6 recommendations to ensure your cloud journey is secure right from the start

PRESIDIO®

Introduction

Securing your data in the cloud has never been more critical. The fast evolution of technology, paired with an increasing reliance on the cloud, has ushered in an era where vast amounts of sensitive enterprise data are stored remotely. This increased attack surface requires different ways of securing it, adding complexities with hybrid and multi-cloud that were non-existent with legacy infrastructure.

Accelerated by the pandemic, this shift to the cloud has helped companies realize unprecedented convenience and agility with seamless access to data—accessible anywhere, anytime. Statista reported that 92% of global organizations moved to the cloud during 2020 due to the pandemic. And the move to the cloud is not slowing down. The adoption rate of cloud technology remains strikingly strong, with roughly 39% of organizations hosting more than half of their workloads on cloud platforms, according to Forbes. In fact, Enterprise Strategy Group (ESG) found that 55% of organizations reported their application workloads run on cloud Infrastructure-as-a-Service (IaaS) today. This number is projected to increase to 62% by 2024. Workloads are migrating to cloud infrastructure, and new applications continue to be natively built on the cloud. And by 2025, Gartner reports more than half of enterprise IT spending in key market segments will shift to the cloud.

Unsurprisingly, business leaders rely on the cloud for many positive outcomes, including greater agility, scalability, and increased collaboration, to accelerate growth, efficiency, and customer experience. (CIO)

62% of organizations plan to run on cloud IaaS in the next year.

Business leaders leverage public cloud to:

83% mitigate business and regulatory risk

80% build net new product/ service revenue

74% expand into new markets

72% provide better sustainability in support of environmental issues

Source: Deloitte

Some companies are new to the cloud. Others are cloud-native. If you have started migrating to the cloud, you may be discovering issues along the way. Perhaps you must constantly modernize or add solutions as you discover missing security or functionality—thus, iterations to Cloud 2.0 and 3.0 continue. You may not have the visibility you need. You may need to understand how to secure your new services or migration more fully. By establishing a solid foundation from the start, you can avoid changes to your cloud later.

This ebook explores some of the challenges companies face, as well as recommendations, solutions, and tools to set yourself up for cloud security success during your migration and beyond.

Security across your extended environment may be inconsistently enforced and complex to manage—and connections are often unsecured.

Here are some challenges you could face on your journey to the cloud.

Stuck with legacy infrastructure

Still operating in a legacy data center? You're not alone. Accenture found that 34% of the interviewed business leaders reported this as a problem. When you're trying to get cost-saving benefits of the cloud while still running legacy infrastructure, it could cause complications for your teams that need to secure multiple environments. You may feel stuck in the middle because your legacy system is not fully compatible with your desired cloud environment, which could lead to data loss, compromise or damage during the migration process. Security between on-premises data centers and clouds is often fragmented and inconsistent.

Burdened by legacy data

Your legacy data may not be structured optimally for cloud systems. This can cause trouble when applying governance policies to your data in the cloud. Additionally, privacy laws and regulations such as GDPR, CCPA or others must be considered. If you are in a heavily regulated industry such as healthcare or financial services, you likely have rigorous regulatory compliance standards you need to meet.

Lack of visibility

If you don't know what workloads you have in the cloud and you're not sure what you need to monitor, you're among the majority. Only 20% of IT professionals say they can adequately monitor their public cloud environments for security threats and application performance, and seven out of 10 say it's harder than monitoring company data centers and private cloud, according to CRN. Before strategizing a cloud security plan, you must know what you have stored in the cloud. You will want to address how you will monitor your applications in the cloud or build the capability to do so.

This can be incredibly challenging with mergers and acquisitions. Multiple ecosystems, stakeholders and systems cause complexity and added difficulty. Even without M&As, siloed organizations often exist. Lack of centralized security visibility across platforms was the second biggest problem reported, according to a 2022 report in Venture Beat.

