

The Zero Trust Guide To Securing Contractor Application Access





I. Executive Summary

Providing application access to collaborators outside your organization – whether they’re contract workers, agencies, or partner organizations – can be a security risk and a considerable logistical headache. Many modern apps are not compatible with traditional identity and access management (IAM) platforms, forcing reliance on makeshift systems that are difficult to manage.

Zero trust network access is a way to overcome these challenges by applying the principle of least privilege to business-critical applications. By applying microperimeters around each application, hiding applications behind encrypted connection tunnels, and logging every request, organizations can simplify processes around IAM, free up valuable development time, and significantly reduce opportunities for data loss.

PART 1

The Principle of Least Privilege: Goals and Challenges

Access control is one of the most fundamental objectives of any enterprise security program. In order to protect proprietary data, critical systems, and product quality, security leaders work to implement the principle of least privilege (POLP), which requires that users only have access to the resources they need to perform their job and that their access be limited to the duration for which it is needed.

This goal is particularly important in the case of contractors, vendors, partners, and other trusted third parties. These users are often brought on board to complete specific tasks or projects, meaning their access should be managed with particular care.

In theory, IAM platforms help organizations implement the POLP in these circumstances by:

- Defining known lists of users (directory)
- Facilitating their access based on defined criteria (authentication)
- Limiting their privileges to what they should be able to access (authorization)
- Adjusting their access to specific resources periodically (lifecycle)

Unfortunately, IAM often looks different in practice. Below we discuss some of the challenges for achieving these goals.

Challenge No. 1: Integrating diverse applications with one IAM system

Most large organizations operate a complex, heterogeneous application and infrastructure environment. Certain software-as-a-service (SaaS) and on-premises apps are a good fit for IAM platforms' standards-based authentication methods, but many applications are harder or impossible to integrate with these platforms. Gartner estimates that currently, only 30 percent of single sign on transactions use modern identity protocols like SAML, OAUTH2, and OIDC 1. The other 70 percent of non-standard transactions involve legacy protocols or custom frameworks that aren't easy to integrate in traditional IAM platforms, and require extra time and development effort to secure. Common applications that fall into the latter category include:



- **Internally hosted applications**
(including internally developed private apps and privately hosted cloud apps)
 - Atlassian apps
 - Drupal
 - Grafana
 - JIRA
 - Splunk
 - DataDog
 - Gitlab
 - Bitbucket



- **Infrastructure**
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
 - Microsoft Azure

To overcome these difficulties, organizations typically fall back on the following approaches:

Method	Challenges and risks
Administer separate usernames and passwords for applications that don't work with the central IAM platform	The organization has another set of user identities to manage, onboard, and offboard.
Deliver applications via a virtual private network (VPN).	The organization must punch a hole in its network firewall to provide users access with a VPN or a remote VPN agent.
Build and maintain custom software on private application servers to enable single sign-on (SSO).	The organization must allocate considerable ongoing effort from developers.

Challenge No. 2: Third-party users bring unique complexities

External users bring further challenges still. Since these users often work remotely or on a temporary basis, security leaders typically fall back on the following approaches, both of which are difficult to implement and potentially insecure:

Method	Challenges and risks
Administer VPN to third party users	<ul style="list-style-type: none"> • Time-consuming and expensive to administer to new users - especially if it requires issuing physical machines to contractors • Risk of lateral movement once a user is connected • Risk of data loss, since users can save personally identifiable information (PII) to personal computers
Create corporate user identities for third party users	<ul style="list-style-type: none"> • Time-consuming manual process to provision user accounts to the right resources • Organization becomes responsible for managing account onboarding, offboarding, and permissions, and takes on costs for extra seats in identity management platforms • Additional communication required between departments like HR and IT
Connect your IAM platform to an existing platform managed by the third party	<ul style="list-style-type: none"> • Time-consuming process to integrate platforms and create one-off permission rules. • Potential incompatibility between platforms • Rarely feasible for individual third parties

