elegancegroup

ATLASSIAN

Understanding Zero Trust Security

Where to start & why it matters

Table of contents

For decades, enterprise security controls were built to protect a large, single perimeter around a corporation. Often described as castle-and-moat security, this approach is based on the principle that the perimeter (or moat) should protect everything within its bounds, and everything inside the network is trusted by default.

This model worked for environments in which applications are hosted on-premise. But castle-and-moat doesn't stand up to the security threats posed by the proliferation of cloud applications, devices, and logins.

The corporate technology space has changed dramatically since the days of castle-and-moat. That change brought the need for a new approach to workplace security. Enter Zero Trust - the new security model industry experts have turned to that addresses the growing security challenges in the modern workplace.

In this paper, we will review the current state of workplace security, the basic principles of the Zero Trust security model, and how you can begin your journey towards a Zero Trust-secure workplace environment.

A new, perimeter-less workplace

It has become increasingly difficult to secure the critical systems, data, and employees that allow companies to successfully operate. Several converging trends in the IT space are to blame.

According to a McAfee survey, the average enterprise employee is using 36 different SaaS apps, and the average enterprise company uses over 1900 different cloud services. In the past, data was consolidated in a handful of enterprise applications, but with the implementation of highly specialized SaaS apps for every type of team, market, and data type, the number of apps that need to be monitored and secured is growing exponentially.

Not only are there more apps available that need to be protected, but there are also ever-increasing ways to access these applications from mobile and personal devices. In a traditional, on-premise environment, most users would only access their work applications at the office, and if they happened to work from home, they would access their work applications using a VPN. The growing adoption of mobile devices, remote work, and BYOD (bring your own device) in the workforce has complicated the barrier between work data and personal data. The increasing relevance of external devices has expanded the necessary security perimeter outwards, making governance and perimeter security much more difficult.

Both of these industry trends fundamentally change the task of IT security. In this new landscape of applications and access points, maintaining a strict security perimeter is nearly impossible.

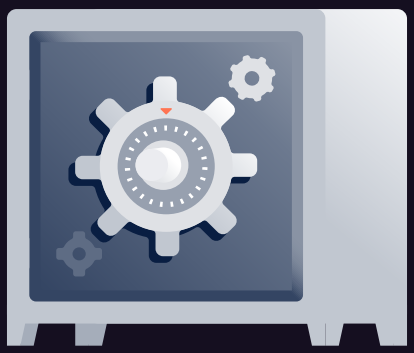
The increased difficulty of maintaining a perimeter renders the castle-and-moat security model obsolete. Because the model was only designed to protect the perimeter, it doesn't provide for ongoing threat detection mechanisms inside the the perimeter. Once the perimeter is breached, an attacker can easily move across security layers and systems. Threats that get inside the network are not immediately identified, and can easily extract sensitive, valuable business data.

Guiding principles: Zero Trust

As the castle-and-moat model diminishes in usefulness, many experts have turned to a Zero Trust model for security in a cloud-oriented environment.

At its core, Zero Trust is a framework in which an organization forgoes one large perimeter in favor of protection at every endpoint and for every user within a company. This approach relies on strong identity and authentication measures, trusted devices and endpoints, and granular access controls to protect sensitive data and systems. The primary principles of Zero Trust are:

- Never trust, always verify: Do not inherently trust anything on or off your network. If you accept that you can't control every IP address and every device, the result is that you can no longer assume trust within the network perimeter.
- Grant access based solely on the identity and device of the user accessing the application, regardless of a user's network location–be it an office, a home network, or a coffee shop. You need to know that the user requesting access to a resource is who they say they are, and you need to verify that they are allowed to access that particular resource.
- Access controls are dynamic and must be continuously verified. In a zero-trust environment, consistent authentication and authorization checks are essential for maintaining security.



Get started with Zero Trust

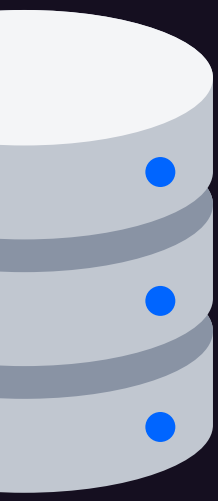
Identity and authentication

Identity authentication is the foundation of a zero-trust security strategy. To continuously evaluate access to resources, you must first centralize user management and establish strong authentication processes.

In order to track and manage all users across your systems, user identity must be centralized in a user and group directory. Ideally this database system integrates with your HR processes that manage job categorization, usernames, and group memberships for all users. As employees join the company, change roles or responsibilities, or leave the company, these databases should update automatically to reflect those changes.

The user and group database acts as the single source of truth to validate all users that need to access your systems. A single sign-on (SSO) system, or centralized user authentication portal, can validate primary and secondary credentials for users requesting access to any given resource or application. After validating against the user and group directory, the SSO system generates a time-sensitive token to authorize access to specific resources.

