cisco SECURE

Solution Guide
Cisco Public

How to go from MFA to zero trust

A five-phase plan for securing user and device access to applications

Contents

Introduction

The rising market adoption of zero trust reflects a changing reality: the way we do business has fundamentally and forever shifted.

Traditional boundaries have blurred thanks to increased connectivity and expanding remote and hybrid workforces. These blurred boundaries—between businesses, suppliers, customers, workers, and home life—dramatically increase risk in ways that outdated identity and access management models are ill-equipped to handle.

Security resilience is the linchpin for long-term organizational success. Ninety-six percent of security executives consider security resilience as "highly important."[1] With an uptick in cyberattacks and the escalating threat of ransomware, organizations are working overtime to secure user access. This heightened threat landscape is driving security leaders to establish a foundation of security resilience so they can better navigate unknown events and changes with confidence.

A zero trust architecture eliminates the assumption of trust by constantly verifying trust at each access attempt—for users, devices, apps, networks, and clouds.

Zero trust security offers a new way of securing access and future-focused leaders are ready to embrace it. A zero trust architecture eliminates the assumption of trust by constantly verifying trust at each access attempt—for users, devices, apps, networks, and clouds. By never assuming trust, continuously verifying it, and applying least privilege to each access control decision, organizations can reduce risk systematically without impacting productivity or operations. In a recent study, organizations with a mature zero trust implementation scored 30% higher in security resiliency than organizations without a zero trust strategy.[2]

Yet the adoption of a zero trust architecture brings a new challenge: What are the steps needed to make meaningful progress towards zero trust?

This guide lays out a practical, five-phase approach for implementing zero trust security for trusted user and device access to applications. Keep in mind that a complete zero trust architecture extends beyond access management to protect app-to-app access, access to multicloud and hybrid IT environments, ID management, user web traffic, and more.

1 https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-vol-3-report.pdf

2 https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-vol-3-report.pdf

Achieving a zero trust environment is an iterative process. Teams ready to adopt zero trust can begin with a specific set of people, expand coverage for their applications, and then further expand coverage for their devices. Once they are continuously verifying trust within this well-defined scope, teams can apply a set of reasonable policies to enforce trust and protect the organization. The final step is to integrate this scope and enforce those policies across the broader organization's IT and security functions, and ultimately shift to continuous improvement. Following these initial steps, an organization can incrementally achieve a zero trust environment.

Like default deny, zero trust begins with no access until trust is established, verified, and enforced based on the principle of least privilege. As a result, excessive trust is eliminated, along with the risks associated with it. Zero trust security builds upon these principles with the following concepts:

The zero trust approach

Principle of least privilege. Limit access rights to only those applications and networks a user needs to do their job.

Visibility informs policy. Provide as much intelligence and insight as possible to the people administering the technology, to produce informed policies.

Trust is neither binary nor permanent. Continually reassess the posture of users, devices, and applications, and adjust your trust accordingly. Be prepared to contain newly discovered threats and vulnerabilities.

Ownership is not a control. Validate and extend trust to devices, applications, and networks that you don't own or manage, from BYOD (bring your own device) and IoT (Internet of Things) devices to SaaS and public cloud.

The perimeter is any place where you make an access control decision. Choose the layers and process points that work for your environment, whether it's at the network layer, the application layer, at the point of identity verification, or during a transaction workflow.

Access decisions are based on re-establishing trust every time. Membership within a group, an application service within a tier, or a device connected to a network location, is not enough on its own to authorize activity.

Containment. Combine least privilege and segmentation with response capabilities to monitor for threat activity and limit its spread by default.

The four functional pillars of zero trust

To compete and thrive in this era of increased risk and unpredictability, organizations must lay the groundwork for more resilient and flexible security operations, with zero trust woven into the fabric of the IT environment. To maximize zero trust efforts and establish more effective access processes, we believe a zero trust platform must perform these four functions:

1. Establish trust to verify each user and device and increase visibility.
2. Enforce trust-based access to grant the appropriate level of access and enforce access policies based on the principle of least privilege.
3. Continuously verify trust by reassessing trust level and adjust access accordingly after initial access has been granted.
4. Respond to changes in trust by investigating and orchestrating response to potential incidents with increased visibility into suspicious conditions related to trust level.

These functions support secure trusted access across each of the core pillars of the CISA (Cybersecurity and Infrastructure Security Agency) Zero Trust Maturity Model:

- **User and Device Security:** making sure users and devices can continuously be trusted as they access resources, regardless of location.
- **Network and Cloud Security:** protecting all network resources on-premises and in the cloud, and securing trusted access for all connecting users.
- **Application and Data Security:** preventing unauthorized access within app environments no matter where they are hosted.
- **Visibility, Analytics, Automation, and Orchestration:** detecting and responding to threats for faster recovery and greater security resilience.

Zero trust for application access

This guide recommends an iterative approach for securing trusted access for users and devices. We've designed it to help you define a set of attainable success criteria. Tightly scope one aspect of the organization, proceed with that scope through the five phases of the journey, and then integrate that scope into your organization's zero trust architecture. This approach treats each initiative as a self-contained project within the larger transformation.

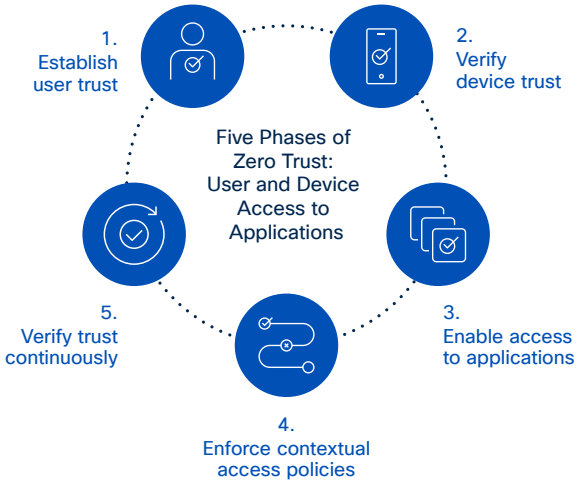
Within the scope of each initiative, use the following sections for each phase of the journey.

Description and objectives. For each of the five phases in the journey to zero trust, we provide an overview along with the objectives we must meet to complete this phase. These objectives align to the zero trust initiative, not to the overall organization. For example, establishing user trust and device trust is specific to the people and their devices within the organizational group we are moving to the zero trust architecture.

Transformation. The beginning of each phase includes a workshop to gain consensus and support, and to identify next steps. Suggested attendees are stakeholders from security, IT operations and support, function and the business units within the initiative's scope. Questions are provided along three disciplines: strategic, management, and operational. By scoring these with on a scale of 1 through 5, the team can determine the organization's maturity for the given phase.

Components and challenges. Successful transformations involve integrating technology while managing potential pitfalls. The components section includes recommended technologies for the given phase of the zero trust initiative. Under challenges, we highlight frequently seen concerns and potential solutions.

Metrics. Metrics are essential for guiding action and tracking success along the transformation. In this section, we suggest metrics for risk management, security, IT support, and IT operations. Each specific scoped initiative can use these metrics to progress through the phases. Once the scoped initiative is completed, the metrics can continue to be collected to measure the efficacy of the overall zero trust architecture.



Phase 1: Establish user trust

Ensure you have the right mechanisms and processes to properly authenticate users attempting to access your resources. You can achieve this in several ways. Multi-factor authentication (MFA) is one of the most common approaches for establishing user trust. Single Sign-On (SSO), passwordless authentication, and other user-friendly innovations have eased the adoption of this zero trust principle for organizations large and small, and we speak to those more in Phase 3. To jumpstart your zero trust program, keep the project scope well defined and focused. The focus of Phase 1 is to verify user trust, enforce the principle of least privilege, and make it easy for users to adopt trusted access.

