Bitdefender® Global Leader In Cybersecurity

CSPM: A Pragmatic Approach to Closing the Cloud Security Gap

English

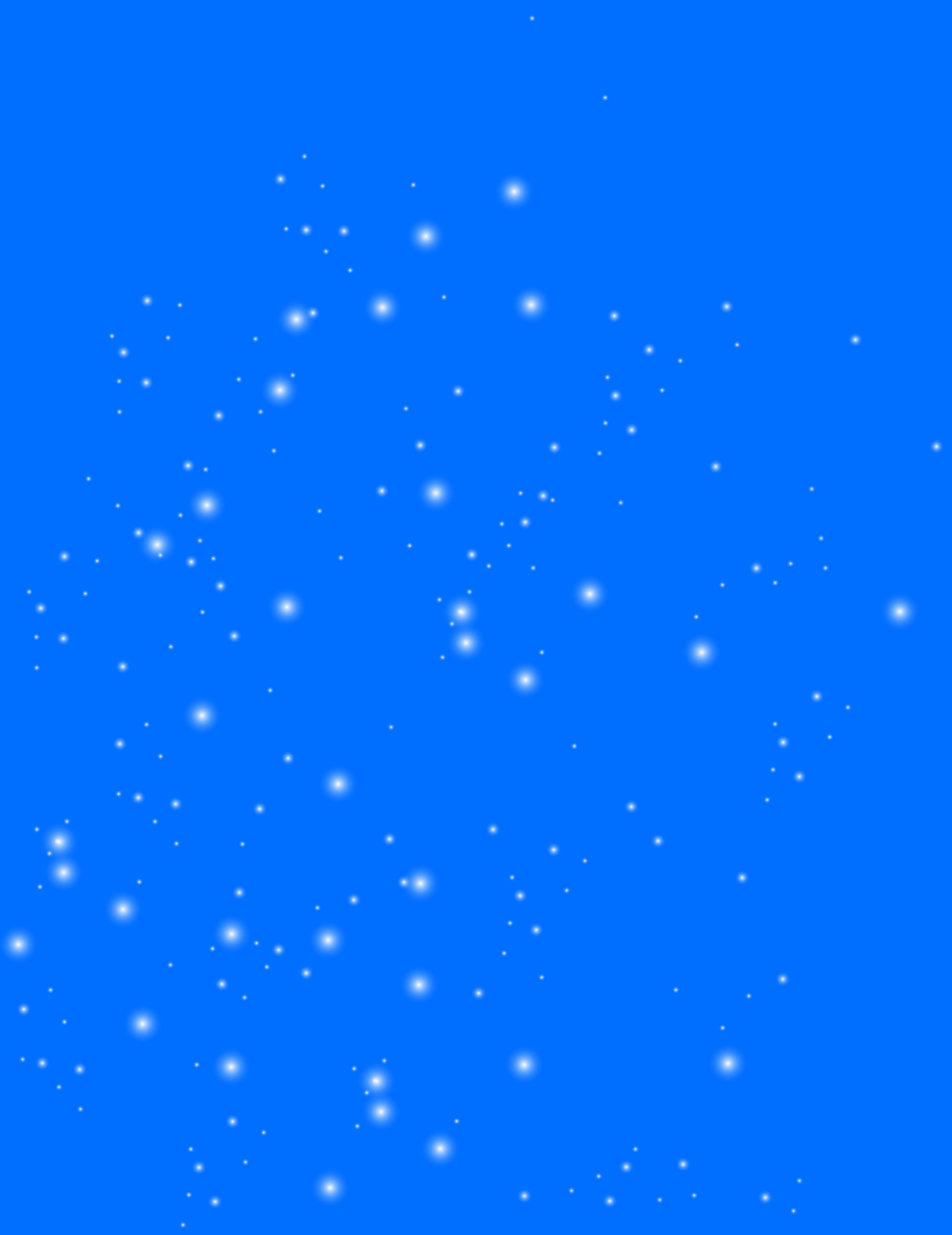


Table of Contents

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 180 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Bitdefender® Global Leader
In Cybersecurity

Introduction

As the public cloud makes up more and more of the IT infrastructure, organizations grow increasingly aware of the need to prioritize cloud security. However, cybersecurity teams don’t grow in proportion to their organization’s cloud infrastructure. In fact, due to a global workforce shortage**, cybersecurity departments are struggling with resource issues. In addition to being understaffed, teams lack the training or knowledge required to meet compliance, cyber insurance, and customer requirements in the cloud.**

Fortunately, cloud security has matured, and solutions have reached the necessary level of sophistication to enable a pragmatic approach to securing the public cloud. In other words, providers have found a way to make cloud security accessible. These modern solutions simplify the complexity of cloud security and enable teams to overcome the resource constraints that prevent them from making measurable improvements in their cloud security posture.

