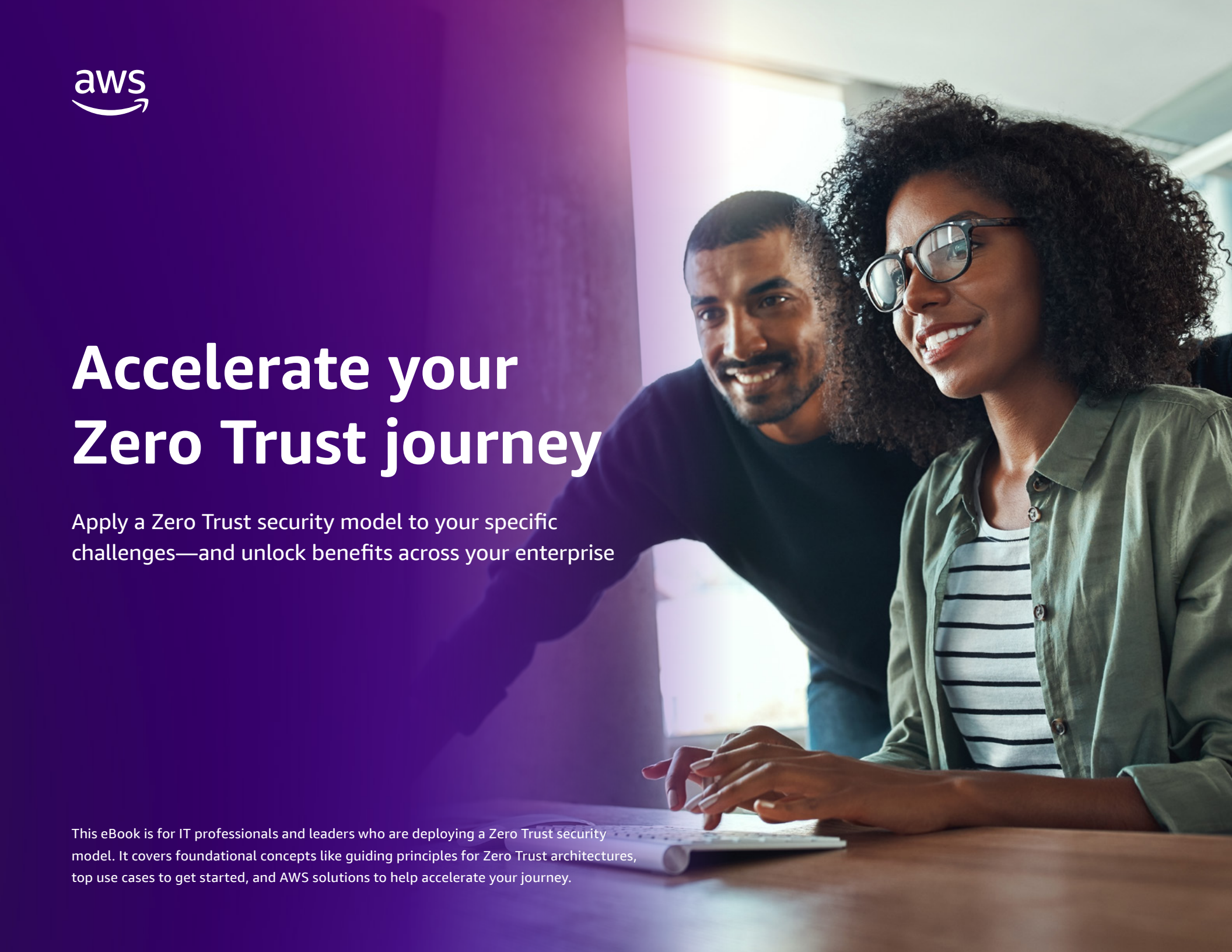


Accelerate your Zero Trust journey

Apply a Zero Trust security model to your specific challenges—and unlock benefits across your enterprise

This eBook is for IT professionals and leaders who are deploying a Zero Trust security model. It covers foundational concepts like guiding principles for Zero Trust architectures, top use cases to get started, and AWS solutions to help accelerate your journey.

