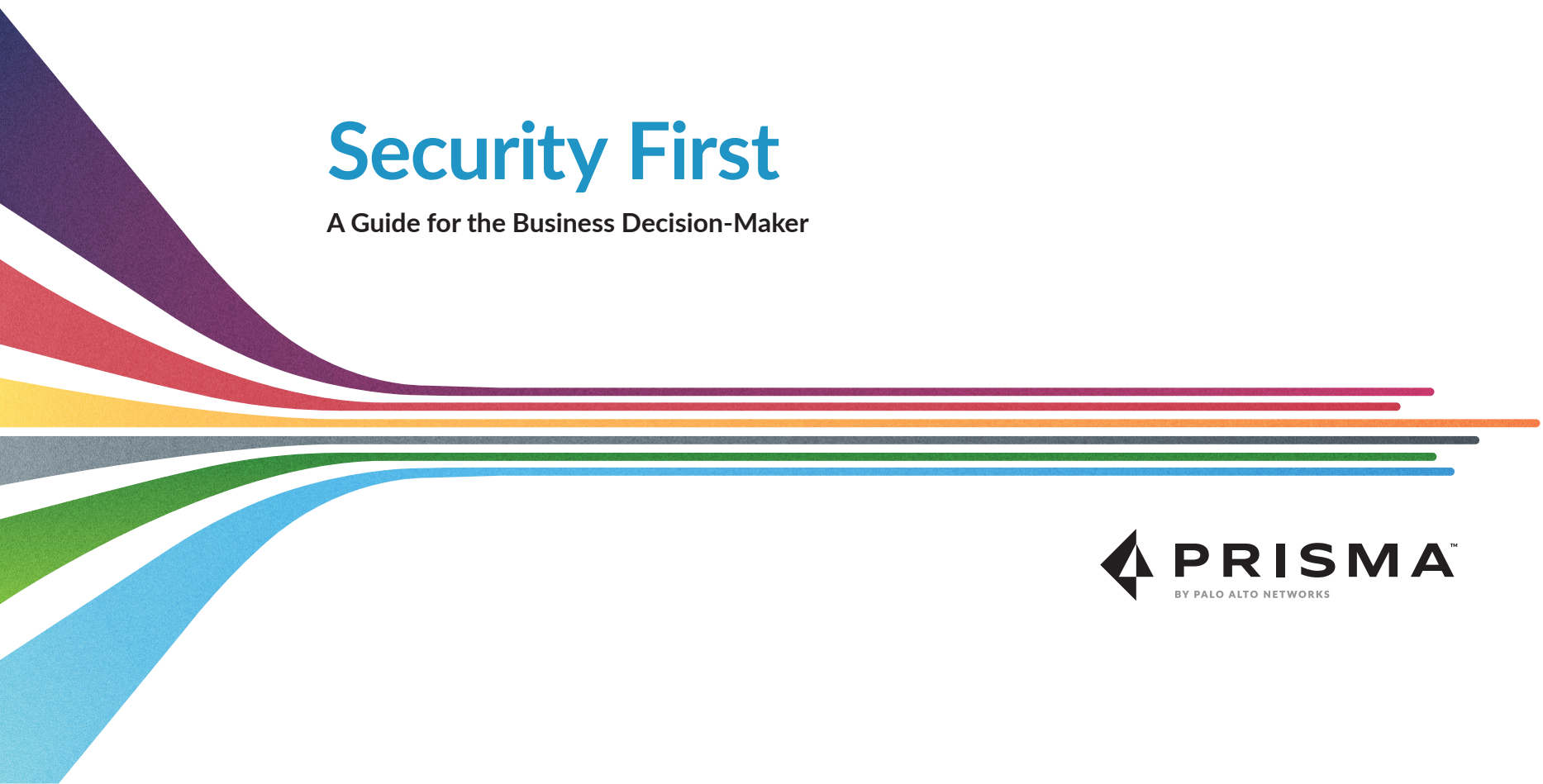
Security First

A Guide for the Business Decision-Maker



PRISMA™
BY PALO ALTO NETWORKS

The State of Cloud Security

One of the most important challenges for CIOs and CISOs is having visibility into their cloud security and being able to manage what happens within. If they can't identify where security or compliance gaps exist, there's no way to put the proper controls or protections in place. Without a roadmap for cloud security, the problems will only get worse.