Description

The perimeter is any place where you make an access control decision. With zero trust user access, the perimeter gets established when a person accesses an application. It is a seemingly simple moment. A click, a fleeting pause, and the application opens. But within that moment, many tasks and verifications are being performed. Many more are possible. Within the authentication workflow, we have a control point to evaluate and enforce trust. The first step in establishing a zero trust architecture is gaining control over identity verification.

Privileges are what people can do with the IT we protect. Trust is whether we have confidence that people will use those privileges in a trustworthy way. Much like the principle of least privilege emphasizes we only assign the privileges needed and no more, the principle of zero trust emphasizes we only trust people as much as needed and no more.

We need to take stock of the areas we trust people and the means in which people can establish or lose trust. We can approach this by type of users; for example, those with privileged access or those with remote access. Alternatively, we can approach this by activity; for example, a critical process or a frequently targeted process. Scope the zero trust effort to one area and assess the people and technology involved.

After scoping the user trust effort, three work streams are required: the first work stream is to *increase security*; the second is to *manage usability*; and the third is to *help people through the change* by communicating and socializing what's to come. For usability, identity verification must be quick, convenient, and nearly invisible under most circumstances. But for security, when the circumstances are suspicious, the identification verification offers a control point to prevent access until trust is established via additional authentication methods. Balancing the two is a success factor in establishing user trust.

Ensuring the security system can trust the user is who they claim to be is the first step in establishing a zero trust architecture. In addition to username and password, two-factor authentication or multi-factor authentication (MFA) provides a stronger assurance that the user is who the user claims—or, when additional trust is required, such as when a user attempts access under suspicious conditions or when an action puts the organization at risk, the security system must be able to challenge the user to re-authenticate or to produce additional forms of authentication. This establishes and maintains strong identity across a variety of situations in a zero trust architecture.

Objectives

- Risk-rank people by role and access to information so they align to the principle of least privilege.
- Go beyond employees to include contractors, temporary workers, and other difficult-to-secure user communities.
- Expand the use of MFA for the most commonly used apps and the number of people using the zero trust architecture.
- Evaluate the use of passwordless for strong authentication; gather use case details and adoption targets.
- Ensure every user is continuously validated each time they request access to a resource.

Transformation

Strategic

The objective here is to determine whether there is an established direction for the organization and may lead to a broad discussion.

Is there a clear identity strategy in your organization?

- Determine whether there is a clear vision and direction, who owns this strategy, and how is it governed within the organization.
- Publish and communicate the strategy so that it is clear to the organization and verify that it is understood in its application and timeline, including individual and team expectations.
- Determine the extent and coverage of the strategy and whether it covers third parties, partners, and the use of external resources such as cloud providers.
- Is the strategy effective and are clear metrics provided?
- By which methods are change and improvements measured, identified, and implemented?

Management

The objective is to define how well the identity and access management (IAM) requirements for the organization are understood and managed on a daily basis.

Do you have a clearly defined IAM function?

- Is there a named group that manages the IAM requirements for the organization?
- What is the level of hygiene of the IAM systems being used?
- How does it integrate with other parts of the business to ensure full joiner, mover, and leaver consistency?
- How clear is the reporting from the IAM function?
- Determine the speed and consistency of changes implemented and whether they are in line with business change.

Has an MFA solution been implemented?

- Has a solution has been identified and implemented?
- To what extent has the solution been integrated into the IAM strategy?
- To what extent has the MFA solution been integrated with the IAM infrastructure?
- Is there clear feedback and reporting on the implementation?
- Have you evaluated your threat model for resilience against the latest MFA-targeted attacks?

Operational

The objective is to identify the extent to which any solution has been implemented across the user base.

What percentage of users enrolled are using MFA?

- Has a solution been implemented?
- Is there a clear metric that shows the number of users enrolled?
- Is there a dependable metric on the user base?
- Is there a metric that breaks down the implementation by user, group, or business area?
- Plan to ensure a full deployment is in place, measured, and monitored.

Metrics

Risk

- Overall risk level
- Risk register – issue mitigation
- Audit compliance – issue mitigation

Security

- Incident reduction
- Account takeover (ATO)
- Business email compromise (BEC)

Support

- FTE usage
- User MFA support tickets
- User MFA support satisfaction (NPS)

Operations

- Apps configured with MFA
- Users enrolled in MFA

Is MFA integrated into other functions?

- Has a solution been implemented?
- Are you providing access to mission-critical applications that require protection against data loss?
- Identify potential areas of security and IT that can benefit from the MFA capability.
- What actionable information is available from the MFA solution?
- How resilient is the MFA solution to attacks targeting MFA-based vulnerabilities (e.g., MFA push harassment or push fatigue exploits)?
- Which method and manner are historical authentication logs or real-time risk signals shared with other functions, automated or otherwise?
- Create a benefits statement showing how the MFA solution improves delivery in other functions.

Are you using authentication methods that rely on user devices as authenticators?

- Do you have a policy established to differentiate between corporate and BYOD devices?
- Are you able to ensure user authentication devices have been updated to a sufficient level to establish trust?
- Do you have a process to replace lost or stolen user devices securely?

Components

Identity Database. Organizations must keep the information and attributes about their users, and to group them where necessary according to organizational, geographical, or other aspects. This is generally provided by the **Identity Provider (IdP)** service.

Strong Authentication. Multi-factor authentication establishes necessary roadblocks for attackers looking to compromise an account. Aside from making it harder to gain access, MFA requests require trust to be re-established. More advanced MFA technology, like passwordless authentication using biometric methods, can provide a frictionless experience for the user and help accelerate wider MFA adoption.

Challenges

Our end users are very hesitant to change. Past security changes have made it harder for end users to get work done, making them resistant to future changes. The journey to zero trust must minimize the impact on people, while communicating and socializing the need for change.

We're focused on securing our remote access. Remote access is a logical starting point for a zero trust initiative. With more apps going to the cloud, the definition of remote is expanding and the perimeter is blurring. Build momentum with remote access and continue on to other workflows.

We can't interrupt workflows across the organization. Nothing will stop a security initiative faster than halting the organization's work. Take the journey to zero trust one workflow at a time with careful planning, testing, and an emphasis on usability.

Phase 2: Verify device trust

Which endpoint is being used with every access request? Is the device company-owned and managed or personally owned, and is it in a healthy and secure state? Is it enrolled in a mobile device management (MDM) or unified endpoint management (UEM) solution? Do you have a robust access security policy in place and the tools to enforce it? This is a key stage for detecting account takeover attempts, compromised systems, and other threats that impact the trustworthiness of devices attempting to access applications and resources on your network.

Description

Ensuring the devices authenticating to your network to access applications are in a healthy and trusted state is the second step in establishing a zero trust architecture. We begin by inventorying and prioritizing applications and devices. The security goal is to establish trust so that users, whether employees, contractors, seasonal hires, or partners, can securely access a given application using their company-issued or personal endpoint without posing a risk to the organization. Therefore, one essential element is to integrate the applications with the zero trust authentication and access controls. The other is to acquire visibility into the access and authentication devices and their accompanying security posture. Together, this builds the device and access portfolio which we can use later to make policy and enforcement decisions in the zero trust architecture.