Table of contents

INTRODUCTION

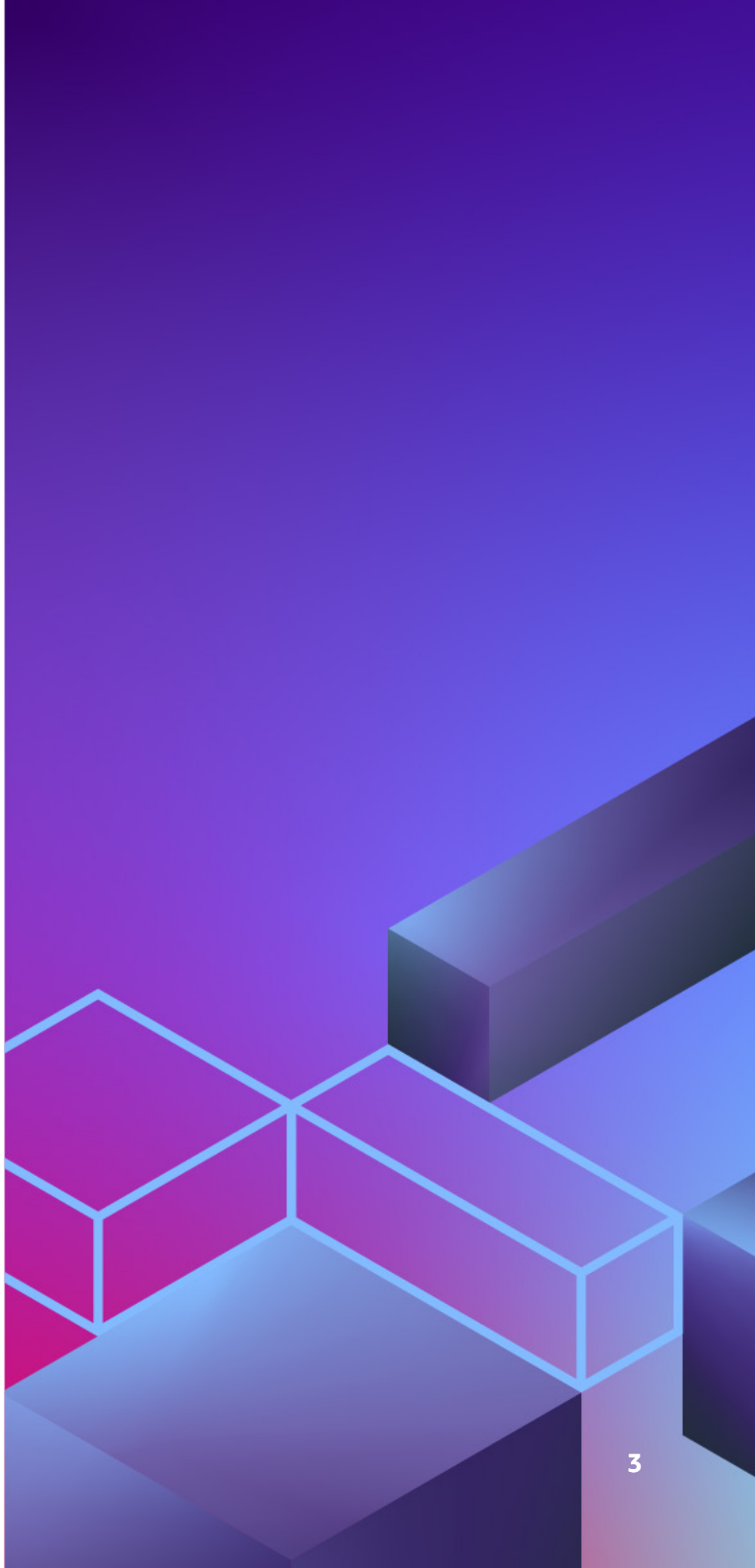
Embracing Zero Trust as a strategic priority

With today's organizations seeking to enhance workforce mobility, strengthen security, and integrate digital technology throughout their businesses, Zero Trust has emerged as a strategic priority. Many organizations are embracing a Zero Trust model to improve or enhance their security posture and controls—while also increasing end-user productivity.