Resistance to change

Some business leaders run into challenges with mindsets stuck in the past. Security engineers may worry that the public cloud, new applications and technologies will take away their jobs. They've been doing network security or working in their field for a long time, and as more workloads are moved to the cloud, it can feel like a different world. They may perceive "infrastructure code" and "automation" as threats. Cloud migration is a significant change. Companies that face resistance from within their organization can benefit from working with experienced third-party advisors to help bring everyone together and get them on the same page.

Overcoming challenges with the right cloud security partners

Presidio brings a consultative approach with decades of expertise across all major industries exhibited through its Cloud Center of Excellence. Presidio and Amazon Web Services formed a strategic collaboration agreement to accelerate cloud adoption and improve outcomes for companies in the cloud. Presidio also teamed up with Fortinet to deliver security solutions and services to safeguard your application and workloads across cloud and hybrid environments.

A modern security solution like Fortinet's Security Fabric is designed to help you rise above challenges, providing visibility, secure connectivity, and application protection across your entire ecosystem.

Finding the right team you can trust to help secure your transition to the cloud can make a world of difference

Six recommendations to secure your cloud journey from beginning to end

1 Start with a solid foundation

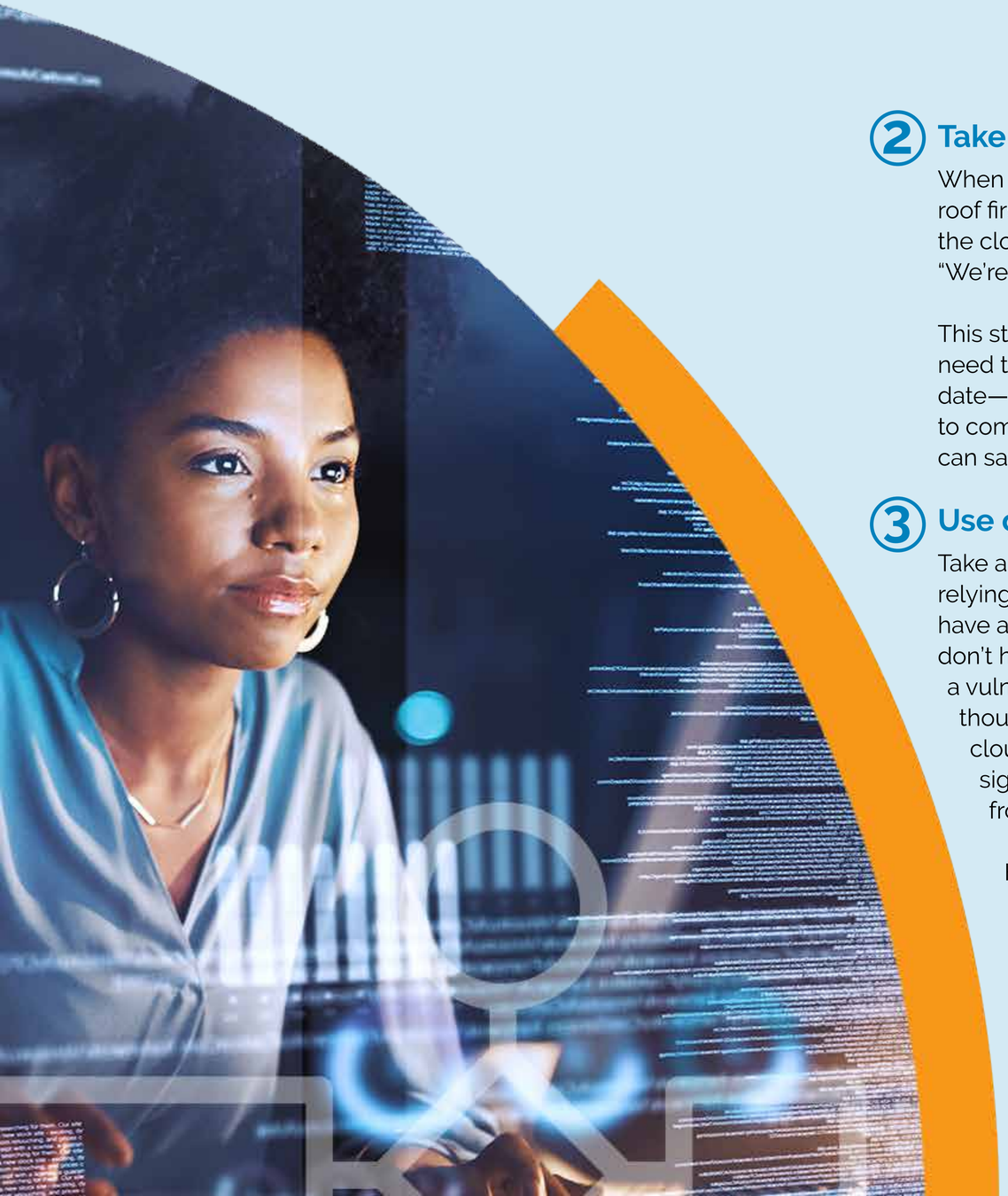
Step back and get your foundation correct with governance, compliance, identity access management policies, etc. This is how to ensure you do it right and securely—from the start.