Authentication and access devices

Under a zero trust model, devices fall into two categories: authentication devices and access devices. Authentication devices, such as a mobile phone or security key, enable users to perform strong authentication to establish and maintain trust. The access device is the one the end user launches and interacts with the application, such as a desktop or laptop computer. Users often have several devices to complete their work, including organizationally issued and personally owned devices. Criminals seek to exploit security vulnerabilities in the device operating system or software to hold the devices for ransom, gain access to sensitive data or otherwise disrupt the organization. The zero trust security system can evaluate trust in the device by answering key questions, including:

- Have we seen this device before?
- Are the device's operating system and browser up to date?
- Is this device owned and managed by the organization or an unmanaged personal device?

- Are there any indications of tampering (jailbroken or rooted)?
- Are security controls like a firewall, password, and encryption enabled?
- Is the device in our inventory database of trusted devices?

In this phase, the objective is to gain visibility into the devices and these associated trust factors before granting access to applications and data.

Traditional IT (trust is assumed) vs. modern IT (trust is verified)

In a zero trust architecture, the path to trust needs more checkpoints, such as authentication factors and conditions placed on the device.

Before the advent of zero trust, device trust was typically based on location. If the device was on the corporate network, we assumed it was supposed to be there, and has access to anything on the network. This led to multiple security issues, from stolen passwords to spoofed network addresses to compromised endpoints. In a zero trust architecture, the path to trust needs more checkpoints, such as authentication factors and conditions placed on the device. One of these conditions can be whether it's a managed, corporate-owned endpoint or an unmanaged BYOD.

Managed devices: how to gain visibility and control

A managed endpoint is typically, but not always, owned by the organization, or at least known to it. Device visibility illuminates the size of the endpoint population. Managed devices may be tracked as part of an inventory, enrolled in a configuration and patch management program, and monitored for security events. For this reason, we may choose to trust a managed device more than we would trust an unmanaged personally-owned device. Many organizations implement a policy that only the endpoints they own and assign to staff are trusted and can therefore be used to access company resources. However, this policy can be difficult to enforce, especially if there's no means to assess the device.

There are different ways to bring a device under management. If the endpoint has a VPN client installed, it's assumed to be an approved and managed asset, allowing the user to access the internal network from the outside (e.g., at home, or from a hotel or coffee shop). With common port-based network access control (NAC), if the endpoint has an 802.1x certificate installed, it's assumed to be an approved and managed asset, so whoever is using it will be allowed to connect to the internal network from inside the building. Finally, enrolling devices in an MDM system allows us to enforce configuration policies by installing an agent.

Certificate-based trust

In each of these cases, we've marked the endpoint as trusted by installing something on it (or given it a second factor—"something it has"). If we don't own and can't manage an endpoint, it's generally more difficult to convince that endpoint owner to let us install something on it. A certificate or other method of fingerprinting is lightweight and may be more acceptable than installing running software. Still, the key requirement is to make that marking unforgeable and prevent it from being copied to another device. The important point is that we've seen the device before and expect to grant it access, as opposed to endpoints trying to access our applications that we've never seen before and may be used by attackers.

Since we will be making trust decisions based on the marking's presence or absence, it functions as yet another authentication factor and needs protection in the same way we protect the primary user credentials (username and password) and the second factor (such as a one-time password, U2F device, or push-based authentication). Certificates offer a way to identify the device as managed. We can take it a step further by including device and user data in the certificate, tying them together so neither one's credentials can be leveraged alone.

Device health-based trust

Another pathway to establishing device trust is by verifying the health and security posture of the endpoint at the time of authentication. Too often have organizations relied on just user trust without checking whether the access device is in a healthy and trusted state, only to fall victim to a data breach from an infected endpoint running outdated software. Endpoints that pass health-related checks at every login such as those listed earlier in this phase provide a higher level of confidence that they are protected from potential exploit due to an outdated OS, browser, plugin, etc. Similarly, checking for the presence of an endpoint security agent, such as endpoint detection and response (EDR) on the device to protect against malware and other threats helps further establish trust.

Performing real-time health and security checks before granting access is a critical step to establishing device trust.

Performing real-time health and security checks before granting access is a critical step to establishing device trust. This can be achieved by adding a lightweight client application to each endpoint. The application reports not only information on the health and security posture of the device, but also machine identifiers that are unique to that device. These unique identifiers can be stored in a cloud-based inventory of trusted devices. At login, the application checks the identifiers on the device and then searches for a match in the inventory database. If a match is found, the device is known and considered trusted, so access is granted. If no match is returned, access can be blocked according to policy.

Flexible deployment for managed company-issued and unmanaged personally owned devices

The net result is a spectrum of device management options, each providing telemetry to establish trust. We can have a fully managed device provided by the organization, with a complete set of agents and insight into every app and action. We can have a traditional BYOD model, with a personally owned device running a single agent, such as MDM, with visibility and control over well-defined areas. Or, we can have a lightweight control such as a cookie, certificate, or app with visibility over what's available from the web browser user agent or user hints at the time of authentication. Managing devices as a portfolio, with specific levels trusted to complete specific activities, simplifies the management and lowers support costs.

Trusting devices only if they're with the right user is the next step towards a zero trust security architecture.

In this phase, the objective is to establish controls over devices and the trust factors available given the device management telemetry.

From a defense perspective, consider the scenario where an attacker steals a user's credentials. Thanks to device trust, the attacker still needs to use a valid endpoint owned by that user to access an application. Having the username and password is not enough to verify access or mitigate the risk of unauthorized access by a compromised device. Trusting devices only if they're with the right user is the next step towards a zero trust security architecture.

Objectives

- Risk-rank and prioritize devices based on risk and data sensitivity.
- Go beyond organizationally owned devices to include BYOD, personally owned devices.
- Establish a portfolio of technologies for trusting devices, including MDM, VPN, VPN-less remote access, and device health.
- Expand the scope of the trusted end-user devices in the zero trust architecture.
- Ensure every access and authentication device is continuously validated.

Transformation

Strategic

Objective: Identify if there is a clear strategy on policy driven device assessments at the point of access.

Is there an existing strategy on trusted devices?

- Identify whether there is a strategy or program for the assessment and control of trusted devices.
- Establish an approach for company-owned and personally owned device management.
- Ascertain whether risk-based policies are applied to identify the level of trust to be granted to an endpoint device.

Management

Objective: Define how well any policy driven assessment of user devices is updated, reviewed, and enforced.

Are policies constantly reviewed against known vulnerabilities?

- If policies exist, are they the responsibility of a clearly named owner?
- Determine whether there is a link between policy development and vulnerability identification.
- Ensure that policy amendments are based on vulnerability identification.
- Identify where policy amendments are tracked and recorded.
- Identify how any asset inventory is amended with policy updates.

Are devices constantly checked at the login stage?

- Determine whether there is a solution to check device hygiene at the login stage.
- To what extent has a solution been implemented within the organization?
- Determine whether there is an integration of the solution with other security and IT functions.
- Determine whether progress is clearly measured and reported.
- Determine whether there is a governance process to manage the solution.

Metrics

Risk

- App risk reduction – critical apps

Security

- Incident reduction
- Compromised devices
- Auth devices – vulnerable devices
- Access devices – vulnerable devices

Support

- Device MFA support tickets
- Device MFA support satisfaction (NPS)

Operations

- Critical apps configured with MFA
- Critical apps configured with SSO
- Access devices – trusted devices

Is the device inventory up to date and regularly reviewed?

- Determine who owns the asset inventory and is responsible for its maintenance.
- What are the methods of updating the inventory?
- Identify whether the use of device identification at the point of access is implemented.
- Is device identification at the point of access being linked to the asset inventory in place?
- Is there constant feedback and review between the inventory status and the access control?