Zero Trust's ongoing evolution has led to a variety of implementations and differing guidance on the best way to roll out this security model across an organization, which has delayed organizations from implementing and reaping the rewards of a Zero Trust strategy. Amazon Web Services (AWS) is here to help accelerate your journey to a Zero Trust security model.

What to expect in this eBook

This eBook offers a wealth of information and guidance for successful Zero Trust adoption. We begin by defining what Zero Trust means for you and your AWS environment. Next, we provide three guiding principles for your Zero Trust journey. We then explore six keys to getting started, followed by an in-depth analysis of three top Zero Trust use cases. Finally, we close with advice on using specific AWS services to maximize the security and productivity benefits of Zero Trust.



Understanding Zero Trust

Traditional security approaches operate under the assumption that any entity entering the network through a secure perimeter can be trusted with broad access to data and applications. Typically, they offer minimal additional defense-in-depth controls.

In today's business environment, however, this assumption is no longer safe to make. In addition, the notion of a "network perimeter" has been blurred by the adoption of cloud-based services and hosted software-as-a-service (SaaS) applications. The Zero Trust security model was developed to help organizations achieve the right levels of security for the modern enterprise environment.

Zero Trust is a security model and associated set of mechanisms that focus on providing security controls that don't solely or fundamentally rely on traditional network controls or perimeters. Put another way, Zero Trust is a security model where access to data and applications is continually assessed and can be further restricted based on factors like who is requesting access to what data using which device and from where. Zero Trust centers on informing intelligent access decisions and enforcing them where they make the most sense for your users and IT teams.

Authorization is key

In a Zero Trust architecture, you have the critical ability to make fine-grained authorization decisions centrally across identity, device, data, and other contextual risk factors. In addition, Zero Trust allows your IT teams to enforce granular, continuous, and adaptive policy-based access control decisions at logical points across your network.

One of the tentpoles of Zero Trust is the idea that when two components do not need to communicate, they should not be able to—even when they reside within the same network segment. Your IT teams can accomplish this by authorizing specific flows between the components, eliminating unnecessary communication pathways, and applying least-privilege principles that better protect critical data.

Zero Trust architectures go beyond simply establishing networking and identity-based controls that work side by side. In a Zero Trust model, network and identity systems are aware of one another, allowing them to work in concert. This helps your IT teams be more exact with access policies and more flexible in where they enforce authorization decisions.

Amazon Virtual Private Cloud (Amazon VPC) endpoints offer a prime example, as they provide private network connectivity to AWS services and allow your IT teams to specify access control policies. These policies and their associated enforcement engine understand the network and the identities accessing it.

Benefits of Zero Trust

Done right, a Zero Trust security model can provide your users and applications with secure, seamless access to the right data while eliminating unnecessary pathways to systems and data. To help raise the bar on security further, Zero Trust also allows your IT teams to make increasingly granular, continuous, and adaptive access control decisions that incorporate a wide range of contexts—including identity, device, location, and behavior.

It is important not to characterize Zero Trust as an effort to meet a checklist of best practices. Instead, a Zero Trust architecture will help your organization realize powerful business and technical benefits—such as stronger protection for your most precious assets, increased productivity, and improved customer trust due to fewer security events. AWS has developed a set of principles that can help guide your way toward unlocking the benefits of Zero Trust.

AWS GUIDING PRINCIPLES

3 guiding principles for your Zero Trust journey

A Zero Trust architecture can better protect your systems and data while improving user experience and productivity. For example, with a Zero Trust architecture, your developers can offload security concerns they previously had to code directly into application logic. Further, they can inherit modern identity management for their application with minimal additional effort.

Here are three guiding principles AWS has developed to help you navigate your journey to Zero Trust.

1

Where possible, use identity and network capabilities in tandem

While a Zero Trust security model decreases reliance on network location, the role of network controls and perimeters remains important to the overall security architecture. In other words, the best security does not come from making a binary choice between identity-centric and network-centric tools but rather by establishing an architecture where these tools are aware of and augment each other.

2

Work backwards from your specific use cases

One of the best ways to pursue Zero Trust is to prioritize the use cases that will provide the most benefits to your organization—and then work backwards to determine the optimal Zero Trust patterns, tools, and approaches to achieve meaningful security advancements. Read on to learn more about today's top Zero Trust use cases.