The best part: a modern, pragmatic approach to cloud security is outcome driven. It allows organizations to close the gaps and make measurable improvements in cybersecurity and regulatory compliance. By taking one step at a time, organizations can establish a cloud security foundation that enables new business opportunities, like expanding into new markets, while meeting compliance, cyber insurance and customer requirements in the cloud.

Kickstarting Your CSPM Journey: Mastering Shared Responsibility

The first step on a cloud security journey is understanding the organization's responsibilities. This might sound obvious, but the shared responsibility model used by cloud service providers can be a source of confusion for organizations as they move from on-premises to the cloud.

Cybersecurity teams are accustomed to being fully responsible for securing their organization's on-premises infrastructure. Moving to the cloud offloads some of the responsibility to the cloud service provider, resulting in a common misunderstanding that the customer has less security responsibility in the cloud than they do on-premises. However, the responsibility isn't less—it's just different.

Cloud providers are responsible for ensuring the security of the cloud infrastructure and services, including the underlying hardware, network, and software components. Customers are responsible for securing their data, applications, identity and access management, and configurations within the cloud environment. But these domains cannot be compared to their on-premises equivalents.

The reality is customers are responsible for ensuring the security of their cloud workloads, which operate on the cloud platform. Cybersecurity teams must understand how to implement security controls within the platform management plane where, compared to on-premises, the scale, granularity, and complexity are multiplied, and the rate of change is accelerated.

From Visibility to Vigilance: Elevating Cloud Security with Compliance

Cybersecurity teams can't protect what they can't see, and cloud and multi-cloud environments are growing increasingly complex. To fulfill their responsibilities in the shared responsibility model, organizations need visibility into the resources that are running on the public cloud. As providers add new platform features and service offerings, the number of configurations multiplies. Teams can be faced with configuring thousands of platform settings—while under pressure to deliver functionality as soon as possible—with little or no visibility into the impact of those configurations.

Organizations also need to understand the misconfigurations in their cloud environment and how they create security gaps and lead to compliance violations. Many regulatory and standards requirements are vague and must be translated into the appropriate, cloud-specific controls. Translating these requirements and tracking configuration settings is a major challenge. Similarly, organizations struggle to find overprivileged identities, which represent significant risk in the cloud.

Many organizations move to the cloud to improve the speed of delivery and innovation. To take advantage of these benefits, organizations need security that keeps pace with the cloud. Annual penetration tests and security reviews don't cut it in an environment that changes multiple times every single day. Visibility and compliance must be automated to match the pace of change in the cloud.

> *Annual penetration tests and security reviews don't cut it in an environment that changes multiple times every single day. Visibility and compliance must be automated to match the pace of change in the cloud.*

CSPM 101: Understanding the Backbone of Cloud Security

A Cloud Security Posture Management (CSPM) solution provides the visibility and compliance capabilities organizations need to fulfill their security responsibilities in the public cloud. A CSPM identifies and remedies misconfigurations and compliance risks within cloud environments and delivers comprehensive visibility across complex, multi-cloud environments.

By managing the cloud's scale, granularity, complexity, and rate of change, a CSPM solution addresses challenges that organizations typically encounter when protecting their cloud workloads. A CSPM collects and analyzes configuration data across the cloud environment to identify and surface potential risks and vulnerabilities in a cloud-native way, which means it can analyze multi- and hybrid cloud environments. This is done continuously to detect misconfigurations that can increase risk by leaving an organization vulnerable and introduce compliance lapses.