Operational

Objective: Identify the extent to which any solution has been implemented to involve end-users in updating their devices, and how effectively it contributes to the rest of the security function.

Are users prompted to update devices to ensure access is maintained?

- Define a corporate access security policy for all devices.
- Determine if there is a clearly defined process for identifying policy non-compliance.
- Determine whether non-compliance is communicated to the end user.
- Ascertain whether users are guided to update their devices to bring them within policy.
- Determine whether non-compliance is reported by users.

What percentage of devices are managed or unmanaged?

- Determine if there is a clearly defined process for identifying managed or unmanaged devices.
- Determine whether there is a centralized inventory for devices.
- Is there a process for maintaining the inventory on a periodic basis?
- Ascertain the reporting on devices.
- Are reports audited or otherwise validated?

Is device trustworthiness integrated into other functions?

- Determine whether any solution providing policy control over devices has been implemented.
- Identify potential areas of security and IT that can benefit from device trustworthiness.
- What are the outputs from such a solution?
- In what method and manner are outputs shared with other functions, automated or otherwise?
- Create a benefits statement showing how enhanced device trustworthiness improves delivery in other functions.

Components

Device inventory database. An up-to-date repository of unique information on all devices you allow to access the network, including type, purpose, network addresses, asset tags, components, configuration, and responsible user or maintainer.

Managed and unmanaged devices. Implement with a spectrum of toolsets and approaches. Corporate-owned devices can be provided with a number of security agents, including EDR. BYOD can be provided with MDM. For other trusted but not fully managed devices, evaluate device trust and health.

Certificate issuer. This is used to mark your managed or otherwise approved devices with a client-side certificate. Depending on which types of certificates you plan to use, the public key infrastructure (PKI) for this may already be part of another security product.

A portfolio of technologies for trusting devices, including MDM, VPN, or VPN-less remote access and device health, will likely be used to establish your zero trust architecture.

Challenges

Our end users are resistant to installing software on their devices. For a variety of reasons, from concerns over privacy to local regulations, people dislike installing agents on their phones and devices. Select a technology to verify security hygiene during authentication without introducing privacy concerns.

We lack the resources to manage all devices. Device management is often time intensive. For a zero trust architecture, the priority is ensuring the access and authentication devices are evaluated for trust. Steadily increase coverage in a scalable and light-touch way.

We already have a mobile device management platform. A full-featured platform may already be in place for device management. A portfolio of technologies for trusting devices, including MDM, VPN, or VPN-less remote access and device health, will likely be used to establish your zero trust architecture. Begin with the investments you have already made.

Phase 3: Enable access to applications

Know what applications your users need to be productive and grant access based on context and keeping security of your data intact. When developing and implementing an application access management policy for the workforce you should consider types of users, locations and devices resources are accessed from, applications (cloud, on-premises, public/private), the expected workload on IT teams, and most importantly, the user experience you want to provide.

Description

Enabling access to workforce applications required for users to stay productive and meet business goals is the third step in establishing a zero trust architecture. We begin by assessing what types of users require access to which types of applications (cloud, on-premises). The goal is to have a clear picture of exactly which applications each employee should get access to, based on their role and business needs. The access management policy should take into consideration the user role, applications they require, and the device and location the employee will access the applications and resources from. It is important to not allow more access than is needed to minimize risk of intentional or accidental data compromise.

Things to consider as you build out your application access security strategy and policies are:

What types of users are accessing your corporate resources?

If you have a mix of full-time, part-time, or seasonal workers, contractors, vendors/suppliers then you must consider the locations, roles, employment status and variety of other things when crafting the application access policies for each. You also have to consider the onboarding experience. For example, ideally you don't want new employees wasting time trying to understand and get access to different workforce applications individually. They can benefit from bookmarking and accessing a centrally hosted web portal that shows them links to all their permitted applications. This is where single sign-on solutions help.

How are your users accessing applications?

Users might have different devices, locations, and work hours that should be considered when building policies that enable access to various applications. For example, there might be a scenario where a trusted user happens to be working from a location that they "typically" don't. The user is known and trusted, but there might be a need to step up authentication and user trust challenge before granting access to the application requested.

How many applications does your organization manage?

If your organization has even as few as five or 10 applications and any is a conduit to sensitive data, it is imperative to apply governance and controls over those applications. Enforcing user trust, device trust, and per-application access policies will minimize risks of a data breach due to unintentional (on behalf of an innocent user) or malicious events (by a threat actor).

How much time does your helpdesk spend on password resets?

Gartner estimates that 40% of all helpdesk calls are related to passwords, such as resetting employees' forgotten passwords.[3] Is your helpdesk team spending much of its time on this task? Reducing reliance on passwords can measurably reduce time and costs associated with managing them for IT and helpdesk teams.

How many times do your users need to log in each day? What concerns do you have around login fatigue and poor passwords?

If users have to log in multiple times a day either to the same or different applications and authenticate multiple times a day, they are likely to get frustrated by login fatigue. This makes them more prone to engaging in poor security practices like reusing and creating simple passwords that are easy to remember. Streamlining the user login experience without compromising security is the way to go.

Why Single Sign-On (SSO)?

When you look at application usage, small and medium businesses (SMBs) rely on an average of five apps to run their business,[4] while in larger organizations, this number goes up tenfold at least. Getting visibility into and managing access to each and every application is critical for organizations to safeguard against data breaches. To compound this complexity, for every application, the user must create and remember unique and complex passwords. Unfortunately, this is cumbersome, impacts productivity, and most importantly, puts the business at risk. Credentials can be easily phished and stolen and are a top attack vector for web application attacks and data breaches.

That is why solutions like federated SSO help by reducing the number of credentials down to just one (single username, single password).

3 Gartner

4 Salesforce Small and Medium Business Trends report

The several benefits of adopting SSO include:

- Reduce your attack surface and data breach risk since there are fewer passwords in use.
- Decrease IT and helpdesk support costs by reducing your attack surface and password reset related tickets.
- Provide simplified access for today's hybrid workforce.
- In conjunction with strong MFA, help adhere to compliance regulations by reducing risks associated with credential compromise and breaches.
- Help transition to passwordless user authentication to further mitigate risk of stolen credentials, since there is no password to create and use at all.

To move an application into the zero trust architecture, three conditions must be met:

1. Integrate with strong authentication (phishing-resistant authentication methods like WebAuthn or others).
2. Ensure anywhere access to any application (public or private), with or without a VPN (such as a remote access proxy).
3. Unify how users launch the application (typically with an SSO portal).

As organizations often have hundreds or thousands of applications, and as activities change over time, the process of identifying and integrating applications with the zero trust architecture is ongoing. Establishing a clear and deep understanding of the applications users need to access, from where and when can help them build and configure the right policies.

Objectives

- Risk-rank and prioritize applications based on their criticality to the business and the sensitivity of their data.
- Gain visibility into the devices and applications in use, including controls in place to verify trust.
- Go beyond on-premises applications to include securing cloud apps.
- Expand the scope of applications in the zero trust architecture.
- Ensure continuous validation of access to every application, to prevent authorized access to data.

Transformation

Strategic

Objective: Identify the applications employees require access to and types of access based on their role, access location, and risk profile.

Is there an existing strategy on secure application (both public and private apps) access?

- Identify whether there is a strategy or program for the assessment and control of corporate applications access.
- Establish granular access controls based on the apps being accessed.
- Determine access needs based on types of apps (private, public, or SaaS), user roles, and locations users connect from (on-premises or remotely) and if there is a need to adopt zero trust, VPN-less access to private apps.

