ManageEngine
AD360

ACCELERATE ZERO TRUST WITH STRONG AUTHENTICATION

Table of Contents

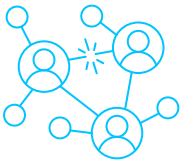
The global pandemic has deeply impacted many business infrastructures. It has been more than two years, and companies are either continuing to operate fully remote or are slowly moving towards a hybrid model. Along with this massive shift has come a significant hazard: a record-breaking increase in the number of cyberthreats.

According to the **Global Cybersecurity Outlook 2022 report**, ransomware attacks saw a significant increase in the first six months of 2021, with global attack volume increasing by **151%**

The traditional pre-pandemic security system is inadequate to handle today's constantly moving workforce. An identity-driven security model is needed to secure the perimeter-less workforce, which can be implemented by Zero-Trust architecture. In this e-book we will discuss what cybersecurity challenges emerged post-pandemic, why Zero Trust is the key to solving these modern-day security problems, and how authentication, of all tools, plays a key role in building an effective Zero Trust environment.

1 Post-pandemic challenges to cybersecurity

Organizations have had to adopt alternate workforce and infrastructure models to survive the consequences of the pandemic, such as an increased reliance on cloud computing and a shift towards hybrid and full-remote workforces. These changes brought many benefits, like enhanced network scalability, accelerated digital transformation, and personalized employee experiences, but along with them came a major drawback of security gaps, such as the following:



i. Absence of a well-defined perimeter

Many employees are now working with flexibility to their location, potentially from anywhere in the world. The flexibility has made securing an organization's network and business-critical assets even more difficult because of the absence of a well-defined perimeter.

Traditional security measures are inclined towards securing physical perimeters, but are not well-prepared for a boundary-less network. Modern day cybersecurity approaches need to be expansive, and must cover every endpoint connected to the network, regardless of where they are connected from.

ii. Shadow IT

A 2021 survey conducted by Bitglass revealed that over 82 percent of organizations have enabled at least some extent of bring-your-own-device (BYOD) policies.

Widespread BYOD has raised concern about shadow IT, which refers to the unsanctioned use of IT systems, devices, and software within organizational networks. Employees use their unmanaged personal devices to download all sorts of information and applications, some of which might contain malware. The lack of alignment of these devices to their organization's IT policies can lead to the inflow of unauthorized traffic, corruption of data and software, and eventually result in hackers and malware gaining access to the organization's network.

iii. Lack of network visibility

The era of the hybrid work infrastructure has made network management even more challenging. When an organization has most of the endpoints or devices connected to its network distributed all across the globe, it is nearly impossible to monitor network activity from a central platform. Beyond an increased difficulty in monitoring traffic from these devices, some of these endpoints might be operating from compromised external networks, leading to increased risk of attack.

2 Mitigating the post-pandemic cybersecurity concerns

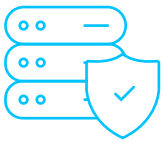
The gradual transition to a hybrid workforce brings a burden of verifying and monitoring a mixed pool of endpoint devices according to the company's specific IT policies. To optimize the benefits of a hybrid model, organizations must adopt a cybersecurity approach that protects all the endpoints and their applications within the network, regardless of whether they are managed or not. One solution is to adopt Zero Trust network architecture, which includes methods for mitigating the post-pandemic cyber security concerns.

3 The principles of Zero Trust

Tackling the post-pandemic cybersecurity challenges has been easier with Zero Trust, as it works on the assumption that no entity within the network can be trusted, and therefore needs to be authenticated, authorized, and continuously monitored, in order to retain access to the organization's network. Some of the core principles that drive Zero Trust include:

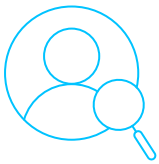
i. Never trust, always verify

As compared to traditional security systems, which rely on creating a physically-defined perimeter to define authorized endpoints, Zero Trust expands the scope of security perimeters. It adopts the "never trust, always verify" approach, which means every entity, regardless of its network location, must undergo a fine-grained verification process before accessing the organization's resources.



ii. Securing data using granular context-based policies

The fundamental architecture of Zero Trust is established with micro-segmentation. Micro-segmentation divides the network into zones, down to the level of individual workload. This segmentation makes it easier to define and secure each zone's data and access by implementing specific context-based security policies, such as the principle of least privilege. This policy ensures each user gets only the minimum required set of access in order to perform their duties. By making security as granular as possible, Zero Trust eventually reduces the attack surface for potential threats.



iii. Continuous monitoring

Employees are entrusted with sensitive data and have legitimate access to the company's assets. They are one of the key elements of an organization, but also one of the biggest sources of vulnerabilities and threats. Hence, the third and equally important ingredient of Zero Trust is mitigating risks with continuous monitoring.

