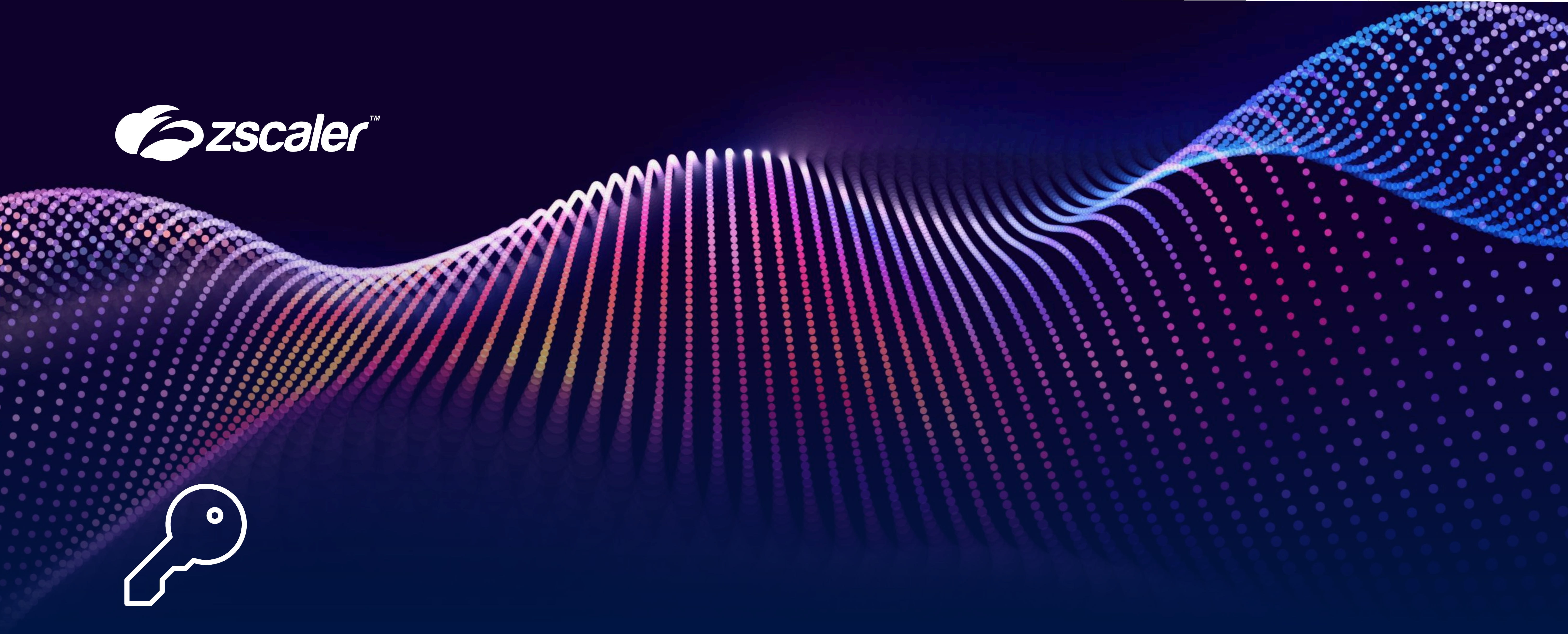


Lock Down Your Cloud: Best Practices for Securing Mission-Critical Applications

For many organizations, the migration from traditional on-premises data centers to public cloud platforms is in its final stretch, and completion may only be a few years away. By 2027, Gartner predicts that 90 percent of organizations will maintain at least some of their applications on public clouds[1]. The following year, cloud computing will have completed its shift from technology disruptor to business necessity[2] — and for good reason.

Cloud environments allow organizations to quickly ramp up resources, roll out new services, and slash infrastructure costs compared to old-school, on-premises setups. By prioritizing cloud adoption for mission-critical workloads, businesses can swiftly adapt, innovate, and thrive in today's dynamic landscape.

But with new opportunities, comes heightened risk.

In the race to move to the cloud, some organizations have prioritized rapid digital transformation over security best practices, leaving them vulnerable. Consequently, cyberattackers view cloud-based targets as potentially easy paths to substantial gains and are evolving their tactics to exploit these vulnerabilities.

In today's hybrid and multicloud world, organizations have more freedom than ever to build where and when they want. But this is juxtaposed with widespread concern over the security of public clouds, signaling a need for the adoption of better security tools and practices.

To navigate this complex landscape, enterprises are turning to zero trust — a modern, cloud-native security framework that ensures only authorized users and devices gain access to critical cloud resources. With a well-designed cloud security strategy, organizations can go a long way toward preventing breaches, improving compliance, and building stronger customer trust.