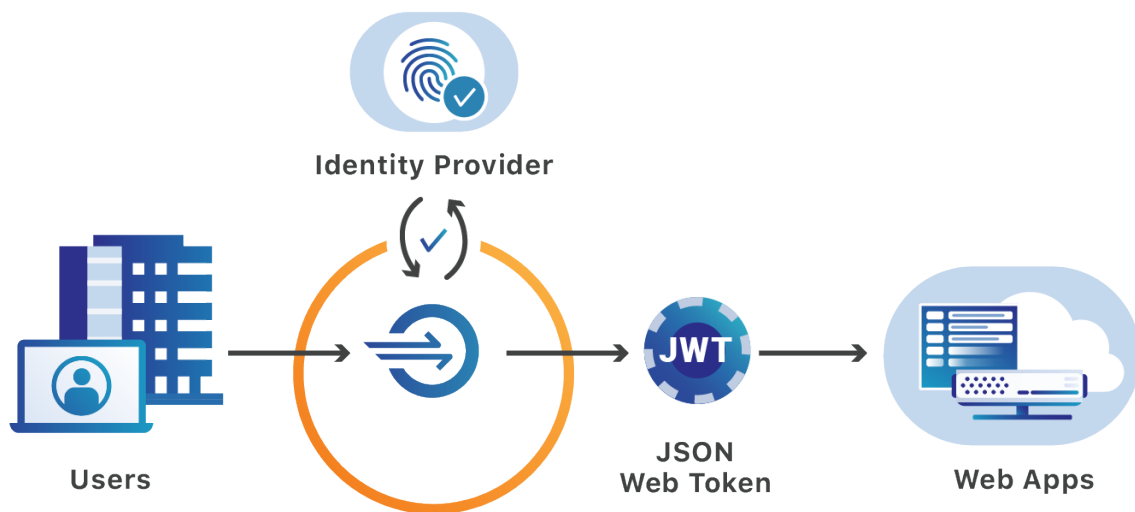
PART 2

The Benefits of Zero Trust Network Access

Zero trust network access (ZTNA) is a framework for overcoming these challenges. It operates on the idea that a company should not trust any user or device at any time, whether they are inside or outside of their perimeter. It alleviates security concerns around third-party access by making access to your internal resources specific, not general.

Zero trust network access accomplishes this by:

- Taking internal applications off the virtual private network and creating a logical access boundary around each of them
- Hiding applications behind encrypted tunnels of connection
- Logging every request made to internal resources (both requests for authentication and requests within the application itself) for increased visibility



These steps effectively allow organizations to apply the granular access controls they have implemented in their existing identity provider to internally-managed applications and infrastructure. It also allows organizations to give third party users access to their internal resources on a per-application level, and to give users from multiple organizations access to internally hosted resources with their own corporate identity.

Here is an example of how this framework can be applied.

Zero trust network access sample use case

Developing new apps and services is a collaborative effort, and many organizations build new products with combined teams of contractors and full-time employees. Protecting an organization's development applications and environments can be challenging if:

- The organization has mission-critical infrastructure (virtual private clouds, for instance) and applications (BitBucket, Git workflows, etc.) that need SSH access
- Product teams are partially remote, including other countries
- Remote developers have access to development environments and applications via VPN, which can slow down connection speed and introduce additional risks

Zero trust network access can address these challenges by:

1. Securing remote access to mission-critical infrastructure
2. Locking down dev and staging sites before they hit production
3. Protecting other internal applications that developers rely on (e.g. GitHub, Jira)

PART 3

Implementing Zero Trust Network Access in Your Organization

Zero trust network access can both secure and accelerate your processes for giving trusted third-party users access to internal apps and resources. Once implemented, third parties do not have to use a VPN to access your applications; they will instead be able to log in with an authentication process your organization defines.