Look at the major breaches making headlines every week. Attacks are coming at companies from all angles, and it's a full-time job just to keep up. Applying security best practices is helping, but many are still paying a high price.

PRISMA™
BY PALO ALTO NETWORKS

To amplify the importance of cloud security, consider the state of the cloud:

- **Public cloud growth:** Organizations are using public cloud services more than ever. According to a recent study from IDG, 76% of enterprises are looking to cloud apps and platforms to accelerate IT service delivery.[1]
- **Shadow IT:** More and more cloud applications are the results of shadow IT initiatives that are often out of security teams' control, deployed by line-of-business managers who may not be familiar with security and compliance best practices.
- **DevOps:** Developer teams continue to outpace security teams. They're deploying public cloud services on their own to accelerate development, and they don't want to be slowed down by security and compliance concerns.
- **Obsolete tools and technologies:** Traditional endpoint monitoring and remediation tools that have been effective in data center environments are simply not effective in securing the public cloud.
- **Pace of change:** Cloud environments change too quickly for manual processes to keep up, assuming organizations can even find and retain personnel experienced in managing cloud security and compliance.

---

1. "2018 Cloud Computing Survey," IDG online, last modified August 14, 2018, https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/.

Automation = Visibility = Continuous Security and Compliance

So, how do CIOs and CISOs gain the visibility they need to minimize risk and maximize protection? As with many questions in IT today, the answer is automation. By automating monitoring, analysis, and remediation across the entire cloud environment, security teams can gain the visibility they need to address their biggest cloud security and compliance challenges.

The architecture of the cloud makes it a perfect fit for an automated approach to security and compliance. Because the architecture of the cloud is based on an API model, organizations can deploy cloud-native, agentless products to give IT, security, and developer teams tremendous flexibility and visibility.

With an automated model, CIOs and CISOs can:

Get a big-picture view across their multi-cloud environments with centralized management and control.

- Allow DevOps and other teams to manage their own cloud deployments with automated controls for best practices in security and compliance.
- Lower costs as well as reduce complexity and risk by replacing manual tasks with automated processes.
- Flag and prioritize risks as well as remediate threats before they affect operations, availability, and compliance.
- Accelerate time to value by securely taking advantage of the public cloud to empower smaller developer teams and individual lines of business.

Public cloud services are creating opportunities for CIOs and CISOs to deliver significant value to their organizations through cost savings, agility, and accelerated development cycles. However, along with those opportunities come risks. The biggest of these–and the most important challenges to overcome–relate to security and compliance. Fortunately, there is a path to success through automation. Now's the time to take the first step: the intersection of security and compliance.

PRISMA™ BY PALO ALTO NETWORKS

Apply a Security-First Approach to Compliance

Security and compliance are shared responsibilities in the public cloud. Although many organizations make the mistake of believing that because public cloud providers manage the security and compliance of the cloud, providers are also responsible for these things in the cloud, this is not the case. It's your data, and your company is ultimately accountable for breaches or compliance violations. It won't do any good to point to a cloud provider and assign blame. Your revenue, your reputation and your customer relationships are at stake—not the cloud provider's.

The security-first model focuses on continuous monitoring and management of cloud security risks and threats, using modern tools and automation techniques to ensure the organization is aware of and prepared to address vulnerabilities. This demands the ability to identify threats in real time, understand their severity, and immediately act to remediate through automated policies, processes, and controls.

PRISMA™
BY PALO ALTO NETWORKS

Benefits of the Security-First Model

An approach that allows continuous monitoring and management of security in the cloud according to policy will give IT and security teams greater assurance that the organization will be compliant within the required frameworks. Among the benefits of this model, it enables you to:

Compile a complete unified view across all cloud accounts.