As organizations move their critical applications to the cloud, it's crucial to rethink your security strategies, particularly with data governance and compliance under the regulatory microscope.

This whitepaper highlights the key risks that IT leaders and cloud security teams face in securing cloud transformations. We will also take a closer look at the proven strategies and best practices enterprises are using to secure mission-critical applications in public cloud environments.

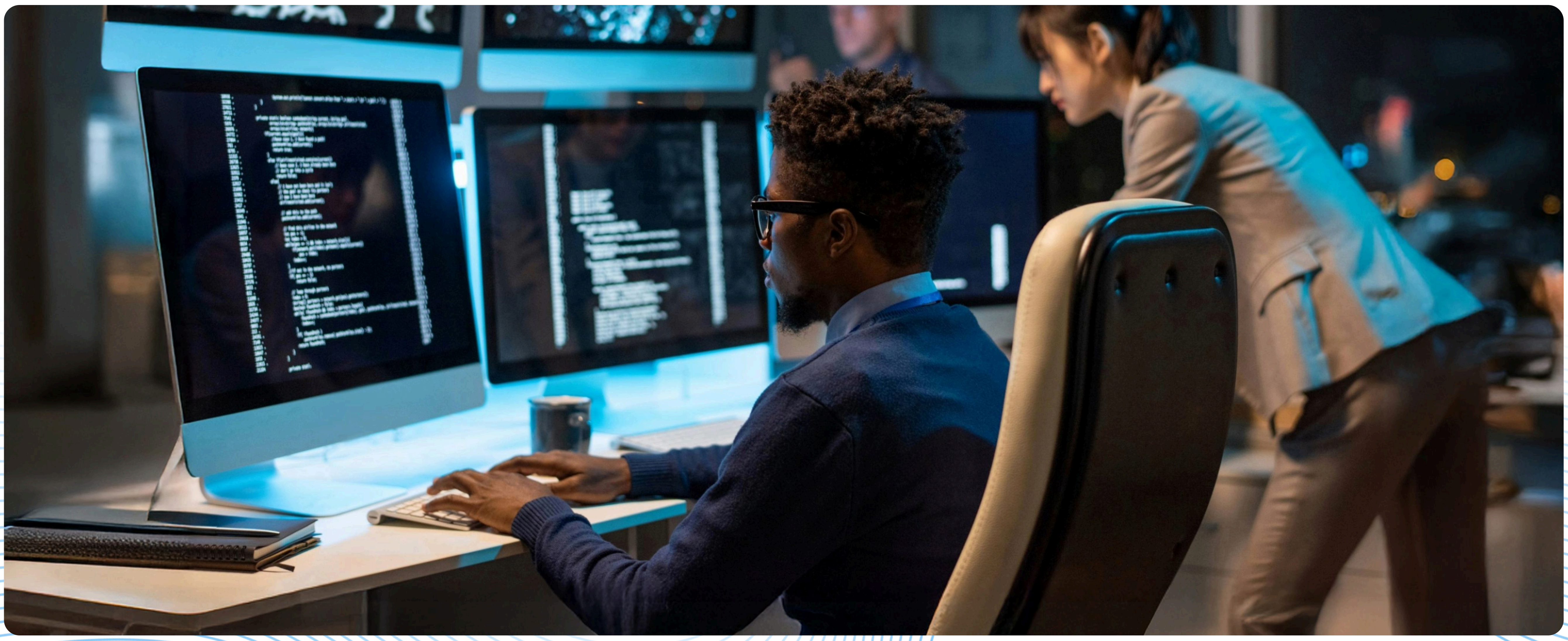
What happens when applications move to the public cloud?

When applications make the leap to the public cloud, they're trading in their old brick-and-mortar homes for sleek, modern apartments in a bustling metropolis. Here’s what happens in this exciting, yet complex, transition:

- **From monolith to microservices:** Instead of one massive application, think of a collection of smaller, independent services, or microservices. Each microservice is designed to perform specific functions and can be developed, deployed, and scaled independently.

- **Chatty APIs:** Cloud-native applications use APIs to talk to each other, creating a super "chatty" environment where services are constantly interacting. While it enhances flexibility and scalability, APIs also increase vulnerability to security threats.

- **Workloads on the move:** Applications are no longer confined to a single server room but are now scattered across different cloud environments in various regions, availability zones, and hybrid setups.



The importance of securing mission-critical applications in the cloud

Mission-critical applications are the lifeblood of any enterprise — the beating heart that sustains business operations. These vital applications, which may include financial transaction systems, healthcare platforms, industrial automation, and enterprise resource planning (ERP) systems, demand unwavering availability, instantaneous real-time processing, and strict regulatory compliance.