3

Apply Zero Trust to your systems and data according to business value

Zero Trust concepts should be seen as additive to your existing security controls. By applying Zero Trust based on the value of systems and the sensitivity of data, you can check that the benefits to your business are commensurate with your effort. As you continue on your journey to Zero Trust, your security posture will improve, with your security controls benefiting from the increased visibility and software-defined nature of the cloud.

GETTING STARTED

6 keys to starting off right

The first steps in any journey can feel overwhelming—especially in the early days of your efforts. These best practices can help you move forward with confidence as you establish the right foundations, avoid common missteps, and chart a path to Zero Trust success.

1. Clearly define your goals

Before you begin, communicate to your organization why you're moving to Zero Trust and what your goals are. Focus on specific steps and real business outcomes rather than describing an ideal future state. List key stakeholders and write a concise summary for each that articulates why they should care about Zero Trust and how your efforts will directly benefit them. Be prepared to consistently deliver, reinforce, and refine these messages as your journey to Zero Trust progresses.

2. Choose the right initial use cases

Start with use cases that demonstrate clear value and deliver quick wins to help you generate momentum. Consider human-to-application use cases—such as remote user connectivity—and software-to-software use cases—such as improving east-west network controls and visibility. These starting points are typically manageable, complementary, and visibly beneficial to multiple groups.

It may be wise to have your Zero Trust team move one of its own applications or application groupings first. This can give other teams confidence in your capabilities when it is time to move the components that are important to them.

3. Develop living reference architectures

Develop dynamic reference architectures that depict your objectives for each use case—and act as living artifacts that are designed to evolve continually. These will allow you to start building quickly and adapt as your efforts progress. Plus, using dynamic reference architectures early in your Zero Trust journey will encourage teams to consider templatizing the architectures for consumption over time.

4. Build confidence as you scale

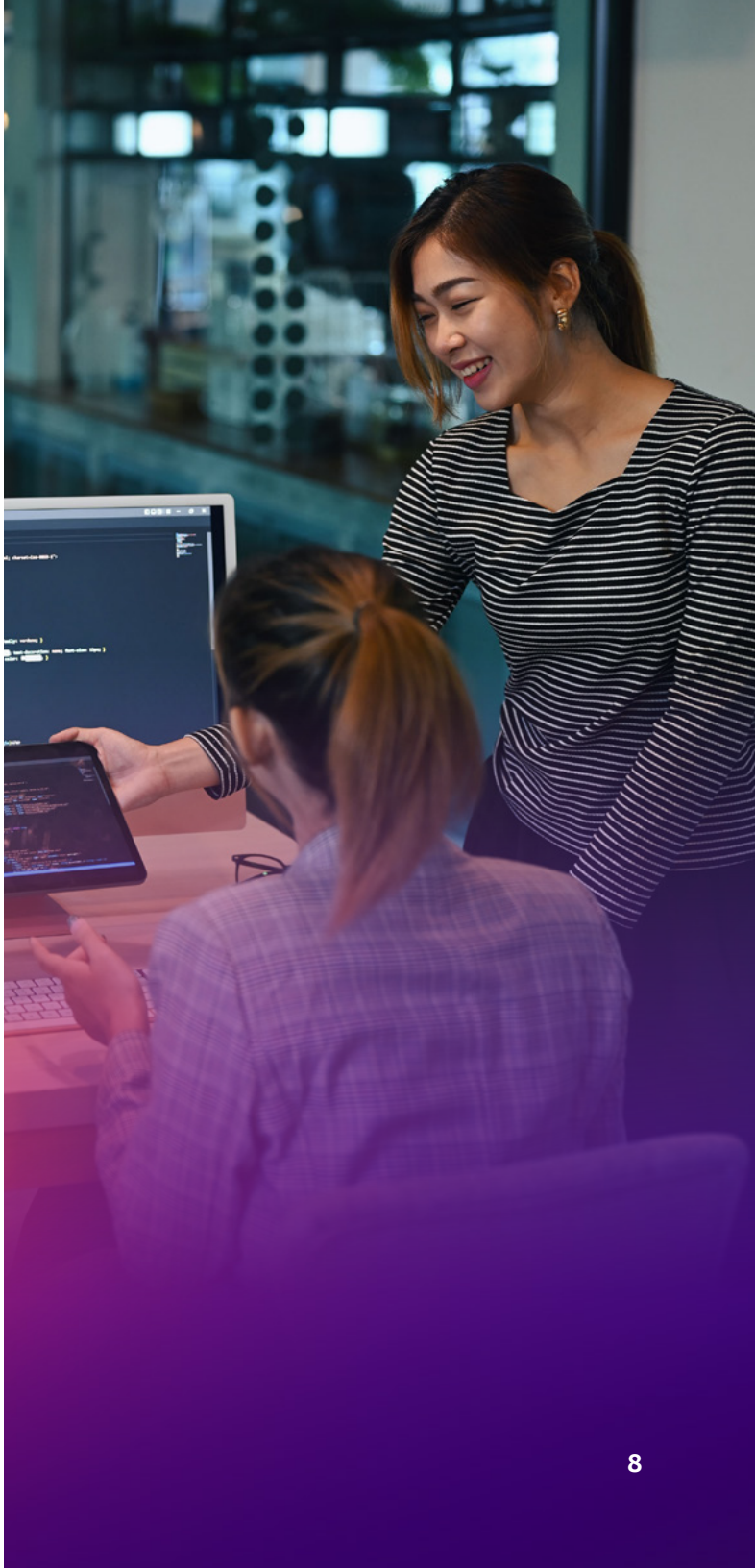
By initially focusing on a small and meaningful set of workloads, you can refine the necessary technical and operational processes in a flexible and iterative way. At the same time, you will build the authenticity and experience necessary to expand efforts throughout your IT environment.

