

A More Secure Everywhere

Key Requirements to Protect Your Journey to the Cloud

The cloud is now mainstream. Gartner estimates that the total cloud market will grow from US\$182.4 billion in 2018 to \$331.2 billion in 2022 at a compound annual growth rate (CAGR) of 16.1%.¹ That's no surprise considering the near-instantaneous benefits: rapid innovation; new and faster routes to market; and new, better ways to acquire, satisfy, and retain customers—the core ingredients of longevity and success for any business.

Despite the accelerated pace of cloud computing adoption, concerns grew among cybersecurity professionals in 2018. Nine out of 10 cybersecurity professionals now say they are concerned about cloud security, an increase of 11% from the prior year's survey results.² If cybersecurity professionals are increasingly concerned, what does that mean for the C-suite and other business leaders?

"There is currently a massive land grab for applications and workloads as the conversion to cloud accelerates. The existential question is who will benefit – and who is staring at oblivion?"

– 451 Research³

The cloud has landed a firm position as a strategic business initiative, and for many organizations, it is the next wave of evolution—but that doesn't change the facts. Today's enterprises are widely distributed. Your users are everywhere, accessing the tools and information they need from a flurry of devices, and your data and applications now reside in a multitude of cloud environments, including private and public clouds, spanning infrastructure-, platform-, and software-as-a-service (IaaS, PaaS, and SaaS) offerings.

With the cloud comes uncertainty, which ultimately creates hesitation in the journey. Enterprises lose their sense of familiarity, not to mention visibility and precise control. Coupled with dramatic increases in complexity, this results in new business risk and operational inefficiencies.

Traditional Cloud Security Approaches Are Insufficient

There's no shortage of security options when moving to the cloud, but many are designed to address only a small subset of security concerns. Acquiring multiple point products to secure the many types of clouds—public, private, and SaaS—can drive up complexity and eradicate the anticipated savings from using the cloud in the first place.

Instead, security should take a holistic view of the cloud—one that consistently provides access controls, protects data, and prevents threats across all cloud environments and infrastructure. The right approach centers around simple management and architecture, which help avoid issues that often stem from the use of non-integrated point products, such as extra operational overhead as well as improper use and misconfiguration of protections.

According to Gartner, through 2023, at least 99% of cloud security failures will be the customer's fault.⁴

1. "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019," Gartner, April 2, 2019, <https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g>.
2. "2018 Cloud Security Report," Cybersecurity Insiders, accessed May 22, 2019, <https://start.paloaltonetworks.com/cloud-security-report-2018>.
3. "2019 Trends in Cloud Transformation," 451 Research, accessed May 22, 2019, <http://go.451research.com/2019-Cloud-Trends-Preview.html>.
4. "Innovation Insight for Cloud Security Posture Management," Gartner, January 25, 2019, <https://start.paloaltonetworks.com/innovation-insight-for-cloud-security-posture-management.html>.

A Holistic Security Approach: The Missing Link

Recent research by ESG indicates a clear desire for vendor and technology consolidation. Why? Tighter product integration leads to a host of other positive security outcomes.

Top 3 Benefits of Buying Cybersecurity Products and Services from a Single Vendor ⁵		
44%	34%	34%
Improved security efficacy	More process automation	Better operational efficiency

Figure 1: ESG survey results

"36% of organizations use between 24 and 49 different security products while 19% use more than 50 different products from an assortment of vendors."

– ESG⁶

There are currently more than 1,000 security technology vendors on the market, many providing just one type of security capability, but many organizations are actively looking to replace point products with product suites that take a holistic approach to security. A shift in the balance of power—toward enterprise-class cybersecurity vendors with broad portfolios of products and services—is likely on the horizon.

Innovation Fosters Complexity

Organizations find themselves at various stages of digital transformation. At the cornerstone of the transformative process, regardless of where an organization may be in the journey, is the cloud. The cloud can help companies bridge the gap between what they can deliver today and meeting evolving customer expectations in the future. With the cloud come scale, flexibility, adaptability, and rapid development, which can dramatically spur innovation. For many businesses, the cloud represents a clean slate—an opportunity to streamline infrastructure and minimize overall complexity.

The journey to the cloud, however, is not a linear one, and organizations may choose to migrate to the cloud in a multitude of ways. The resulting complexity is the enemy of security. To overcome this complexity and succeed in the cloud, organizations must demand security technology that can quickly and effectively scale with changing business needs.