Problem is, any disruption can lead to significant business, financial, and reputational damage.

So while moving mission-critical applications to the cloud has its benefits — scalability, agility and cost savings, to name a few — it also introduces a number of potential downsides, such as:

- **Increased exposure to cyber threats:** Applications that process highly sensitive data are prime targets for attackers looking to exploit vulnerabilities.
- **Operational complexity:** The shift to multicloud environments introduces distributed architectures, API-driven communication, and dynamic workloads, which increase the attack surface.
- **Regulatory compliance challenges:** Enterprises operating in industries such as healthcare, finance, and government must adhere to strict compliance frameworks like HIPAA, GDPR, and PCI DSS, making cloud security governance critical.

40% **of data breaches involved data stored across multiple environments.**[3]

It probably comes as no surprise that legacy architectures simply can't handle the job of protecting mission-critical workloads in the cloud. That's because...

01 Legacy security solutions, such as firewalls, VPNs, and perimeter-based defenses, were built for static, on-prem environments and lack the flexibility to secure highly dynamic cloud workloads.

02 Traditional network-based security does not provide granular application-level controls, leaving gaps in protecting API-driven, microservices-based architectures.

03 Legacy access models rely on implicit trust, making them vulnerable to credential-based attacks, lateral movement threats, and insider risks.

And in the high-stakes world of mission-critical applications, a single security failure can trigger a devastating cascade of consequences.

Downtime can:

- Cripple operations
- Bleed revenue
- Erode customer trust

Data breaches expose sensitive data that leads to:

- Regulatory fines
- Legal battles
- Irreparable reputational damage

$5.17M **Average cost of breached data stored in public clouds.**[4]

Challenges in securing mission-critical applications

The shared responsibility model and its pitfalls

In recent years, the cloud has evolved from an emerging technology to an indispensable backbone for modern businesses. It’s important to recognize that the cloud, however, is not inherently secure. Instead, cloud security operates as shared responsibility between the customer and the cloud provider. Think of it like living in a building where the landlord maintains the structure, but you're responsible for securing your apartment and belongings.

In this shared responsibility model, cloud providers safeguard the underlying cloud infrastructure, while customers are responsible for securing their workloads, applications, and data. It’s not uncommon to misunderstand this model and mistakenly assume that cloud providers fully protect customer workloads. This can result in:

- **Exposed storage buckets**, poorly configured cloud storage that leads to publicly accessible sensitive data.
- **Weak identity and access controls**, overly permissive IAM roles allowing unauthorized access to mission-critical applications.
- **Compliance failures,** lack of continuous monitoring and enforcement, leading to regulatory penalties.

Broader security challenges in securing mission-critical applications

Beyond the potential pitfalls of the shared responsibility model, enterprises face additional risks when securing mission-critical workloads in the cloud. These range from:

- **Unauthorized lateral movement:** Legacy security models, such as firewalls, VPNs, and perimeter-based defenses, struggle to protect dynamic cloud environments, increasing the risk of unauthorized access and lateral movement.
- **Visibility gaps:** Maintaining consistent security policies across hybrid and multi-cloud environments is difficult, leading to fragmented security postures and gaps in visibility.
- **Poor policy standardization:** Multi-cloud complexity creates additional risks, as different cloud providers have inconsistent security frameworks, making policy standardization difficult.
- **Lack of segmentation:** Insufficient integrated data protection and segmentation allow attackers to spread across cloud environments after a single point of compromise.

79% Organizations that cite cloud security as a top challenge.[5]

5 best practices for securing mission critical applications in the cloud

To effectively secure mission-critical applications in the cloud, what strategies should enterprises include in their security toolkit? Since it isn't automatically impenetrable; it requires strategic planning and robust defenses. Think of these five best practices as the cornerstone of your cloud security strategy, each playing a vital role in protecting your cloud-based assets and maintaining compliance.

01 Implement least-privileged access based on identity and authentication

- Adopt zero trust access controls to ensure that only authorized users, devices, and workloads can communicate with mission-critical applications.
- Hide your applications by not publishing IP addresses. What is hidden cannot be attacked by malicious actors.
- Continuously monitor and adapt access policies based on user behavior and real-time risk analysis.

02 Secure applications, not networks

- Shift away from traditional network-based security by connecting applications rather than entire networks, eliminating the need for backhauls, firewalls, and VPNs.

- Adopt cloud-delivered security solutions that protect workloads at the application level, ensuring direct, secure connectivity without exposing the broader network.

- Leverage zero trust network access (ZTNA) to provide secure, granular access to applications without increasing attack surfaces.

