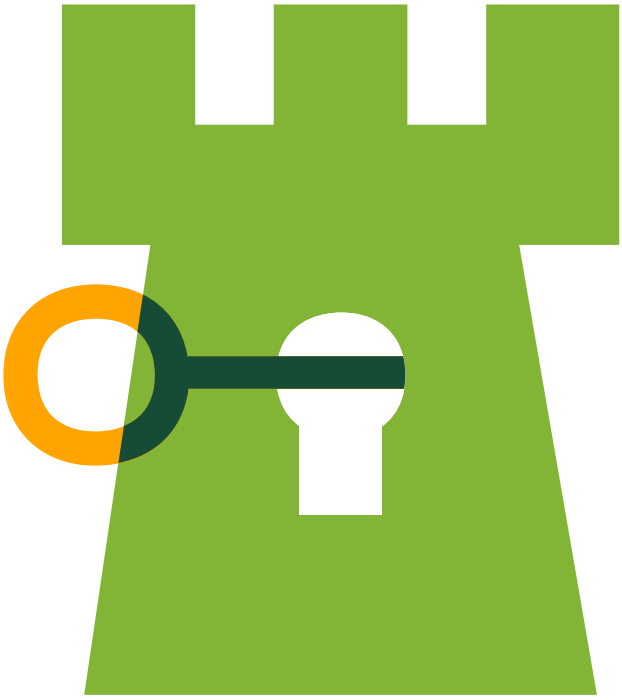


ATLASSIAN

Understanding zero trust security

Why it matters and where to start

Table of Contents

Traditional on-premises enterprise security controls were built to protect a single perimeter around a corporation; this was effective when applications and employees were centralized within the walls of an organization's perimeter.

This approach is based on the principle that the perimeter should protect everything within its bounds, and everything inside the network is trusted by default. This approach didn't stand up to the security threats posed by the proliferation of cloud applications, devices, and multi-cloud environments. The corporate technology space has changed dramatically as organizations switch to hybrid work locations, requiring flexibility for users to access an organization's data with unmanaged personal devices. These changes and the pressures from evolving regulatory compliance requirements have become a forcing function for organizations to adjust their approach to workplace identity and access management (IAM) security.

To address the growing security challenges of modern workplaces, organizations of all sizes have adopted a zero trust approach to cloud IAM. In this paper, you'll:

- Uncover the current state of workplace IAM and the common challenges that have made securing users and data difficult at scale
- Learn the basic principles of the zero trust security model
- Dive deeper into the zero trust best practices you can implement across your organization to strengthen your cloud security posture

Keeping pace with the evolving workplace security landscape

It has become increasingly difficult to secure the critical systems, data, and users that companies need to successfully operate. Across all industries, the number of apps that need to be monitored and secured continues to grow exponentially. This makes it challenging for organizations to scale users securely and apply data controls effectively. In a study, **59% of IT professionals reported SaaS sprawl challenging to manage**. As your organization scales, so do error-prone manual tasks, and the risk of compromise through poorly managed authentication policies. Teams want to use tools that help them work faster and more efficiently and may seek out their own solutions without IT's knowledge or approval. Known as **shadow IT**, these unmanaged cloud instances often don't follow central IT's security protocols and can leave the entire organization vulnerable to attacks.

76% of SMBs admitted shadow IT posed a moderate to severe cybersecurity threat to the business.

Keeping all the risks in mind, your growing organization can't afford to compromise innovation for security. Instead, your business must find ways to adapt to the evolving threat landscape with security best practices that encourage innovation. In a traditional, on-premises environment, most users would only access their work applications through company owned devices at the office. The growing adoption of mobile devices, remote work, and bring your own device (BYOD) in the workforce has complicated the barrier between work and personal data. In a report, **82% of organizations surveyed allowed some BYOD usage in the workplace**. It is important to set controls that encourage frictionless collaboration for users anywhere and on any device.

For organizations to be successful in this new hybrid or cloud-first model and to be able to adapt to a constantly evolving operating environment, they need to go beyond the traditional perimeter approach to balance flexibility with stronger security controls to secure users and their data. This means incorporating processes and policies to protect users, detecting and addressing risky behaviors, and having plans in place to respond in the event of a data breach.

Zero Trust Principles: A scalable approach to cloud IAM

Taking a zero trust approach to IAM requires your organization to implement several changes across people, processes, and technology.

Zero trust is a framework in which an organization forgoes one large perimeter in favor of protection at every endpoint and for every user accessing your data. This approach relies on strong identity authorization and authentication measures, trusted devices and endpoints, and granular access controls to protect sensitive data and systems.