Management

Objective: Define how you will assess if application access control policies for the workforce are working as expected.

Is access to applications fully controlled for users?

- Ascertain whether there is a clear inventory of applications.
- Have applications have been assessed as to the level of risk any compromise poses?
- Do you have a way to ascertain the number of internal vs. external users?
- Are policies in place to control the external access to applications and clearly restrict the use of any other assets?
- Is there a governance process to manage the policy update process?

Operational

Objective: Identify the extent to which an access management solution has been implemented across the user base and how effectively it contributes to the rest of the security function.

What is the user experience when employees are accessing applications via the SSO portal?

- Determine whether the end user will see all applications in a similar fashion.
- Ascertain whether there is measurement of user expectations and approval rating.
- Identify whether improvements and exceptions are reported to a clear owner.

Is passwordless authentication in use?

- Do applications support FIDO2 WebAuthn?
- Do all or groups of user endpoints include support for biometrics (facial or fingerprint)?
- Do all or groups of user endpoints carry corporate or BYOD smartphones to provide biometric (facial or fingerprint) verification as an authentication device?
- Do all or groups of user endpoints have security keys that support FIDO2 WebAuthn such as the YubiKey Bio Series?
- Is Active Directory in use?
- Has an SSO solution been implemented?

Metrics

Risk

- Single sign-on policy coverage for apps
- VPN or VPN-less remote access policy coverage for private apps

Security

- Reduction in compromised credentials

Support

- Reduction in password reset support tickets
- If adopted VPN-less remote access, reduction in VPN related concerns and support tickets

Operations

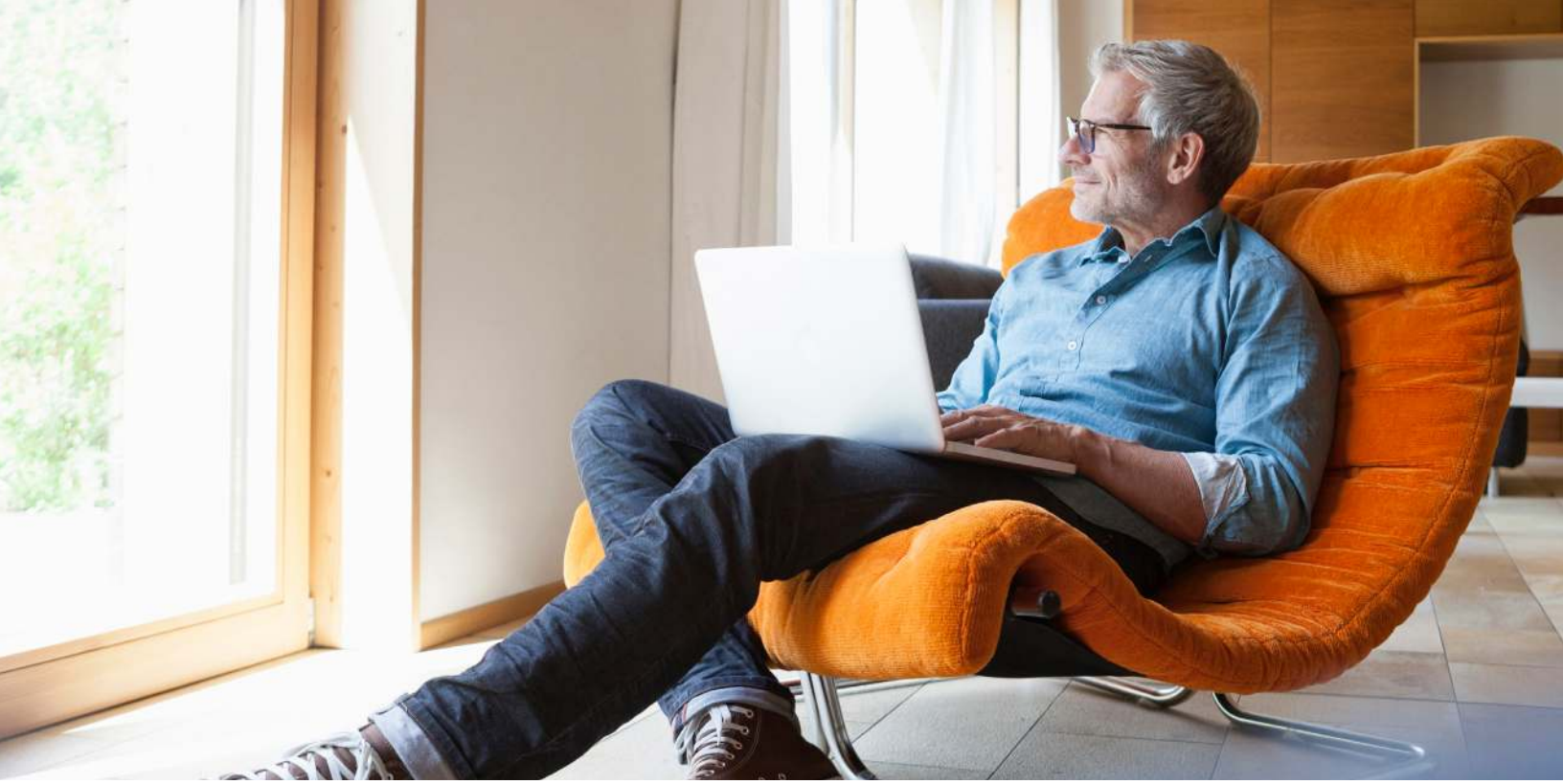
- Single sign-on policies enforced
- Users save time accessing apps with single sign-on portal

Components

Single Sign-On (SSO). Simplify user experience by providing one centralized web portal for access to all applications and resources. SSO complements MFA, strengthening trusted access management and reducing risk of data breaches. By reducing the number of login credentials to be provisioned and managed and by offering multiple self-service capabilities, SSO helps IT and helpdesk teams save time and costs associated with onboarding new users to applications, password resets, device management, and more. SSO enables seamless, trusted access.

Passwordless. Strengthen security while simplifying user experience by deploying passwordless authentication. Bring an end to the well-documented issues with pasword maintenance and weaknesses. On the back end, you will need to ensure applications support the FIDO2 standard. On the front end, make sure access endpoint browsers also support FIDO2 and biometrics. You may also employ vendor solutions that offer alternatives to biometrics on access devices with them on authentication devices (smartphones).

VPN-less (remote) access to private applications. Encrypt session traffic in tunnels from user endpoints to private applications hosted on-premises or in hybrid cloud environments. Enforce the zero trust tenant of “least privilege” by establishing application specific connections that provide only the access required for the user to be productive. Apply that functionality through a proxy host that acts as a gateway between the unprotected internet and those protected environments to provide VPN-less remote access without exposing internal applications. Leveraging such technologies increases security posture while alleviating the burden on hardware and bandwidth employed by traditional VPN access solutions for remote access.



Offer a consistent login experience for users without exposing the surface of sensitive resources unnecessarily and ensure only authorized users can gain access. Integrate access with SSO to improve flexibility, agility, and scalability, enabling organizations to deliver a quality remote application access experience while reducing the risk of attack. Provide access from any device, using any browser, from anywhere in the world with minimal agent installation or configuration on user endpoints, while supporting access over leading service delivery protocols including SSH, RDP, and SMB to server hosts without full VPN deployment.