A CSPM also translates compliance requirements to each cloud provider environment, and then automates critical security tasks to provide cloud compliance expertise across a number of regulatory standards such as GDPR, banking regulations, and/or voluntary standards like SOC2 and ISO 27001. This is done by identifying areas of non-compliance, providing contextual analysis, and ensuring security policies are enforced across an entire cloud environment.

> *A Cloud Security Posture Management (CSPM) solution provides the visibility and compliance capabilities organizations need to fulfill their security responsibilities in the public cloud.*

5 Best Practices for Implementing CSPM

While CSPM has matured to make cloud security accessible to the majority of organizations, solutions are not one size fits all. When choosing and implementing a CSPM solution, consider the following.

01

Look for a Good Fit

A pragmatic approach to cloud security requires a CSPM that fits your existing cybersecurity team. Look for a solution that simplifies cloud security and overcomes resource constraints. It should be plug and play, and deliver immediate value. While the first CSPM tools were initially too “noisy,” newer ones are designed to minimize alert fatigue and provide contextual analysis. When evaluating CSPMs, consider whether the solution limits issues to one-line descriptions or provides detailed explanations that are accessible to those who have less experience in cloud security.

02

Don’t Forget About Identity and Access Management

Cloud security isn’t just about platform configuration. It’s also about managing permissions. Organizations use thousands of cloud services from file storage to load balancing, and it’s nearly impossible to know what entity is accessing what asset and why. Look for a CSPM that manages and secures identity and access management in cloud environments, ensuring that permissions are appropriate, and enforcing the principle of least privilege.

03

Keep it Actionable and Outcome-Driven

Choose a CSPM that actively reduces the burden of cloud security and doesn’t add to it. For example, alerts should not only include security findings but also instructions on how to resolve them, enabling administrators to confidently take immediate action with step-by-step instructions available right in the console. The CSPM should also monitor and measure compliance to demonstrate outcomes and assist the cybersecurity team in meeting SLAs.

