly. This could pose a risk as it gives no assurance against internal attacks. In contrast, Zero Trust extends the capabilities of VPN with the "never trust, always verify" principle. It uses a variety of methods to implement it like multi-factor authentication, least-privilege access, real-time monitoring, and more. Connecting to the VPN is often as simple as entering the authentication details.

Replacing VPN with Zero Trust in remote work

A Virtual Private Network (VPN) that gives remote access to the employees usually allows the users to sign in to the company network from anywhere as long as there is an internet connection.
In contrast, there is greater visibility of each user and device on a Zero Trust network. The user has to go through authentication on every connection request, which means that the user would not get access to any company resource unless verified. Zero Trust helps to give access as needed for the users, without assuming that the users on the network are all trustworthy.

How does Hexnode help you in achieving Zero Trust within your organization?

Enrollment and device provisioning

The first step in achieving Zero Trust security is to securely provision devices for users with a Unified Endpoint Management (UEM) solution. With Hexnode UEM, you can easily onboard your devices across iOS, Android, Windows, macOS, and tvOS platforms using a variety of methods. Both BYOD and corporate devices can be enrolled over the air using services like Apple Business Manager or Android Zero Touch Enrollment. Provisioning the devices using a UEM solution gives the IT admin the control to assign the users to the corresponding devices, establishing both device and user trust.

Securing connectivity

An unsecured corporate network leaves many doors open to potential attackers who want to steal valuable data or customer information. To implement zero trust, we need to assume that the users are potential attackers. Hexnode allows you to set up and connect your devices to a secure Wi-Fi network without the user knowing its password. For additional security, you can also add a SCEP or PKCS certificate. You can also configure network usage rules for iOS devices and data usage restrictions for Android devices. Using features like Web Content filtering, you can restrict user access to trusted websites and decrease the surface area for hackers.

Defining contextual policies

The zero trust model is based on adaptive access. The policies have to define on the basis of full context, i.e., verifying the user and the device, configuring app permissions, securing the networks, and overall threat management should be monitored on a regular basis.

Enforced compliance

The IT admin can customize compliance rules and enforce it in different ways. For example, if the device is not application compliant due to missing apps, the admin can install the missing application from the Hexnode Web Console. If the device is lost or stolen, the admin can remotely wipe or lock the device to prevent the loss of any important data.

Secure app distribution

Which apps are trustworthy and which are not? All decisions are in the hands of the IT admin. The admin can blacklist/whitelist apps, configure app permissions, configurations,,

install and uninstall apps silently on supported devices, and design custom app stores. In addition, Hexnode provides work and personal app segregation.

The role of Kiosk mode in app security

For corporate devices that are meant exclusively for work purposes, you can lock down the managed devices into the required work apps. With Hexnode, you can lock down these work-specific devices into a single app or multi-app kiosk mode. Such dedicated devices reduce employee distractions, save time, provide easier access to the apps, and also secure the device against attacks from unknown and unauthorized applications.

Data protection

Mobile devices are prone to data leakages and it is essential to protect critical information. The threat management capability of Hexnode helps you to secure data from the network, app-based and physical threats. The admin can configure password policies to enforce strong passwords, configure restrictions that enforce encryption, and carry out full-disk encryption of Windows with BitLocker and macOS with FileVault. The encryption ensures that the data is secured and the data integrity is maintained at all times.

Updated reports

For adaptive access, continuous monitoring is important. It is only possible with good reports that are up to date with the latest device and user information.

In summary...

Trust is a vulnerability that can be exploited. The castle and moat mentality has become outdated as more and more organizations are moving towards zero trust. Now, with Work From Home becoming increasingly normal, Zero Trust is the preferred model for addressing remote work security challenges. The very first step in achieving zero trust in your organization is to use a Unified Endpoint Solution to manage your devices. One of the major challenges that an IT admin faces while trying to implement a zero-trust model is the different types of users, devices, and applications. With Hexnode UEM, the process becomes simpler as the admin can easily manage everything from a single console.