A centralized user database supporting a single sign-on system is essential. Data in a SaaS application environment must be assumed vulnerable unless access is limited to an endpoint that you control. Once that database is in place, you can introduce an authentication process such as 2FA (two-factor authentication) or MFA (multi-factor authentication) to harden your system and ensure that the users accessing your applications are who they say they are.



Device authentication

Like identity authentication, device authentication uses a centralized database to manage which devices can access which systems. The Zero Trust model relies on two primary device databases. The first is the Asset database, which verifies ownership of a device. The second is the device posture assessment, which determines compliance before providing access. All devices must be uniquely identified and referenced to their records in these databases before being granted access to a system. This is often accomplished with a PKI (public key infrastructure) to create certificates that are unique to each device. To receive a certificate, a device must be both present and valid in the Device Inventory Database. The certificate is typically stored on a hardware or software Trusted Platform Module (TPM) or on a qualified certificate store.

As mentioned earlier, most users typically access their work applications from many different devices. The first step in securing these entry points is to identify the risk associated with each platform and, with cross-functional input, decide on the security measures necessary for each platform. This framework informs which devices qualify as 'managed devices' and, in turn, how each device is monitored and authenticated. To simplify device management, many organizations maintain 'service access tiers' to establish standard levels of security requirements for common device types.

Here is an example of how Atlassian has organized their service tiers:

Tier	Platform	Security Requirements	Application Criteria
OPEN	All platforms	Must comply with acceptable use policies	Service does not store or grant access to any personal identifiable information (PII), user generated content (UGC), or IP.
LOW SECURITY	Personal mobile	• Management agent (MDM) must be installed • Password-protected screenlock • Operating system must be up-to-date, no end-of-life or out-of-date versions • Local drive encryption • Malware protection • Device is not rooted/ jailbroken	**Apps in this tier can:** • Store or grant access to staff PI • Be used for basic collaboration (chat, email, Intranet) • Act as repositories for unstructured corporate data (Dropbox, Google Drive) **Apps in low tier can do these but where possible should be allocated to High:** • Store financial, legal, or security information • Store information related to product development • Store information related to product/ corporate development **Apps in this tier cannot:** • Store or grant access to user generated content (UGC) • Acquire, store or process credit card and/or payment information • Have privileged or administrative access to Atlassian customer facing systems
	Personal laptops and desktops	• Enrolled in management platform • Password-protected screenlock • Operating system must be up-to-date, no end-of-life or out-of-date versions • Local drive encryption • Malware protection	

Tier	Platform	Security Requirements	Application Criteria
HIGH SECURITY	Mobile	Bring your own device (BYOD) is not permitted in the high security tier	**Applications in this tier can:** • Store or grant access to user generated content • Acquire, store or process credit card and/or payment information • Have privileged or administrative access to Atlassian customer facing systems
	Corportate laptops and desktops	• Enrolled in management platform • Atlassian owned & managed asset • Approved contractor devices • Password-protected screenlock • Operating system must be up-to-date, no end-of-life or out-of-date versions • Local drive encryption • Malware protection • Adherence to password policy • Ability to do forensics on the device in the case of security incidents	

Building on this foundation, you can begin device health checks using authentication and tracking tools such as mobile device management (MDM), SSO platforms, and multi-factor providers like Duo. These providers enable you to gain visibility into devices being used to access corporate applications, whether or not the device is corporate-managed. From there, you can continuously inspect all devices used to access corporate applications and resources, to determine their security posture and trustworthiness. If any devices are being used in a way that falls outside of their service tier, you will be able to identify that device and work with the employee to secure that endpoint.

Access management

Building on the identify and authentication mechanisms, the next step is to define and implement policies around who can access specific data and when they can access it. What makes the Zero Trust approach unique is that in order to minimize the 'perimeter' of any given individual and isolate the risk associate with that user, the Zero Trust approach supports the idea that an employee should only be given the minimum access and permissions needed for that employee to do their job. By limiting access in this way, risk is minimized. Should an attacker gain access to the credentials of a user in marketing, for example, that perpetrator is 'laterally' limited in that they cannot gain access to any of the tools, assets, or information outside of that user's specific role.

There are several ways to ensure that an employee's access is restricted to the tools and assets required for their job. The first is granular, role-based access and permission levels. These should be defined for each role within your organization, with cross-functional input agreement. Your organization's appetite for risk and the breadth of access needed to effectively collaborate across teams will determine the level of granularity needed for team and individual role-based access levels. Once these role-based access levels have been defined, you can begin to map out the controls needed for each system and vendor in your organization. While your SSO or identity provider may be able to support some of your access control needs, you may find that not all applications provide the level of granularity needed to limit access in this way. Access controls are an important part of any vendor risk management assessment and integral to the long-term implementation of Zero Trust.

In order to the adhere to the 'continuous verification' tenant of the Zero Trust model, you will also need a way to consistently analyze audit logs to verify access controls and identify suspicious or unsanctioned activity in your systems. This information helps detect suspicious activity within your systems and supports the application of access and permission levels by allowing you to verify that those levels are implemented correctly and that there aren't any suspicious actors that have gained access to a user's credentials.