04

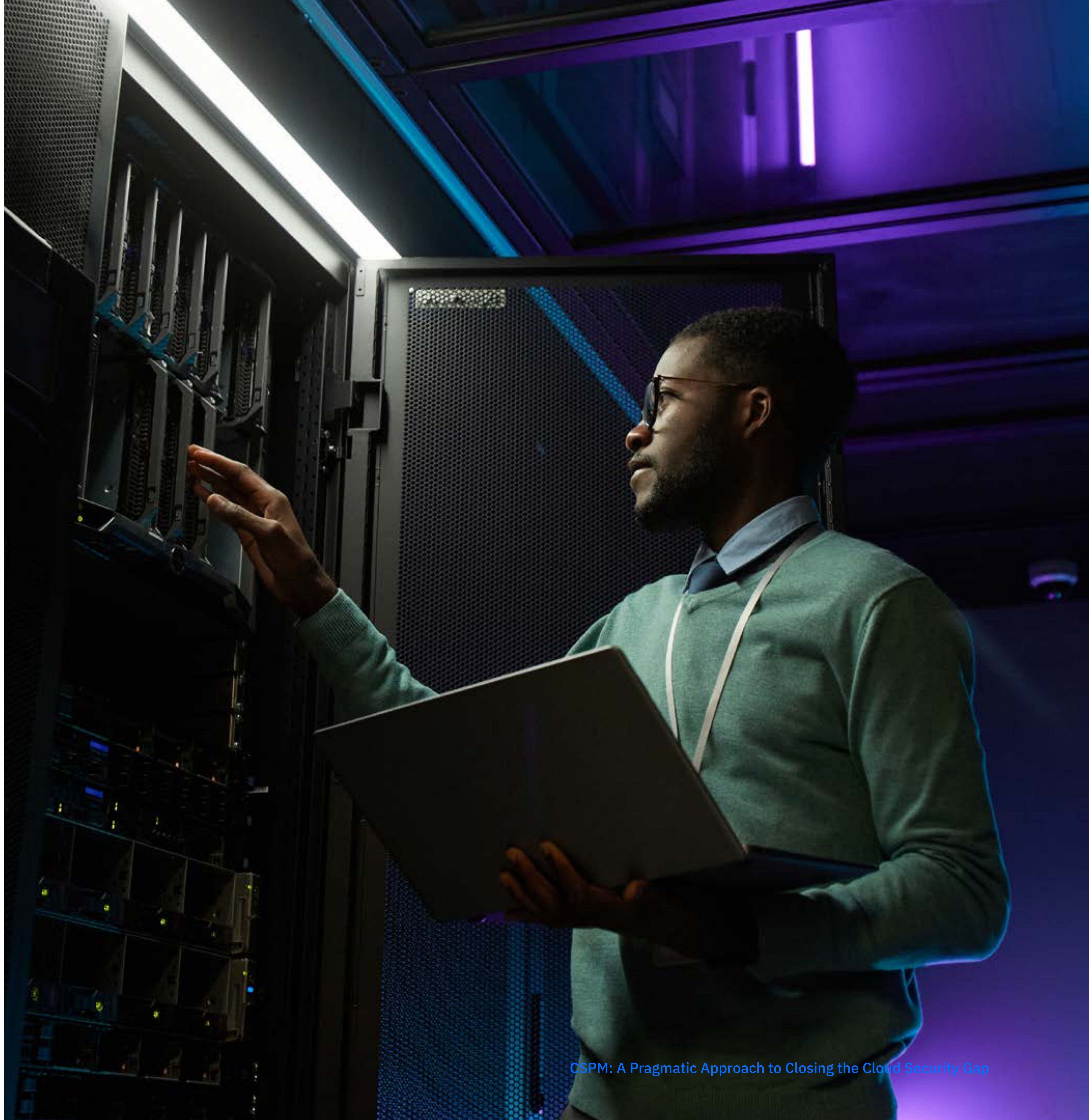
Build a Program Around CSPM

Technology alone does not solve cloud security challenges. It’s important to build a program around the CSPM solution that provides on-going coverage and involves the teams that will be implementing fixes. This means creating a process for taking action on the visibility delivered by the CSPM solution. A program is necessary for ensuring cloud security success.

05

Take One Step at a Time

Identifying gaps in coverage is critical when planning to bring your posture up to the recommended standards. But be careful to take one step at a time to avoid becoming overwhelmed. Your CSPM should allow you to follow basic cybersecurity guidelines like those published by CIS. Then, once you have your bases covered, you can add more industry- or organization-specific guidelines and regulations that make sense for your business.



Beyond CSPM: Building on a Strong Foundation

A CSPM is the foundation from which cloud security matures. The prevention achieved via a CSPM solution must be followed by protection—defeating active threats at the workload and container level—and detection and response at the endpoint and across the enterprise.

But the cloud doesn't exist in a silo. For optimal manageability, the visibility delivered via a CSPM should seamlessly integrate with the organization's full digital footprint. Ideally, this means employing a unified platform that encompasses both cloud environments and all other digital assets, rather than focusing exclusively on one area.

Bitdefender GravityZone CSPM+ gives organizations the visibility and compliance capabilities they need to establish a solid foundation in cloud security. Bitdefender GravityZone CSPM+ enables organizations to manage their security and compliance risks without requiring deep cloud security expertise and broad teams. GravityZone CSPM+ simplifies the assessment, monitoring, and management of cloud infrastructure configurations and ensures identities accessing resources are valid to enforce set policies, adhere to regulatory compliance, and help minimize risk of cybercriminal exploitation or abuse.

With GravityZone CSPM+ you get all this plus:

- Cloud risk visibility—Inventory your cloud assets, find and prioritize misconfigurations and over privileged identities to lower risk.
- Compliance mapping—Eliminate high-profile manual efforts to quickly surface problematic configurations based on your compliance needs.
- Threat detection and response—Detect threats and leverage actionable, human-readable outcomes in the graphical interface.

GravityZone CSPM+ also enables organizations to mature their security programs. CSPM+ forms Bitdefender Cloud Native Security when combined with Cloud Workload Protection delivered by GravityZone Cloud and Server Security and GravityZone Security for Containers.

GravityZone CSPM+ is powered by the GravityZone Platform, a unified security and risk analytics platform that provides advanced endpoint protection including endpoint detection and response (EDR), extended detection and response (XDR), and security across physical, virtual, and multi-cloud environments. The platform delivers deep security context to detections and offers a seamless path to Bitdefender Managed Detection and Response (MDR) services.

Bitdefender®

Trusted. Always.