Presidio recommends taking a holistic approach. Don't start with the tool. That should not drive the discussion. Look at the various needs within your organization.

Presidio helps you examine your business needs and drivers—evaluating how they function today and determining your desired future outcomes.

When moving to AWS, Presidio will help you implement landing zones immediately by utilizing AWS Control Tower. This offers the easiest way to set up and govern a secure, multi-account AWS environment. Your landing zone will be a well-architected, multi-account baseline that adheres to AWS best practices. We will also help you establish:

- controls to ensure governance rules for security, compliance, and operations.
- automation, DevOps and Infrastructure as Code (IaC) to identify gaps and misconfigurations at the foundational level. This forces teams to define their infrastructure before it gets deployed. When found early, changes can be made before your teams move on to another project. Earlier feedback means more secure deployments.



2 Take your time

When building a house, you cannot start with the roof first. Often, when companies want to move to the cloud, it is because an executive has decided, "We're going to the cloud, and that's that."

This starts a chain reaction, and IT leaders feel they need to move out of the data center by a specific date—it's false urgency. Taking two or three months to come together, organize, and build a foundation can save time and money in the long run.

3 Use one set of tools

Take a platform approach to security instead of relying on individual products. Different products have alerts and things they want you to fix, but they don't have the context around that. You might have a vulnerability management tool spinning out a thousand alerts and another tool looking at your cloud misconfigurations with bunches of other signals. You will be experiencing alert fatigue from all those different systems.

Having a single platform approach with context around those alerts helps you focus on what's most meaningful and impactful. The Fortinet Security Fabric provides broad visibility across the entire digital attack surface, both on-premises and in multiple clouds. It uses native integration with each of the major cloud providers and enables automated, centralized management of the entire security infrastructure from a single pane of glass.

4 Keep your eye on the prize

Stay focused on the business outcomes you want, not the technology itself. If you aim to bring products to market faster, you can adopt DevOps practices that integrate applications across legacy infrastructure and clouds. If you need to improve your customer experience, modernized cloud solutions can free data trapped in legacy systems to enable AI and advanced analytics to generate insights about customer needs.

Whatever outcome you desire, Fortinet helps secure the digital acceleration of your application journey across hybrid and multi-cloud environments. We do this by offering cloud security solutions natively integrated with all major cloud platforms and technologies. Fortinet Security Fabric reduces operational complexity, provides greater visibility, and delivers robust security effectiveness.

5 Get everyone on board

The Presidio Cloud Center of Excellence helps bring people together. This engagement fosters executive alignment within your organization, uniting security teams, application developers, infrastructure, and networking. It may take work to ease tension between different groups within your organization, but ultimately, it is worth it when you gain alignment.