5. Compare retrofitting with modernization

Consider your options as you evaluate a Zero Trust security model for a particular application or use case. Compare the effort and value of retrofitting Zero Trust onto the application as is versus rearchitecting the application with Zero Trust as part of a broader modernization or cloud migration initiative. Retrofitting may still be the best choice—however, your existing application modernization project may be a great opportunity to architect in a Zero Trust security model as another key step in the journey.

6. Recognize champions to fuel adoption

Zero Trust simplifies security for end users. For developers, it offloads security concerns and may provide a "free upgrade" to modern application identity. For security teams, it provides assurance for application access and shrinks the risk surface area. And, for every team, Zero Trust allows for greater flexibility and secure connectivity that can improve productivity and customer experience. By recognizing champions and celebrating wins along the way, you can create advocacy and enthusiasm that fuels your efforts.



Expanding your journey

As your Zero Trust team gains experience and more users enjoy the security model's benefits, your rollout will gain momentum. You will also begin to see fewer security events, leaving you more time to focus on improving security and the end-user experience—and generating enthusiasm that further fuels adoption. Over time, a flywheel effect can take hold, where your Zero Trust rollout can then accelerate and expand on its own.

It all starts with finding the Zero Trust use cases that provide you with the most value. In the next sections, we will examine three top use cases for today's organizations.

THREE TOP USE CASES

Top Zero Trust use case #1:

Secure workforce mobility

The modern workforce requires secure access to business applications from anywhere work happens. This allows you to develop new flexible work arrangements, widen your available talent pool, and increase your capacity to adjust to evolving customer needs.

With **AWS Verified Access**, you can provide your workforce with secure access to corporate applications—no VPN required. By connecting your existing identity provider (IdP) and device management service, you can tightly control application access based on the security and compliance state of user devices—while allowing users to continue leveraging their existing credentials. AWS Verified Access verifies each access request in real time and connects users to the application when specific security requirements are met.

For secure workforce mobility scenarios where you may not own the hardware device, you can use services like **Amazon WorkSpaces Family** or **Amazon AppStream 2.0**. These services stream applications as encrypted pixels to remote users—while keeping data safe within your Amazon VPC and other connected private networks.

"With Verified Access, our Security and Technical engineers were able to provision zero-trust-based access to corporate applications in just minutes, without using VPNs. Verified Access allowed us to tackle the crucial challenge of aligning essential service delivery with user experience enhancement, all without compromising our strict zero-trust policies."