Challenges

We don't have the IT expertise or bandwidth to onboard applications to SSO. Many teams are stretched thin. They have neither the time nor expertise to easily configure applications with SSO. Fortunately, it's not all or nothing. Start with applications that a subset of users require access to. Steadily increase coverage in a prioritized and systematic way. If needed, get services and support from your SSO solution vendor to be successful.

Why would I want to move away from a VPN which works and I am familiar with to a VPN-less remote access solution? We recognize many organizations already have a VPN in place. But there's no reason to abandon the VPN: it will serve the organization during the gradual transition to VPN-less, and it can serve as a backup to VPN-less remote access.

Phase 4: Enforce contextual access policies

Do you know which applications are mission-critical to your organization? Obviously, those that process or house sensitive data will need more stringent access policies. To manage risk appropriately, implement requirements for access based on the sensitivity of the resources and the known security state of the access device. These policies can range from allowing only corporate-managed devices to requiring certain versions of patched software, encryption, or step-up authentication. Enforce policy compliance based on contextual factors such as user behavior and role, location, and access device. Then, gather insight on the status of operating systems, browsers, and plugins accessing protected resources from connected devices.

Description

Organizations can set policies requiring the use of known and trusted endpoints to access the most critical data and applications (for example, privileged users must use a corporate-issued device). The access proxy takes on the role of enforcing access to corporate resources, regardless of whether users are outside or inside the traditional perimeter. Enforcement strategy is one way we express risk tolerance; right-sizing those policies depends on factors such as sensitivity, threat, user community, regulatory requirements, and other considerations.

A major drawback to the classic network perimeter security model was that organizations tended to have one level of trust everywhere on the inside. Building in different tiers required network segmentation that was often too complex to implement and manage. The zero trust approach separates out levels of trust at the application layer, which is why the phased approach emphasizes determining early on where critical and sensitive data and applications reside. To access these, users and their devices may need a higher level of trust depending on the context, which means they need to pass more stringent tests and comply with stricter requirements.

Set a baseline, then expand

Start with a baseline level of trust for all users and devices regardless of what they're accessing, and then add more to reach the level of risk management needed for access to the most sensitive tiers. We can determine the trust level of users by establishing if this is the first time we're seeing the person, their role and group within the organization, which factors they use to authenticate, the applications they are attempting to access, and if there are signs of impersonation or malicious activity. We can determine the trust level of devices by whether or not it's the first time we're seeing the access device,

if it's company-issued or BYOD, whether or not it's managed, if it's running an up-to-date operating system and web browser, if security features like screen lock and encryption are enabled, and if there are signs of infection or tampering. Using this information, zero trust access policies must be flexible to allow access but nudge for remediation, require remediation to improve trust, step up authentication requirements, or altogether block access as untrustworthy.

Access policies should be granular yet adaptable so organizations can respond to changes in context as needed without introducing unnecessary friction for the user.

Use context to enforce policy compliance

Understanding and applying context is a critical step in the authentication flow. Over time, user and device context changes. For example, users may alter their routine such as logging in to applications at different times. They may move to a new location or assume a different role within the organization, resulting in a change to their user privileges. They may take on a new access device. That device also has its own set of attributes. The operating system, as well as the browser and any plugins, will need to be updated continually to the latest versions to avoid vulnerabilities and the potential for exploit. Access policies should be granular yet adaptable so organizations can respond to changes in context as needed without introducing unnecessary friction for the user. The contextual data on users and their devices gathered during the login process can then be used to assess compliance before determining whether access to applications is granted or denied.

Gather data to gain insight

An effective technique for establishing device context is to gather data at the time of authentication. Doing so provides useful insights into the status of endpoints used to access resources. Information on OS, browser, and plugin type and version, the use (or lack) of disk encryption, screen lock and biometrics, and whether the device has been tampered with (jailbroken/rooted) all serve as indicators of each device's security hygiene. Building an inventory of all devices and the corresponding standing of each attribute paints a relative picture of the organization's overall security posture. The data can be further refined and analyzed to identify specific devices that are susceptible to the latest vulnerabilities and attacks.

Highlight suspicious access attempts

With potentially thousands of login attempts each day, sorting through authentication logs to identify which ones pose a risk is both time-consuming and challenging. To assess risk properly, we need to create a baseline of normal login activity and compare future authentications against our baseline. Those that deviate sharply are surfaced for investigation.

The key to identifying whether a login deviates from the baseline is context. Understanding the context behind why a particular authentication is considered anomalous helps put it into perspective. Contextual factors such as the user's role in the organization, their behavior (when and from where the user is authenticating and what device and factor they are using to authenticate), and the application being accessed provide the details we need to determine whether a login is legitimate or suspicious and requires further action.

The most important thing is to carve away at the devices, software, sources, and behaviors you know you don't want to allow, thereby reducing your exposure to attacks. Changing the security lifestyle of an organization takes dedicated work, but once the controls fit more closely to where they belong — the users, their devices, and the applications — you'll be addressing the gaps in today's traditional security paradigm and moving beyond it.

Objectives

- Establish an enforcement strategy to express your risk tolerance.
- Apply policies to authentication workflows based on trust indicators.
- Take action for the continuously validated people and devices.
- Identify potentially risky access attempts and tighten policies as needed.

Transformation

Strategic

Objective: Identify and establish a clear strategy for asset and user access policy control.

Have policies been implemented to control users' access based upon user and device trust?

- Is there a clear strategy to ensure that access to resources is controlled by policies based on a risk-based decision derived from the context of users, their devices, and the applications they are accessing?
- Identify ownership and responsibility for such a strategy.
- Ascertain whether these policies are being applied in the organization.

Management

Objective: Define how well any adaptive policy is managed and updated.

Are users and devices managed consistently according to policies?

- Has a baseline of trust been established for users, their devices, and the applications they access?
- If policies exist, are they the responsibility of a clearly named owner?
- Ensure that policy controls are clearly defined.
- Identify processes by which policies are implemented.
- Identify any measurements for the implementation of policies.

Is there a process in place to update user privileges?

- Ascertain whether there is a link between policy development and policies managing users and devices.
- Is there a clear set of policies to ensure changes to user and device policies are reflected in the controls upon access to resources?
- Determine whether the output of risk assessments on resources, especially applications, is linked to any policy update process.
- Are policy updates clearly measured and reported?
- Is there a governance process to manage the policy update process?

Operational

Objective: Identify whether there is visibility over users and devices, as well as processes to manage any exceptions.

Is device visibility integrated into other functions?

- Determine whether any solution providing visibility over devices has been implemented.
- Identify potential areas of security and IT that can benefit from device visibility.
- What are the outputs from such a solution?
- In what method and manner are outputs shared with other functions, automated or otherwise?
- Create a benefits statement showing how enhanced device visibility improves delivery in other functions.

Are out-of-policy users and devices identified and reported?

- Determine if there is a clearly defined process for identifying policy non-compliance of both users and devices.
- Determine whether there is a clear reporting of any non-compliance.
- Ascertain whether the policy update process takes into account exception reporting.
- Determine whether there is a clear ownership of exception reporting and actions required.
- Identify whether exceptions are reporting to other IT and security functions.

Is there an exception workflow in place to manage out-of-policy users?

- Determine whether exceptions are recognized and acted upon.
- Identify how the output is integrated into operational actions.
- Is that integration automated or manual?
- Are the processes measured and reported on?
- Is there a clear owner for the process and its continued development?

Metrics

Risk

- Policy coverage for apps
- Policy coverage for devices

Security

- Incident reduction

Support

- Policy exceptions (workflow)
- Policy support tickets
- Policy support satisfaction (NPS)

Operations

- Policies enforced
- Policy compliance
- Accounts – inactive
- Access devices – inactive
- Auth devices – inactive
- Auth devices – shared

Components

Access control engine. The repository of all your access policies, such as "only this group of users, together with their up-to-date, assigned, and managed devices, may use this sensitive application."