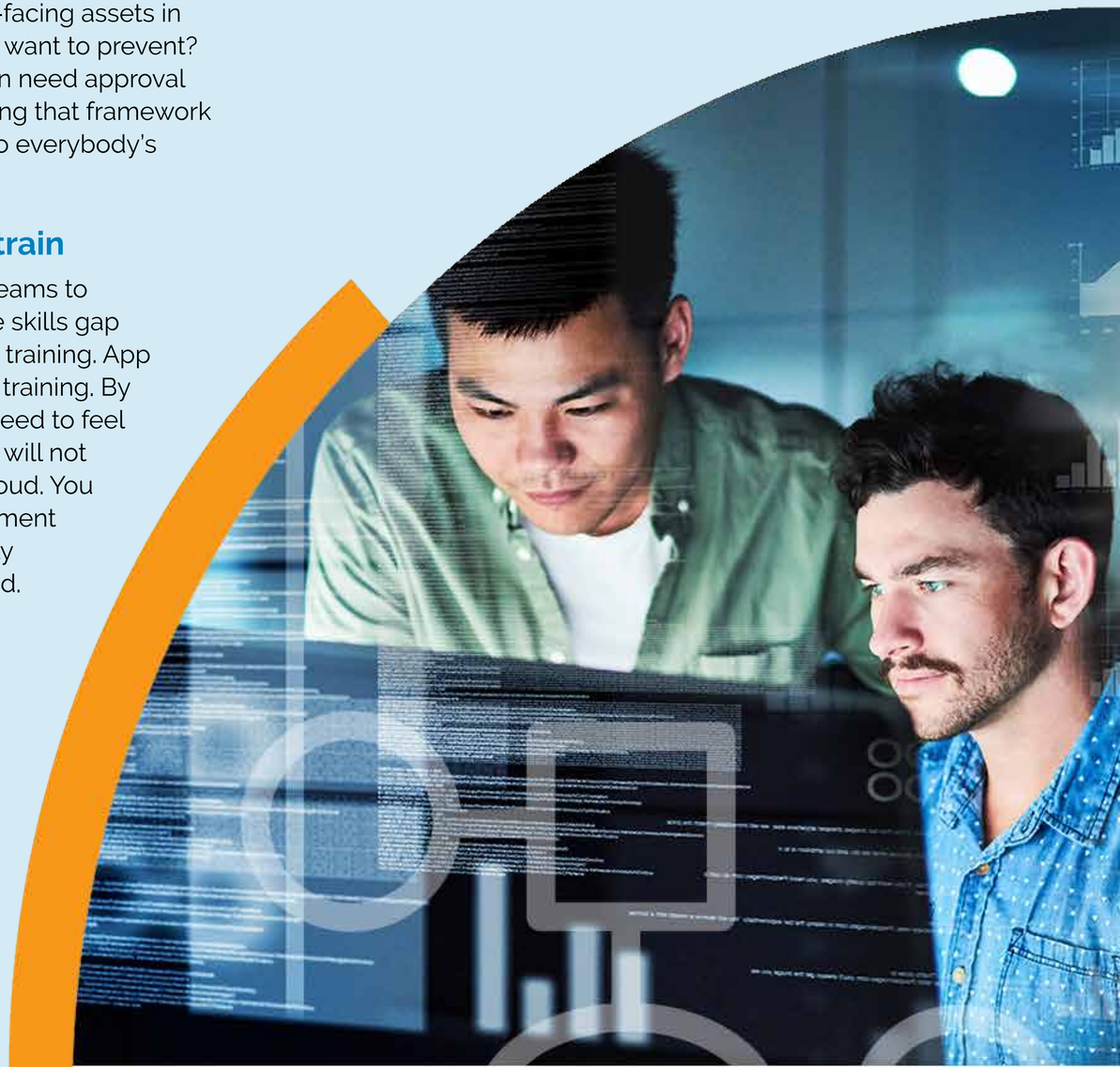
Cloud deployments require the most coordination between executives, business units, and IT and security professionals who must understand that “meeting business goals” can mean different things to different people.

Anyone who’s going to be involved in the cloud migration should be part of the process from the beginning. Having all major players involved upfront helps you align on essential issues such as how to run your networking in the cloud, how to run your external-facing networking, how to connect on-premises, how to organize your accounts or subscriptions, where to place security controls, how you are going to leverage automation and DevOps, and what type of policies are needed around the cloud?