Eric Ellis, AVP Enterprise Cloud Technology, Avalon Healthcare Solutions

THREE TOP USE CASES

Top Zero Trust use case #2:

Software-to-software communications

Modern architectures include software components that are constantly communicating with other applications, data sources, and cloud-based application programming interfaces (APIs). By eliminating unnecessary communication pathways to data, you can strengthen your security posture.

A Zero Trust architecture can secure software-to-software communications from end to end and free your developers to focus on innovation instead of security. You can accomplish this by authorizing specific flows between software components and maintaining tight control over what and how components within your application network are able to communicate.

With AWS, this can be done by using application networking services to help connect and secure your applications, implementing request-level evaluation, and applying **least-privilege permissions** to better protect critical data.

For simplified application-level connectivity across virtual private clouds (VPCs), accounts, and a mix of compute types, you should use **Amazon VPC Lattice**—an application networking service that consistently connects, monitors, and secures communications between your components. Amazon VPC Lattice raises your security posture by creating a dedicated application layer network for software-to-software connectivity with embedded authentication and authorization. This removes unregulated communication paths between software components, allowing your developers to focus on application logic and deliver applications faster.

"[Securely] connecting applications to data sources across multiple accounts was extremely difficult and time consuming for us…[Amazon] VPC Lattice enabled our developers to easily and securely connect our applications and data sources across accounts without introducing network complexity."

Suman Sriram, DevOps Team Lead, Altus Group

THREE TOP USE CASES

Top Zero Trust use case #3:

Authorization in your custom applications

Today, your end users can authenticate to your custom applications with SAML-based third-party IdPs using AWS Verified Access integration with **AWS IAM Identity Center**. If you already have a custom IdP solution that is OpenID Connect compatible, AWS Verified Access can authenticate users by directly connecting with your IdP.

However, the authorization logic may still be implemented in your custom application itself. Over time, the code and permissions can grow increasingly complex to develop and maintain. And, as more custom applications are built, handling authorization in this way can cause needless duplication of effort and fragmentation.

On AWS, your developers can efficiently implement fine-grained access controls in applications by using **Amazon Verified Permissions**. This scalable, performant, and fully managed service externalizes authorization from applications and allows you to centralize the definition and management of access policies. By moving authorization logic out of your application code, you can provide developers with a consistent, scalable way to authorize user actions within and across custom applications. And, your developers can align application access controls with Zero Trust principles like least privilege and continual authorization for the resources and data within their applications.

Both AWS Verified Access and Amazon Verified Permissions use the **Cedar policy language**. Cedar is an expressive and analyzable open-source policy language that allows developers and admins to define policy-based access controls using roles and attributes for more granular, context-aware access control. This allows for better analysis and auditability of who has access to which applications and to what resources within applications.

AWS SERVICES

AWS services for your Zero Trust journey

The following services from AWS can help you operationalize Zero Trust faster and with less disruption—while harnessing the greatest benefits to your organization.