Trust inference. Deciding what conditions will cause you to place or lose trust in a device (such as hardware changes). The trust inference engine will rely on a steady input of data from the sources you choose.

Historical authentication analysis. Historical end user telemetry data should be referenced to determine if the current risk profile requires additional verification to establish trust including location, network, impossible travel, operating system, browser type, time of access, authentication methods, and more.

Device insight. Inventory devices at authentication to gather data on operating system, platform, browser, and plugin versions, as well as passcode, screen lock, full disk encryption, and rooted/jailbroken status to identify devices susceptible to the latest vulnerabilities and attacks.

Anomalous authentication identification. Visibility into abnormal access attempts helps to identify potentially suspicious activity, tighten access policies, and aid in investigations around compromised credentials, account takeover, and application access abuse.

Challenges

We can't block users across the organization. Nothing will stop a security initiative faster than halting the organization's work. Start small with policies and perform policy modeling and testing to get the appropriate results.

Our risk management isn't well defined and we haven't agreed on a risk tolerance. Rather than talk broadly about risk reduction, point to specific risks that policy addresses. For example, doctors will not be able to access electronic health records from jailbroken devices. Effective policy is explicit in the threat scenarios it prevents.

IT, security, and the business unit are at odds over the policy. Different stakeholders often have different understandings and different priorities. Given the importance of policy decisions, be sure to include these stakeholders early on in this phase of the zero trust initiative.

Enforcing policies increases our help desk call volume. A key support metric to track is support tickets related to zero trust projects. Use this metric as feedback to lower the helpdesk impact on future projects in the journey to zero trust.

Phase 5: Verify trust continuously

By this point, all applications and systems within scope are covered by the previously listed stages. Monitoring and response to threat scenarios are ongoing. People have a consistent experience across devices and activities. How are you assessing the modern attack landscape as it evolves? Have you created procedures to analyze security logs for vulnerable attack surfaces? How are you strengthening security policies to mitigate modern attacks? Are only strong phishing-resistant authentication factors allowed? How are you training and enforcing users on adaptive policies that may impact their workflow? When developing and implementing security optimization strategies for the workforce, you must consider technologies that accelerate trusted access using a reliable contextualized signal and prepare for the impact it will have on users and administrators. It's time to optimize security by verifying trust continuously.

Description

To optimize security, we must understand the attack landscape. The Verizon 2022 Data Breach Investigation Report listed credential attacks as the top attack surface (followed by phishing, vulnerability, and botnet attacks) and that "82% of attacks involved the human element."[5] As we can see, identity (aka the user or admin) is the new perimeter, and is the first, last, and sometimes the only line of defense an organization has between the attacker and the resources they are targeting. Regardless of the increased risk, 80% of organizations are not prepared to protect themselves against modern attacks.[6] The attackers are successfully finding ways to bypass weaker security implementations in access management controls and are focused on manipulating user behavior through push phishing attacks, man-in-the-middle (MitM) attacks, one-time-password attacks (OTP), and vulnerable device attacks.

Evaluate risk level to establish trust

One method to mitigate modern attacks is the ability to assess authentication requirements using risk-based authentication (RBA). RBA uses a series of signals to evaluate risk during a login attempt and provide the right level of friction for the user based on the corresponding risk level at the point of login. RBA enables security policies and risk signals to work in concert to create an automated and dynamic experience for the end user.

5 https://www.verizon.com/business/resources/Tda1/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

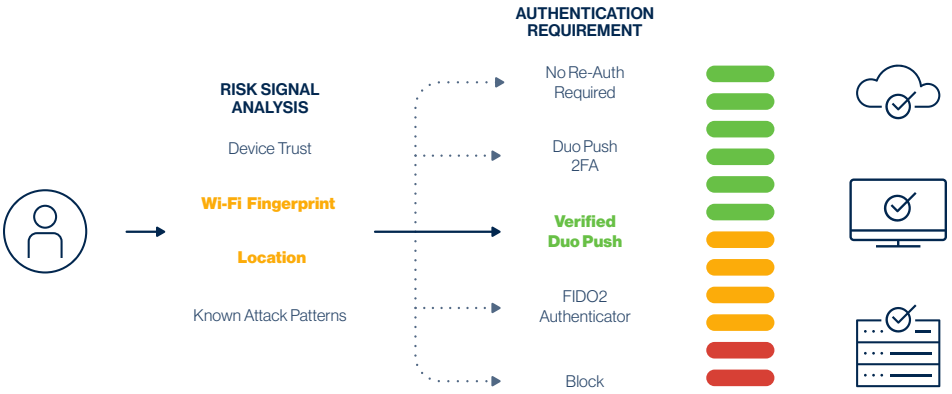
6 https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html

Implementing adaptive access policies is critical to an effective security strategy that helps mitigate modern attacks.

The key to context: shared signals

Implementing adaptive access policies—policies that adapt to changing user posture and device hygiene—is critical to an effective security strategy that helps mitigate modern attacks. The signals used to determine risk should not rely solely on unreliable signals such as IP address. They should instead rely on contextual signals such as user location (end-user data collected to determine location risk should be anonymized but provide a high level of assurance on location) and network, device attributes (OS and browser version, firewall, security settings), XDR/Anti-Virus status, and management status coupled with signals from known attack patterns provide information to evaluate a user's risk level.

How adaptive access works. In real time, a decision engine analyzes risk signals and decides where the authentication falls in the trust spectrum. If a user logs in at their normal time and location on their corporate device, the decision engine would label it as "high trust" and not add extra steps to the login process. However, if the decision engine deems the authentication to be "low trust," the user may be required to take additional security measures. These may include remediating a non-compliant device, using a more secure authentication factor, or entering a verification code as an additional step during the authentication process.



Trust is ephemeral, constantly verify it

Assessing risk level to determine trust doesn't stop at the time of authentication. It should be continuous across the user's session. At the point of authentication trust is high. However contextual conditions can change and erode confidence in trust. For example, the user may join a different network, or the access device may fall out of compliance with one or more policy attributes.

Organizations should create policies that reflect their trust tolerance. If a user's trust does not erode below the established threshold, the session is extended. This decreases the time spent authenticating and improves user experience and productivity. If the risk signals indicate a drop in trust below the threshold, the new risk level should be communicated to the user, who can then take steps to remediate and reauthenticate so trust is restored. Continuously adapting to changes in user context between authentications provides an additional layer of security.

Objectives

- Identify critical access applications and users.
- Identify vulnerable attack surfaces.
- Tighten security policies to mitigate modern attacks.
- Train users on strong authentication factors that are phishing-resistant.
- Apply policies to authentication workflows based on trust indicators.
- Act to continuously validated people and devices.
- Log all authentication and security events.

Transformation

Strategic

The objective is to ascertain whether a zero trust strategy being implemented achieves the benefits, and to identify if there is a clear alignment of a zero-trust strategy with the IT and business units.

Is there a clear statement of benefits that zero trust delivers to the overall IT and business strategy?

- Identify whether there is a clear zero trust strategy with a set of principles.
- Does the strategy have a clear statement of what benefits are expected as a result of implementing that strategy?
- Is there a clear link between the strategy and the organization's IT and business strategy?
- Identify ownership and responsibility for the continued development of such a strategy.
- Are benefits measured and reported in a systematic manner?

Management

The objective is to define how well any zero trust strategy has been implemented.