"These days, value in the cloud comes from reliability and stability, and finding ways to let organizations do things they otherwise couldn't."

– 451 Research⁷

Introducing Prisma by Palo Alto Networks

Prisma™ by Palo Alto Networks is the industry's most complete cloud security offering for today and tomorrow. It provides unprecedented visibility into data, assets, and risks in the cloud; consistently secures access, data, and applications without compromises; enables speed and agility as organizations embrace the cloud; and reduces operational complexity and cost with a radically simple architecture.

Regardless of how your business is taking advantage of the cloud, Prisma secures your end-to-end cloud journey:

- **Secure access:** Take advantage of secure access to the cloud from branch offices and for mobile users in any part of the world without compromising the user experience.
- **Secure SaaS:** Bring together data protection, governance, and compliance to safely enable SaaS application adoption.
- **Secure public cloud:** Get continuous security monitoring, compliance validation, and cloud storage security capabilities across multi-cloud environments. Plus, simplify security operations through effective threat protections enhanced with comprehensive cloud context.

5. "Toward Enterprise-class Security," ESG, May 2019.

6. Ibid.

7. "What's on the Minds of Cloud-Focused CTOs in 2018?" 451 Research, accessed May 22, 2019, <http://go.451research.com/what-is-on-mind-of-cloud-focused-CTOs.html>.

Drilling down further, Prisma addresses specific use cases to ensure optimal security outcomes at every stage of your journey to the cloud.

Optimal Security Outcomes Spanning the Cloud Journey	
Use Case	Prisma Outcomes
Cloud-Enabled Mobile Workforce	<p>Remote access VPN was not designed for cloud applications. Proxies, secure web gateways, and DNS filtering were not designed for consistent protection or user experience.</p> <p><i>Your cloud-connected mobile workforce needs consistent security wherever they are in the world. Prisma Access delivers protection from the cloud that makes access to the cloud secure.</i></p>
Cloud-Connected Branch	<p>Your branch networking strategy is changing as your organization adapts to use the cloud. Make sure your security strategy is ready to adapt as well.</p> <p><i>Prisma Access protects branches and retail locations with cloud-delivered security everywhere you need it.</i></p>
Zero Trust Cloud Security	<p>As your applications shift to the cloud, you can't rely on traditional network security to secure access, but that doesn't mean you have to lose control.</p> <p><i>Take control of your cloud environments with Prisma Access. Apply Zero Trust principles for secure access to public cloud, private cloud, and SaaS applications.</i></p>
Cloud Governance and Compliance	<p>Ensuring compliance is becoming harder than ever given expanding usage of cloud services.</p> <p><i>Prisma continuously monitors your distributed multi-cloud environments and SaaS applications, proactively alerting you of any misconfigurations or compliance violations, and automates remediation so you can embrace the cloud with confidence.</i></p>
Cloud Data Protection	<p>An organization's data is spread across multiple cloud storage environments and SaaS applications with varying levels of visibility and control, leaving the level of risk and exposure unknown.</p> <p><i>Prisma enables discovery, classification, monitoring, and protection of data with automated remediation before leaks can occur.</i></p>
Cloud Threat Protection	<p>Non-integrated security controls lack cloud context and fail to detect advanced threats, leading to alert fatigue among your security teams.</p> <p><i>Prisma helps you with simplified security operations and continuous, effective cloud threat protections augmented with comprehensive cloud context.</i></p>
Secure DevOps	<p>Embedding security early in the software development lifecycle requires controls that are automatable and API-driven.</p> <p><i>Prisma provides open security APIs and automated security controls that integrate with your CI/CD pipelines.</i></p>

Digital transformation is a balancing act for the C-suite. Although whether the business should move the cloud may no longer be a question, there's still much discussion to be had around how, what, and whom to bring alongside your enterprise to secure the journey. Done right, the journey to the cloud can unite disconnected lines of business, starting with the security team. Once thought of as a roadblock to innovation, your security team can now be seen as a strategic business partner that enables other key facets of your business. With a cloud-forward mindset and approach, and the right suite of integrated security, your business can take advantage of the cloud with confidence.

To learn more, visit the [Prisma Resource Center](#).



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. a-more-secure-everywhere-ds-082919