03 Deploy integrated threat protection and real-time security inspection

- Implement advanced threat protection, including intrusion detection, behavioral analytics, and AI-powered anomaly detection to identify and mitigate cyber threats.

- Use data protection solutions that provide end-to-end encryption, data loss prevention (DLP), and continuous monitoring.

- Utilize a cloud-delivered security platform capable of real-time threat inspection at scale to detect malicious activities before they impact mission-critical applications.

04 Enforce workload segmentation to prevent lateral movement

- Apply microsegmentation to isolate workloads, limit east-west traffic, and prevent attackers from moving laterally across cloud environments.

- Ensure segmentation across multiple cloud layers, including:

A. **Process-level segmentation** — Restrict communication between workloads within a host.

B. **VPC and availability zone segmentation** — Limit access between different cloud environments to minimize exposure.

C. **Multi-cloud segmentation** — Enforce uniform security policies across AWS, Azure, Google Cloud, and hybrid infrastructures.

05 Leverage automated enforcement for regulatory compliance

- Align cloud security strategies with industry-specific regulations such as HIPAA, GDPR, PCI DSS, and NIST.

- Use automated policy enforcement and compliance auditing to ensure continuous adherence to security frameworks.

How Zscaler helps enterprises secure mission-critical applications

Zscaler is a powerful ally for enterprises striving to secure their mission-critical applications. With its cloud-native Zero Trust Exchange™ platform, Zscaler delivers direct and secure workload-to-workload connectivity, effectively eliminating the need for traditional VPNs, firewalls, and backhauls, all while keeping applications shielded from the internet's threats. By continuously inspecting traffic, detecting threats, and enforcing policies across hybrid and multi-cloud environments, Zscaler ensures real-time visibility and robust protection for cloud workloads.

- **A fully cloud-native Zero Trust Exchange™** platform delivers direct and secure workload-to-workload connectivity without exposing applications to the internet or relying on VPNs, firewalls, or backhauls.
- **Real-time visibility and protection for cloud workloads** continuously inspects traffic, detects threats, and enforces policies across hybrid and multi-cloud environments.
- **Automated policy enforcement for secure and compliant application access** ensures consistent security policies for applications, reducing the risk of misconfigurations and compliance violations.

Validating Zscaler’s impact: insights from the SANS product review

A product review by SANS provides a professional validation of Zscaler's capabilities in securing mission-critical applications[6]. Here's a breakdown of the key areas where Zscaler shines, according to the review:

- **Zero trust model:** Zscaler eliminates attack surfaces by directly connecting workloads, reducing exposure and risk. This approach ensures workloads are less discoverable and lowers the risk of exploitation.
- **Lateral movement prevention:** Zscaler enforces microsegmentation and identity-based policies across cloud workloads, mitigating lateral movement through app-to-app segmentation.
- **Real-world threat mitigation:** Real-time traffic inspection, continuous monitoring, and AI-driven security analytics effectively mitigate threats, with data protection through DLP and SSL at scale.
- **Comprehensive monitoring and control:** Zscaler's Cloud Connector platform monitors and controls access to applications and cloud services, manages data flow, and assesses application security posture.
- **Intuitive Interface:** The interface and policy engine are user-friendly, simplifying the configuration and management of security policies.

In short, the SANS review validates that Zscaler's cloud-native security model is the industry leader, helping global enterprises like Siemens, Micron, and Mahindra Group, protect their most critical applications, meet compliance requirements, and simplify the complexity of multicloud security.

Achieve comprehensive security in the cloud

As enterprises move mission-critical applications to the cloud, they face significant security risks that demand immediate attention. But the right strategies can pave the way for secure and efficient operations. A modern zero trust architecture allows organizations to securely connect applications anywhere to minimize the attack surface, prevent lateral movement, and reduce the risk of bad actors gaining access to your data. This positions enterprises to confidently navigate the complexities of cloud security and achieve comprehensive protection of their most valuable assets.

Take the next step to ensure the safety and integrity of your cloud-based assets. Request a demo to see firsthand how you can radically simplify cloud workload protection.

REQUEST A DEMO

Or, take your own test drive of Zero Trust Cloud in our Self-Guided Lab.

SEE GUIDE

zscaler™ | Experience your world, secured.™

About Zscaler Zscaler
(NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025

[2] Gartner Says Cloud Will Become a Business Necessity by 2028

[3] IBM Cost of Data Breach Report, 2024

[4] IBM Cost of Data Breach Report, 2024

[5] Flexera 2023 State of the Cloud Report

[6] How to Use Zero Trust to Secure Workloads in the Public Cloud, SANS, 2023