- Identify, prioritize, and remediate security risks as they arise.
- Monitor compliance throughout the entire development lifecycle and generate compliance reports without the need for specialized knowledge.
- Avoid events that disrupt developer teams with last-minute compliance fire drills.
- Demonstrate to auditors that the organization is managing security 24/7 year-round, not just in the last few weeks before an audit.
- Speed investigation through automated reconstruction of events across networks, endpoints, and clouds.

Continuous compliance automation also helps your compliance and DevOps personnel. Compliance can respond more quickly to third-party security audits, making security a competitive differentiator. Development teams don't get bogged down with stopping projects for yearly compliance audits.

Fortunately, some modern security offerings have been designed specifically to meet the challenges of public cloud environments. With a modern approach, organizations can take advantage of a security-first model that enables continuous visibility through automation. This strengthens security and gives compliance and developer teams the tools they need to meet the requirements of the cloud era.

PRISMA™
BY PALO ALTO NETWORKS

The Intersection of DevOps and Security

Developer teams are under enormous pressure to accelerate development cycles and improve quality assurance. Demands for speed, accuracy, and cost savings are also driving DevOps' growing reliance on cloud services.

In the long run, lack of coordination between DevOps teams and security teams is counterproductive. If there is a breach or compliance violation, the entire business suffers not just from lost revenue, but also from damage to the organization's reputation and customer goodwill.

In addition, if a security or compliance risk comes up late in the development cycle, it can cause software bugs and serious delays in availability.

DevOps adoption of cloud services rose to 78% in 2017, according to RightScale.[2]

2. "RightScale 2017 State of the Cloud Report Uncovers Could Adoption Trends," RightScale, February 15, 2017, https://www.rightscale.com/press-releases/rightscale-2017-state-of-the-cloud-report-uncovers-cloud-adoption-trends.

PRISMA™ BY PALO ALTO NETWORKS

The Need for Automation, Continuous Security, and Compliance

DevOps teams know all too well that today's development cycles leave no time to stop for security evaluations before the delivery of new products and features to the business. The answer to this problem is to deploy a modern approach to cloud security founded in automation.

With automation, developer teams can ensure security best practices are deployed and enforced without hindering the speed, accuracy, or quality of their work. Automation enables continuous security and compliance to support continuous development.

This model helps developers avoid bugs and delays in addition to alleviating some of the stress and conflict inherent in the relationship between developer and security teams.

PRISMA™
BY PALO ALTO NETWORKS

Here's how key stakeholders can benefit from a continuous security and compliance model as well as participate in its success:

- **Developer teams** can deliver quality products with less concern about security bugs. With the monitoring capabilities they gain from continuous security and compliance, they can catch unexpected risks or errors much earlier in the development cycle. In addition, they gain a learning tool to deliver better code. As they spin up new infrastructure for new projects, they can rely on built-in, preapproved protection, accelerating development cycles.
- **Security teams** can get out of reactive mode and take more control over DevOps and other shadow IT initiatives. We've seen developer teams outpace security to the point that security teams now struggle to even understand what kinds of infrastructure services their DevOps teams have deployed. Continuous security and compliance can help monitor when hundreds or thousands of code changes are being pushed into production.
- **Operations teams** can accelerate development cycles and improve quality assurance. Plus, a continuous security and compliance model is simpler to manage as well as less risky, and enables DevOps and security teams to work together.

By using a modern, cloud-native approach to security and compliance as well as taking advantage of automation and the API-centric architecture of the cloud, developer teams can enjoy accelerated development cycles while reducing the risk of delays or breaches. This is a winning formula for DevOps that will also ease the stress on security teams, IT leaders, compliance officers, and corporate management.

An Automated Approach to Cloud Security and Compliance

If you're responsible for IT, security, or compliance, you can reduce costs, improve protections, and assert greater control over cloud deployments and shadow IT.

If you're in DevOps, you can move quickly, without waiting for approval from security, while eliminating the potential for disaster that always looms if proper security and compliance checks and balances are not in place.

With the right cloud security, your organization can use automation to reduce risk and minimize the human element in vital processes. Automation allows you to achieve complete, continuous visibility across your cloud deployments, enabling consistent duplication among usage environments, such as development, staging, and production.