We will also work with your teams to develop your policies around the cloud. For instance, will you allow your employees to create publicly-facing assets in the cloud, or is that something you want to prevent? Will people within your organization need approval for those types of things? It’s building that framework for how you’ll leverage the cloud so everybody’s doing it together.

6 Reskill, upskill and cross-train

You may need to cross-train your teams to bring them together and overcome skills gap issues. Security teams need cloud training. App development teams need security training. By providing the training your teams need to feel comfortable in their new roles, you will not lose talent as you move into the cloud. You must ensure learning and development continues to keep pace with quickly evolving technologies like the cloud. A robust skills plan will help your company prosper in any business environment.



Why Presidio?

Presidio's Cloud Migration Services provide comprehensive offerings to help you define and execute your cloud strategy with a structured approach for a full-stack migration that includes applications, infrastructure, and DevOps automation. This approach is focused on delivering business value-based outcomes without compromising risk mitigation, security or regulatory requirements. Our Cloud Migration Framework is designed to be a forward-thinking approach to provide long-term benefits such as cost reduction, faster time-to-market, and continuous innovation for your application workloads migrated to the cloud.

We also provide a migration strategy roadmap for migrating each application workload, leveraging the industry-accepted 6-R methodology (rehost, re-platform, re-factor, re-architect, retain, retire and replace.) This roadmap is perfectly aligned with your business and designed to mitigate risk, all while delivering value to your organization as quickly as possible.

We help our customers Get Cloud Right—the right workloads on the right clouds, at the right cost, providing the right level of service.

PRESIDIO®

Why Fortinet?

Fortinet protects your AWS environment with best-in-class security solutions, helping you gain end-to-end visibility and control across your workloads. We deliver network, application, and platform security solutions that integrate with AWS to provide comprehensive threat protection. All your security data is visible and actionable through single-pane-of-glass management and security automation.

FortiGate Next-Generation Firewalls (NGFWs) provide secure connectivity, network segmentation, and application security for hybrid-cloud-based deployments. They help ensure centralized, consistent security policy enforcement and connect through a high-speed virtual private network (VPN) tunnel. The latter protects data without compromising performance.

FortiGate VMs are virtualized instances of FortiGate NGFWs. FortiGate VMs can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in an on-premises data center.

FortiManager provides single-pane-of-glass management across the entire extended enterprise—including Fortinet NGFWs, switches, wireless infrastructure, and endpoints. FortiManager makes enterprise security management easier, enabling you to create and modify policies and objects with a consolidated, drag-and-drop-enabled editor. You can also manage devices in a Fortinet Security Fabric group as a single device, ensuring that security policies are enforced consistently across all environments. Finally, you can simplify and track changes and make them auditable through integration with IT service management (ITSM) applications such as ServiceNow.

FortiAnalyzer enables organizations to analyze, report, and archive security events, network traffic, web content, and messaging data. A comprehensive suite of easily customized reports simplifies the measurement and documentation of compliance.

The comprehensive management view helps you streamline operations, ensure policy consistency, and unify your workflows across different workloads. From those you build net new on AWS to those you lift and shift straight out of your data center, regardless of location.

FORTINET®

Better Together

Fortinet and Presidio work to secure the largest enterprise, service provider, and government organizations worldwide. Together, we empower you with intelligent, seamless protection across the ever-expanding attack surface.

Whether expanding your AWS footprint, securing hybrid cloud assets, or migrating to AWS, our unparalleled expertise, solutions, and services secure your applications and workloads across your cloud and hybrid environments and help you take on the ever-increasing performance requirements of a borderless network today and tomorrow.

Contact your Presidio representative today to secure your cloud journey.

About the authors:
Troy Gerber, Director, Cloud & Application Security at Presidio
Matt Larkin, National Global Leader for Fortinet & Presidio
Chris Wilson, Strategic Alliance Director - Universal SASE Solutions, Fortinet

Presidio.com

PRESIDIO® FORTINET® aws