Implementation of security information and event management (SIEM) helps in collecting employees' digital activities. Once this data is centralized and contains sufficient historical information, a baseline of usual behavior for each individual user and machine can be established through the use of user and entity behavior analytics (UEBA) solutions. Any deviation from the established baselines for each user and entity is identified as abnormal and is then sent for a profile assessment for further potential risks. If the risk score surpasses a particular threshold due to an increasing amount of abnormal activities, the system flags a security alert to notify the network admins.

4 Why use Zero Trust?

When speaking of why Zero Trust should be used, let's have a look at the traditional network security model: The castle and moat strategy.

Castle and moat is inspired from a medieval defense strategy of securing a castle by building a moat to surround the castle walls. Linking it back to network security, the castle and moat model ensures that no one outside the network perimeter can access the organization's data. The use of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) each help secure the network perimeter.

However, what about an insider threat, such as a disgruntled employee or an outsider that gains access to the network by stealing credentials? How does a castle and moat strategy secure a perimeter-less network? What's become evident over time is that the castle-and moat model fails to address these concerns, which eventually gave rise to Zero Trust architecture. Zero Trust takes care of every worst-case scenario by not only securing the entire network, like the castle and moat approach, but by going beyond the network perimeter.

By avoiding placing trust as a binary, Zero Trust is unbiased when it considers who or what to allow access. Binary trust implies that a users should either be trusted with everything or nothing. But in an organization, not everyone needs access to everything. Making sensitive data available to everyone means increasing its vulnerability. To protect an organization from insider attacks, continuous verification and monitoring of employees are both necessary, which also means not putting a permanent trust in them.

Another reason of your organization should use Zero Trust is because it is driven by context. Context helps Zero Trust to ensure the appropriate implementation of security policies and access levels. For example: If a legitimate user is logging in from a new geographic location, instead of completely blocking their access, Zero Trust allows that user to access the network, but only after first employing contextual or adaptive authentication (which we'll explore in a later section). Contextual clues based on the user and the network—such as the type of device used, which department the user belongs to, the access device's geographic location, the user's employment type, which resources are being accessed, and what they are doing with the resource, helps Zero Trust to monitor and evaluate the network security.

According to the State of Cloud Security 2021 report, "36% of cloud professionals say their organization has experienced a serious cloud data leak or a breach in the past year." While this statistic is concerning, organizations don't have to feel powerless when it comes to securing the cloud. Zero Trust keeps cloud data leaks contained by providing better visibility and access management into cloud infrastructure. Zero Trust security policies keep the cloud architecture secure by governing asset access and continuously auditing cloud servers.

To summarize, Zero Trust is an inclusive cybersecurity strategy that can be adopted for both cloud and on-premises IT infrastructures. It supports and secures the modern workforce by validating and authorizing each user and device in the network, using an exhaustive set of policies. Micro-segmentation helps organizations to get fine-grained enterprise visibility and implement security policies. Furthermore, continuous user and entity monitoring and auditing helps to track unusual activity and determine the risk level. With each of these elements of Zero Trust implemented, an organization can always stay one step ahead of cybersecurity threats.

5 Authentication: the first leap to Zero Trust

Authentication is the process of verifying a user's identity. It contributes to the backbone of an organization's network security architecture. If the organization's authentication process is ineffective, the entire network security will ultimately collapse.

As we already discussed, a hybrid workforce comes with a package of unmanaged network and devices; thus, in order to tighten existing security gaps, it is crucial to guard the right user and machine identity.

Getting granular is what makes Zero Trust authentication more secure. With the help of micro segmentation, it breakdown multiple accesses and enforces the right level of authentication to safeguard each of these segments. This process helps to remove the unnecessary access to organization's data to irrelevant employees.

Furthermore, by providing flexible way of authentication based on their context, Zero Trust ensures frictionless entry of legitimate employees to the organization's network.

6 IAM capabilities to accelerate Zero Trust

Identity and access management (IAM) is a set of policies, processes, and tools which helps to authenticate the right identity for users and provide them with the right level of access. Before selecting an IAM solution, the IT security administrators should look out for these must-have authentication features to get started with Zero Trust:

i. Single sign-on (SSO)

Even though security professionals insist on creating a strong password, it is quite hard to remember dozens of passwords for several different applications, ultimately leading to password fatigue.

As per the 2022 Verizon Data Breach Investigations Report, credentials are one of the key paths to a data breach.