Cloud deployments move too quickly and can change too rapidly for organizations to rely on manual resources. The challenge is that most organizations still use legacy tools, technologies, and practices to manage cloud security and compliance.

PRISMA™
BY PALO ALTO NETWORKS

Fortunately, new cloud-native offerings are available that deliver agentless security and compliance checks designed specifically for modern public clouds. These take advantage of the cloud's API architecture to derive tremendous flexibility in scaling and management. The following describes the steps required of a modern, automated approach to continuous cloud security and compliance:

- **Step 1—Monitoring:** The cloud environment is consistently changing. These changes can encompass the routine activities of your DevOps or IT teams as well as the work of people who would do harm to your business. As changes are made across all clouds, regions, and services, your cloud security must monitor the configurations of the infrastructure to ensure it adheres to security and compliance best practices.
- **Step 2—Evaluation:** Your cloud security must securely collect data about your cloud services and continuously perform checks against a series of predetermined best security practices. It must also perform checks against any predefined custom signatures to determine, on a continuous basis, if there are any potentially exploitable vulnerabilities.
- **Step 3—Deep Analysis:** Your security should then analyze misconfigurations and exposures to determine whether to rank them as high-, medium-, or low-risk.
- **Step 4—Automated Remediation:** The resulting analysis should be displayed on a dashboard and be ready to be sent to integrated systems to kick off auto-remediation workflows.
- **Step 5—Detailed Reporting:** Detailed reports should provide your teams with comprehensive information about your risk, including user attribution and affected resources.
- **Step 6—Correction:** Afforded everything they need, your teams should be able to use easy-to-follow remediation steps to get your infrastructure back to a secure state.

Four Ways to Improve Cloud Security

The cloud requires a new way of approaching security. Traditional data center and endpoint security technologies and methodologies are inadequate to protect the highly connected architecture of the cloud, leaving your environment vulnerable. However, you can address the cloud's inherent risk-related challenges by employing a modern, cloud-native security model that uses automation to provide continuous monitoring, analysis, and remediation for cloud security and compliance. This model provides comprehensive protection in the cloud.

As you continue to rely on public cloud to drive day-to-day business activities and innovation, you must reduce security risks and simplify the processes to ensure protection and compliance. Continuous, automated security and compliance allow you to maximize the value of the public cloud while minimizing risk. To achieve this, security experts recommend focusing on four key elements:

1. Rapid Discovery to Keep Up with the Fast Pace of Change in the Cloud

With the growing volume of cloud deployments, it isn't unusual for organizations to have millions of data points that need to be evaluated. You need security that can handle all the data in real time and rapidly isolate any variation or deviation from known states.

PRISMA™
BY PALO ALTO NETWORKS

2. A "Single Pane of Glass" to View Your Entire Cloud Environment

When teams are very large, communication can be challenging. Your model should let teams own their own security while also giving security operations teams and corporate management a big-picture view. Your security must be able to evaluate data in isolation, as part of the global customer base, or across time and geography, to warn about potential issues before they occur.

3. Automated Response

You need to automate monitoring, analysis, and remediation to keep up with the volume of threats. You should have flexibility in determining the course of automated response and be able to inform human administrators if any other action may be required.

4. Detailed Reporting

Your teams need to be able to measure as well as demonstrate security and compliance progress daily, not just during yearly audits. With the right product, you should be able to view your past and present security and compliance stances at the push of a button.

PRISMA™
BY PALO ALTO NETWORKS

Is Your Business Prepared?

Prisma™ Public Cloud (formerly RedLock) analyzes more than 10 billion events every month. That analysis shows us that poor configuration, permissive behaviors, and lack of policies lead to many openings for bad actors and unidentified risks to exploit. Taking a security-first approach to your cloud environment will help keep your data safe and enhance your organization's credibility with stakeholders.

By proactively detecting security and compliance misconfigurations as well as triggering automated workflow responses, Prisma ensures you continuously meet the demands of your dynamic cloud architectures.

Experience the benefits firsthand with our free, 30-day Prisma Public Cloud trial.

CLICK FOR A FREE TRIAL

PRISMA™
BY PALO ALTO NETWORKS