To better understand how to implement a zero trust approach at your organization, let's explore the core principles of zero trust:

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.

Follow the principle of least privilege

Reduce the risk of a successful attack by minimizing access privileges to sensitive data and applications. Set policies that require users to request up-leveled access to data with justification for the request. Maintain least privilege by scheduling frequent permission certifications to confirm if the user still needs access to sensitive data and automate user lifecycle management to remove access once a user moves departments or leaves the organization.

Assume breach

Reduce risk by continuously monitoring your actions across the organization. In a zero trust environment, consistent authentication and authorization checks are essential for maintaining security. If anything is abnormal, have processes in place to detect and respond accordingly.

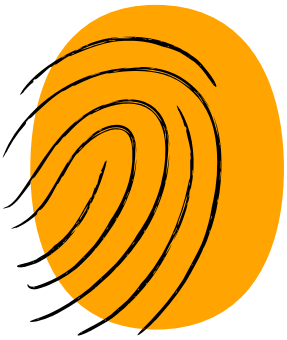
With these principles in mind, it is also important to monitor user behavior and grant access based on several factors presented by the user, including: the user's device, location, time of day, IP address, and the sensitivity of the data in that application. Regardless of a user's network location – 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.

To continuously evaluate access to resources, your organization must centralize access management, establish strong authentication policies, and implement IAM best practices organization-wide.

Centralize access management

In order to track and manage all users across your systems, user identity should be centralized in a 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. When these systems are properly integrated with your **user lifecycle management processes** you can minimize risk by automatically removing permissions that allow access to sensitive data when they are no longer necessary for users. By centralizing access management, you significantly reduce the risk of overprivileged access and time spent on manual administrative tasks.

Establish strong authentication policies



74% of all breaches include human element via error, privilege misuse, stolen credentials, or social engineering. Combat these risks by implementing IAM best practices such as requiring additional layers of authentication for every user. Require your users to authenticate using **single sign-on (SSO)**, to improve both security and user experience. Requiring SSO authentication helps 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. Next, you can introduce an authentication process such as **two-factor authentication (2FA)** or multi-factor authentication (MFA) to harden your system and ensure that the users accessing your applications are who they say they are. Further customize your **authentication policies** to set session duration limits, password requirements, and **API token controls**.

As an organization, it is important to understand how users will interact with your applications and data. You should also take into account that some users may be external to your organization, such as partners, vendors, or customers. Once you understand your external user needs, you'll need to map out unique permissions for all users groups. Finally, create clear policies to limit their access down to what is strictly necessary for successful collaboration.

Identity and access management best practices

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 risk associated with any given 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. This is the principle of least privilege, in other words, by limiting a user's access to the data that is required for their job tasks, you can significantly reduce the risk of damage or data loss if their credentials are compromised or they attempt to carry out a malicious insider attack. Should a bad actor 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.

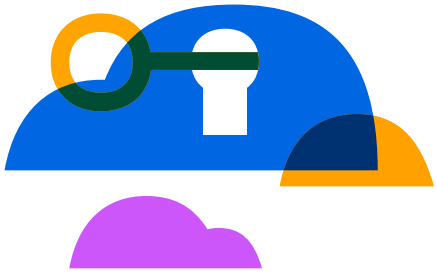
There are several ways to ensure that an employee's access is restricted to the tools and assets required for their job. The first is granular, role-based access and permission levels. These should be defined for each role within your organization, based on your organization's security best practices and the breadth of access needed to effectively collaborate across teams to determine the level of granularity needed for team and individual role-based access levels. Once these role-based access controls have been defined, you can begin to map out the additional controls needed for each system and vendor in your organization.

Add another layer of controls using mobile security settings such as **mobile device management (MDM)** or **mobile application management (MAM)** to control access to sensitive data on mobile devices. While your 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 to meet your requirements.

Access controls are an important part of any vendor risk management assessment and integral to the longterm implementation of zero trust.

In order to the adhere to the never trust, always verify 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.

Implementing the zero trust security model is an iterative process that involves changes across people, processes, and technology in order to be successful. For many organizations, getting started with a foundational zero trust approach can help significantly reduce risk to users and data in the cloud. From there, your organization can continue to mature its security posture over time and incorporate policies that encourage collaboration, improve user experience, and protect your data.



Protect your users and data in Atlassian cloud

Beginning to implement the foundational elements of zero trust security is the key to securing your sensitive company data in the midst of the proliferation of cloud applications, devices, and user identities. Learn more about how you can take a zero trust approach in Atlassian cloud with Atlassian Guard.

Learn more at
Atlassian Guard: Enhanced Cloud Data Security & Governance

ATLASSIAN