With SSO, a user authenticates themselves using only one set of login credentials to access multiple applications. It eliminates the need for multiple authentication requests across diverse platforms, minimizing password fatigue and increasing employee productivity.

ii. Multi-factor authentication (MFA)

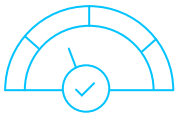
Due to the increasing sophistication of cyberattacks, username and password-based credential systems are insufficient. By adding a layer of security to the user's authentication process, MFA protects from password vulnerability. The most common security layers or the verification factors are:

- Something you know; e.g. passwords
- Something you have; e.g. one-time password (OTP) verification through mobile
- Something you are; e.g. biometric verification

Even if the password is compromised, by forcing an authentication attempt to be validated by more than one method, MFA ensures secure access to the network.

iii. Contextual authentication

One can elevate their MFA authentication process with contextual authentication. During the authentication process, each profile is assessed with respect to their access request context such as location, time, device, network, and application. If the user's context matches with the IT security set conditions, the system will authenticate that user and provide them with full access to the features they've been assigned. In cases where there's a minor anomaly, they might be provided with only partial access and if the user's context doesn't qualify the security condition, their access will be blocked.



iv. Adaptive authentication

Adaptive authentication brings context-based and machine learning techniques under the same roof. Adaptive authentication, also known as risk-based authentication, is when an appropriate level of authentication is selected based on an employee's risk score.

User login and online behavior is assessed for each profiled, then classified with a risk score. Based on this risk score, the verification tool decides whether to ask for additional credentials, such as an OTP via email or SMS, or will grant access with fewer credentials.

7 IAM and Zero Trust: A compatible duo

The ability to optimize a user's identity profile is a feature shared by both Zero Trust and IAM. Although an IAM policy of identity governance is what provides a base for Zero Trust architecture, we cannot just start with Zero Trust strategy without considering IAM. Here's how IAM supports Zero Trust:

- Whether the employee is logging in from the office or remotely, IAM validates every user's identity. Combining the Zero Trust approach of "never trust, always verify" with strong IAM policies, an organization ensures secure access to the right identity every time someone tries to enter the network.

- Along with verification, IAM also binds the right level of access with the right identity, ensuring that each employee can retrieve only the bare minimum data which is required to complete their work. This is one way of implementing policies that uphold Zero Trust's principle of least privilege.

- IAM tools exhaustively monitor and audit access logs. This information can equip IT security teams to have fine-grained visibility of the behavior of each user and device.

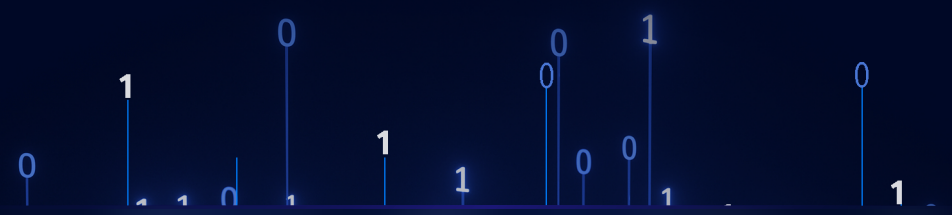
- With SSO and MFA, IAM strengthens an organization's credential game, thus boosting the verification process.

- Zero Trust continuously monitors users and assesses their access privileges. IAM aids this principle with automated life cycle management and identity governance, both of which help manage user identities and update their accesses across their life cycle.

8 Zero Trust - the ManageEngine way

The first step and the foundation of all Zero Trust strategy is identity. With ManageEngine's AD360, all identity and access management needs can be met at one place. It helps accomplish all critical IAM operations such as user provisioning, self-service password management, Active Directory change monitoring, MFA, SSO, and so on with a simple and easy-to-use interface.

It's core capabilities include automated risk assessment and threat intelligence, as well as adaptive authentication and automated user life cycle and entitlement management for enhanced identity governance. By automating routine IAM tasks—like user provisioning, modification, and deprovisioning—AD360 helps remove human errors and redundancies. It helps enforce least privileged access, which is essential for detecting and preventing privilege abuse. Furthermore, it facilitates continuous monitoring and auditing of employee activity. Whether it's on-premises, cloud-based, or hybrid, AD360 can make an IT infrastructure safer and easily manageable.



About ManageEngine AD360

AD360 is a unified identity and access management solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, secure SSO, adaptive MFA, approval-based workflows, UBA-driven identity threat protection, and historical audit reports for AD, Exchange Server, and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for all your IAM needs, including fostering a Zero Trust environment.

$ Get Quote

Download