Has a clear zero trust architecture been defined and implemented?

- Does the strategic architecture cover the organization's total IT environment?
- Discover the extent to which the architecture has been implemented.
- Identify processes by which architecture is reviewed and improvements or adaptations identified.
- Can the environment's benefits get measured and reported in a systematic manner?
- Does an inventory exist of all apps, with documentation noting: what the apps are used for; who needs to access them and why (use case); and what level of access is required for workers to do their jobs?

Operational

The objective is to identify whether the zero trust strategy has been implemented to improve end-user experience while reducing security risk.

Is continuously verifying trust integrated into other functions?

- Determine whether any solution providing adaptive access has been implemented. What are the outputs from such a solution?
- Identify potential areas of security and IT that can benefit from continuously verifying trust.
- Are logs being examined for vulnerable attack surfaces? In what method and manner are outputs shared with other functions, automated or otherwise?
- Create a benefits statement showing how enhanced device visibility improves delivery in other functions.

Are all use cases mapped to ensure all critical access applications require continuously verifying trust?

- Determine if there is a clearly defined process for identifying policy non-compliance of both users and devices.
- Determine whether there is a clear reporting of any non-compliance.
- Ascertain whether the policy update process considers exception reporting.
- Ascertain whether there is a clear ownership of exception reporting and actions required.
- Identify whether exceptions are reporting to other IT and security functions.

Is there an exception workflow in place to manage out-of-policy users?

- Determine whether exceptions are recognized and acted upon.
- Identify how the output is integrated into operational actions.
- Is that integration automated or manual?
- Are the processes measured and reported on?
- Is there a clear owner for the process and its continued development?

Components

Continuous trusted access. Continually establish trust by analyzing contextual attributes gathered at the time of authentication and in mid-session to assess user and device risk and adapt access requirements in real time. For example, administrators can require users to self-remediate a risky login by invoking a verified push as an effective defense against "push harassment" attacks.

Wi-Fi profile analysis. Detect and assess user context outside of traditional mechanisms like IP Address such as using a user device's Wi-Fi profile (or Wi-Fi Fingerprint). Using such a profile to intuit working location and detect changes to that location when the Wi-Fi Fingerprint varies is an innovative approach to assessing risk.

User privacy is a key consideration when deploying security controls – particularly those that analyze location data – so ensure that vendors anonymize this information.

Hygiene and posture analysis. Devices that have successfully authenticated should be analyzed continually to ensure a device hygiene or posture change doesn't create a security risk. For example, a user's device firewall is disabled in the middle of a user session which requires the user to address the issue before re-gaining access, or XDR/Anti-Virus detects a high-risk security issue with the device.

Metrics

Risk

- Assessment of risk at login
- Assessment of risk continuously throughout the user session lifetime
- Assessment based on dynamic contextualized signals

Security

- Incident reduction of compromised credential attacks, MFA phishing attacks, and vulnerability attacks

Support

- Threats mitigated by RBA and continuously verifying trust
- Threats found to be false positives or false negatives

Operations

- Critical apps requiring strong phishing-resistant authentication methods, risk-based authentication, and continuously verifying trust

Challenges

We have legacy technology. Many organizations have to support technology that's years or decades old. Not everything has to plug into the zero trust architecture. The objective is mindfully moving workflows into the security model to reduce risk and improve security where it makes the most sense. If you can segment or modernize legacy applications to minimize risk, it should be done so effectively.

We don't see value in zero trust. In the latest Cisco Security Outcomes Study, respondents with mature zero trust implementations boosted their security resilience rating by 30% over organizations that haven't started that journey. Furthermore, zero trust correlated with significantly higher success rates for eight out of nine security resilience outcomes we discussed earlier.

There's no trust for zero trust beyond the board room. While most CISOs are bullish about zero trust because it helps increase urgency and attention for security investments, IT practitioners remain skeptical. To build trust for zero trust, remember that everyone is an end user. Prioritize solutions that eliminate unnecessary decisions, deliver consistent access, and respect user privacy. That's where trust begins, with the end user.

Next steps

The iterative approach detailed in this guide results in transforming one aspect of the organization's IT into a zero trust model. The final phase is integrating that aspect into the broader organization-wide zero trust architecture. The integration and move to continuous improvement must result in a consistent experience for end users, IT administration, and security operations.

This final step begins with a look backwards. Ask these questions:

- Were the success criteria met?
- Did the zero trust initiative produce the expected results?
- Did the initiative align with the organization's strategy and design principles?

The gaps between the expectations and results – both positive and negative – point to areas to explore for lessons learned. By measuring and reporting benefits and results in a consistent way, we can compare the individual initiative to the collection of initiatives in the transformation, providing another area to explore for lessons learned. By looking backwards, we can better prepare for future initiatives, thus accelerating the overall transformation process.

Pro-tip: Leverage reference architectures

There are many varieties to choose from, but we recommend the Cybersecurity Infrastructure and Security Agency (CISA) Zero Trust Maturity Model. CISA's Maturity Model for Zero Trust reflects the reality that zero trust security is an ongoing quest, not a "one and done" project. Using this model allows teams to assess where they are, where they have gaps, and how to make progress.

The CISA Maturity Model offers organizations a roadmap for adoption of zero trust controls across these domains:

- Identity
- Device
- Network (or environment)
- Applications (or workloads)
- Data

Across each of these domains are capabilities such as visibility and analytics, automation and orchestration, and governance (or compliance). Additionally, there are maturity levels based on the strength of the control or the way it is deployed: traditional, initial, advanced, and optimal.

Cisco architectural frameworks and design guides

Cisco offers several reference architectures, frameworks, and design guides, including for zero trust. The Cisco Security Reference Architecture provides an overview of the Cisco Secure portfolio, commonly deployed use cases, and the recommended capabilities within an integrated architecture. The reference architecture covers the domains that align closely with industry security frameworks such as NIST, CISA, and DISA. Additionally, our Zero Trust User and Device Security Design Guide provides a map of business flows to analyze and identify threats, risks, and policy requirements to guide application of the specific capabilities necessary to secure each flow.

The quest continues...

Finally, we recommend maintaining ongoing operations and enabling future iterations of your zero trust initiative. Tracking the metrics along the entirety of the zero trust architecture provides visibility into what is working and where improvements are needed. The individual initiative we tracked through the five phases is at an end, and it's time to hand it off to operations for ongoing support and improvement. Future initiatives will continue the momentum, moving more of the organization's people, devices, and applications onto the zero trust architecture.

Summary

This guide has laid out the journey for a zero trust transformation focused on securing user and device access to applications. One key to success is specificity. Define the scope or your implementation around a specific activity, that is, a set of applications used by a specific set of users, completed in support of an organization's function. Be specific in the threat scenarios that we're avoiding by requiring people and devices to establish trust. Another key to success is iterating. Launch an initiative to transform one activity on to a zero trust architecture. Learn along the way, and then repeat.

For decades, we have discussed eliminating excess trust. We have debated telemetry and monitoring techniques to continuously evaluate trust. Finally, in recent years, technology has caught up with the philosophy. By following the steps in this guide, your organization can implement these ideas with off-the-shelf software at a sustainable pace. The zero trust revolution is well under way. Join in.

About Duo Security

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and trusted access provider. Duo comprises a key pillar of Cisco Secure's zero trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo's flexible solutions offer dynamic cyber security, adapting to changing threat landscapes faster with full-scale visibility, unmatched reliability, and intuitive user interfaces. Try it for free at duo.com/trial.

For more details on Duo editions and pricing, click here.