Making changes to your login experience has a major impact on users. Doing it right requires communication and planning across teams. Successful programs often start with a small pilot group of users and one target application. We recommend creating an index of internally managed applications and identifying which ones contractors and other external parties must access.

From there, use the index to identify one application to pilot for ZTNA with a test group. Priorities should be applications that meet the following criteria:

- [Web applications](#)
- [Applications that use HTTPS](#)
- [Not protected with existing SSO providers](#)
- [Used by 5-10% of overall company base](#)

Here is an example of such an index:

Application/ Resource	Who accesses it	Onboarding process today	No. of users impacted	Fit for ZTNA pilot (1-5)
Grafana	Internal - billing dept External - consultants	Azure AD + VPN	45	4
Drupal	Internal - marketing, support External - offshore development	Azure AD + VPN	1000	3
Jira	Internal - all departments External - multiple contracted teams	Azure AD + VPN	10,000	1

After you identify the right pilot application and contractor user group and test the application for right-sizing, consider how you will identify and verify contractors' access to your systems. If you have chosen a strong vendor partner for ZTNA, you will have multiple options for how to deliver access to partners:

Option 1: Allow contractors to log in with their corporate SSO provider

If the external organization you work with uses SSO to provide access to their applications, you may choose to allow the contractors to log in to your application using their own corporate identity.

This approach can be a good fit if:

- You can spend time up front establishing federation between your SSO and the partner organization's SSO
- You want to take advantage of secure access policies like multi-factor authentication (MFA) that have been implemented in the contractor organization's SSO
- You do not want to manage the lifecycle of the contractor identity if they leave your organization: the identity is only valid for as long as the user is in the contractor organization's directory

Example use case:

1. Jose from Company A logs into his CRM platform with his Company A username and password, using SSO.
2. When he logs in to your application, he is redirected to Company A's login page to log in with his corporate credentials.
3. If he is verified by the SSO and has been given application access in your ZTNA platform, Jose can access the application.

Option 2: Use email one-time-PINs to deliver partner login

If you need to give contractors access to a specific application but do not want to establish a federation with another organization's identity provider (IDP), email one-time-PINs (OTP) are a simple method of authentication. With this approach, your organization gives application access to a contractor group with a simple list of email addresses and delivers unique login codes to those users' email addresses every time they need to log in to your service.

This approach can be a good fit if:

- You do not want to issue a corporate IDP account to the contractor
- You do not want to establish a federation with the contractor's own corporate SSO
- You consider email access to be an appropriate trust level for application access
- You are collaborating with contractors from multiple organizations

Example flow:

1. Karen from Company B is working with your marketing team on a new landing page. The staging site is hosted in your CMS.
2. When Karen goes to access the CMS to work on the design, she is asked to enter her email address.
3. When she checks her email, she gets a code that she can copy and paste into the login screen for access.

Option 3: Use an agreed-upon social identity

In some scenarios, you may want to allow contractors to use social identity providers like GitHub or LinkedIn to access your application.

This approach can be a good fit if:

- You are collaborating with users from small organizations that do not use corporate identity management systems
- You need a common framework (GitHub, LinkedIn) to authenticate contractors from multiple different organizations

Example flow:

Robert is a vendor working with your development team to QA a new mobile application. When he attempts to log in to your web application, he is redirected to his LinkedIn login screen. If he successfully logs in to LinkedIn, he gains access to your application.

How Cloudflare can help implement zero trust network access

Cloudflare for Teams is Cloudflare's offering that helps organizations secure their devices, networks, and internal applications. It protects your team's connections on the open Internet, delivers lightning-speed access, and, crucially, allows you to control user access to applications and embrace zero trust architecture.

For more information, and to contact a member of our team, visit teams.cloudflare.com.

Endnotes

1. "Magic Quadrant for Access Management 2019", Gartner, <https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management>, Accessed February 24, 2020



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

© 2020 Cloudflare Inc. All rights reserved.

The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

REV: 200323