AWS Verified Access

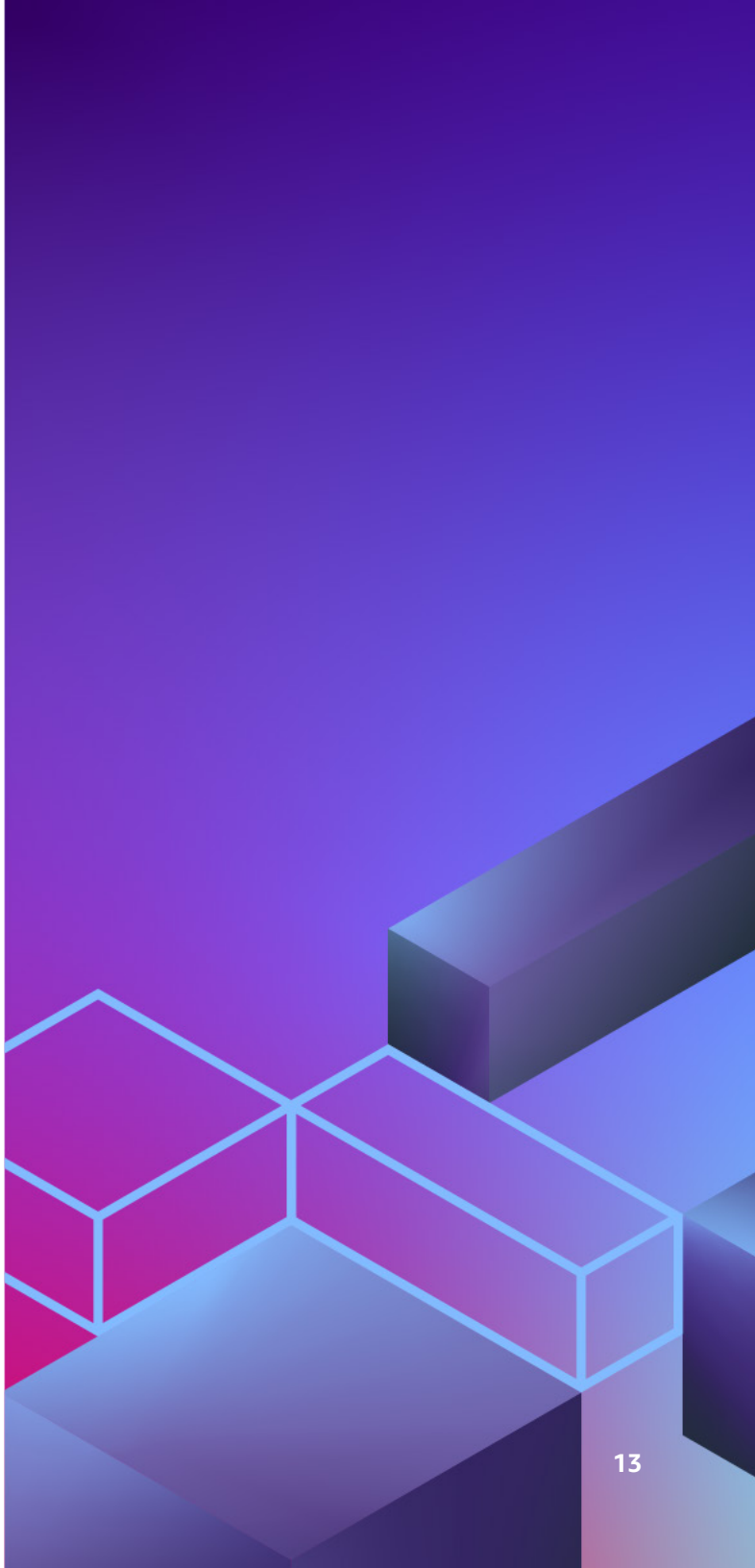
Built on Zero Trust guiding principles, this service provides secure access to corporate applications without a VPN. It simplifies the remote connectivity experience for your end users and reduces management complexity for IT.

Amazon VPC Lattice

This application networking service simplifies software-to-software connectivity, security, and monitoring with embedded authentication and context-specific authorization. You can define granular policies to connect software components in a consistent way across instances, containers, and serverless applications. This service also helps to eliminate unnecessary communication paths between components.

Amazon Verified Permissions

This scalable service allows your developers to implement fine-grained access controls for the applications they build. It also provides your administrators with tools to centrally manage permissions policies and audit application resource access. Plus, your developers can define policy-based access controls using roles and attributes for more granular, context-aware access control.



CONCLUSION

Next steps

Zero Trust architectures offer much more than improved security. They can reduce operational burden on your business and technical teams, allowing them to move faster and with greater agility, make smarter and more confident decisions, and be more productive.

With greater flexibility and less time spent worrying about security, your teams can focus more on delivering great results for your customers and your business. In this way, Zero Trust can even spark innovation—providing your teams with the peace of mind and courage to experiment, explore, and ultimately bring bigger, bolder ideas to life.

At AWS, we embraced Zero Trust early, incorporating its principles into the design of our infrastructure to help meet the needs of the most security-conscious organizations in the world. Today, our breadth of security, identity, application development, and networking services delivers the building blocks of Zero Trust as standard features that you can apply to new and existing workloads. Plus, AWS offers guidance that can help you realize the full benefits of Zero Trust along every step of your journey.

Following the guidance in this eBook can help you lay the foundation for Zero Trust success—and ultimately transform your organization into a secure, flexible enterprise that's built for today and ready for tomorrow.

Learn more about Zero Trust on AWS ›