Bitdefender

WHITEPAPER

Online Version Only

The Ultimate Guide to CSPM+

Trusted. Always.

Contents

Foreword

Cloud Security Posture Management (CSPM) solutions have the potential to be a major security asset for organizations leveraging cloud computing. The ability for a single tool to aggregate security and compliance risks from a myriad of evolving cloud instances and services — and in many cases, automatically reduce these risks — severely handicaps attackers who target this exploding attack vector in the cloud.

> "82% of breaches involved data stored in the cloud. Organizations must look for solutions that provide visibility across hybrid environments and protect data as it moves across clouds, databases, apps and services."

IBM Cost of a Data Breach Report 2023

To help businesses better select a CSPM solution that suits their needs, this whitepaper documents the common factors for CSPM purchases based on responses from prospects and customers using public cloud.

An Introduction to CSPM

As organizations adopt cloud services, they may be exposed to an expanding attack surface because of the complexity introduced by the sheer number of configurations available. The gaps left exposed by misconfigurations can lead to security breaches, data leaks, or compliance violations. CSPM, or Cloud Security Posture Management, addresses these issues by continuously scanning cloud environments to detect misconfigurations, vulnerabilities, and deviations from best practices, preventing potential exploits. Coined by Gartner as a category of security products that help automate security and provide compliance assurance in the cloud, the term is defined as following on their website:

> "Cloud security posture management (CSPM) consists of offerings that continuously manage IaaS and PaaS security posture through prevention, detection and response to cloud infrastructure risks. The core of CSPM applies common frameworks, regulatory requirements and enterprise policies to proactively and reactively discover and assess risk/trust of cloud services configuration and security settings. If an issue is identified, remediation options (automated or human-driven) are provided."

CSPM also ensures regulatory compliance by enforcing security policies, automates security monitoring and remediation to reduce human error, and enhances visibility by providing a centralized view of cloud security. Key components of this tool include continuous monitoring, policy enforcement, vulnerability assessment, threat detection, and remediation workflows, collectively safeguarding cloud environments and bolstering cybersecurity.

Key Takeaways

- ↳ The widespread adoption of public cloud, coupled with a lack of cloud security experience, increases the risk profile of organizations by increasing their attack surface
- ↳ CSPMs give organizations the tools they need to stop the leading cause of cloud data breaches: misconfigurations
- ↳ Organizations who are considering CSPM solutions should prioritize features including resource inventory, risk prioritization, and compliance management

A Growing Security Concern: Misconfigured Cloud Infrastructure

Over the last few years, cloud adoption has become mainstream with a growing number of organizations moving from small-scale proof of concepts to large deployments and embracing a cloud-first strategy.

Unfortunately, the skills and expertise required for cloud technologies - in particular around security - has not been able to match this rapid acceleration of adoption and has left many organizations ill-equipped to manage the digital journey. By 2025, only 50% of enterprises will develop skills for infrastructure automation across hybrid and multi-cloud platforms, up from less than 10% in 2021, according to Gartner.

> "By 2025, a single, centralized cybersecurity function will not be agile enough to meet the needs of a digital organization."
>
> Gartner

The most viable approach for tackling this skills shortage is to leverage automation and tooling to supplement security teams. This requires expertise baked into the processes and software which enable organizations to scale security outcomes faster than the size of their security teams. Cloud security and management is a constant work-in-progress and the combined effort of multiple teams. If the investment in automation integrated within workflows has a higher return than the cost, then short-term effort of deployment will be saved many times over by reducing the burden of manual efforts on teams, freeing them to focus on high-value projects.

Classifying Cloud Security Controls for Public Cloud

The move to public cloud has radically changed the paradigm of how infrastructure is managed and secured. Largely due to the introduction of new technologies, the central management plane - sometimes referred to as control plane - of public cloud allows infrastructure and services to be provisioned, modified, and deleted instantly at the click of a button or with a single line of code.

The shift also introduces the concept of a shared security responsibility model into the relationship between the Cloud Service Providers (CSP) like Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure and their customers. This model changes who handles the security requirements, who the assumed security risk resides with, and has implications on how organizations should handle compliance requirements.

Thus, traditional security controls that have historically worked well for on-premises environments need to be adapted and tuned towards cloud environments for them to be effective. Although conceptually similar, security approaches need to take into consideration the much larger diversity, granularity, scale and pace of change that come with cloud environments.

Some of the most important security controls are still applicable within a cloud context and can be broadly divided into the following categories:

- ↳ Identity and Access Management
- ↳ Network Protection
- ↳ Data Protection
- ↳ Audit Logging and Monitoring

Identity and Access Management

Identity and Access Management (IAM) encompasses policies and technologies crucial for governing digital identities and access privileges within your organization. These mechanisms wield the power to regulate entry into cloud resources, ensuring both authentication and authorization of users, the enforcement of access policies, and meticulous activity logging.

IAM provides the means to exercise control over:

- ↳ **Access Control:** Determining the identities permitted access to your cloud resources.
- ↳ **Authorization:** Specifying the actions authorized identities can undertake on these resources.
- ↳ **Temporal Control:** Dictating when authorized identities are allowed to carry out these actions.

Furthermore, IAM plays a pivotal role in compliance adherence by offering comprehensive audit trails and access reports, thereby showcasing the 'who,' 'what,' 'when,' and 'how' of user activities.

For instance, consider an application hosted on Amazon Web Services (AWS). With IAM, you can construct a policy granting the identity used by this application the ability to read data from an S3 bucket while prohibiting the capacity to modify or delete it. This ensures that only identities with explicit and distinct authorization can alter your data.

Key features integral to IAM solutions include:

- ↳ **Multi-factor Authentication (MFA):** Bolstering security with an additional layer of verification beyond passwords.

↳ **Role-based Access Control (RBAC):** Facilitating fine-grained control by associating permissions with distinct roles.

↳ **Least Privilege Access:** Restricting user privileges to the minimum necessary for performing their tasks, thereby minimizing potential security risks.

Network Protection

The transition to the cloud has revolutionized how networks are managed and defended, driven by the instant provisioning and modification capabilities offered by Infrastructure as a Service (IaaS) platforms. Cloud Service Providers (CSPs) like AWS, GCP, and Azure introduce a shared security responsibility model, altering the traditional division of security roles between providers and customers. This shift necessitates the adaptation of established security controls for on-premise environments to suit the cloud where the software-defined nature of network configuration leads to more segmented networks with fine-grained access control.

Within the spectrum of security controls, network protection remains paramount in safeguarding cloud-based infrastructures. It encompasses measures to secure communication channels, prevent unauthorized access, and mitigate potential threats.

Data Protection

Securing data in the cloud effectively is paramount for maintaining a strong security posture, particularly as organizations increasingly entrust critical or sensitive data to cloud environments. This security endeavor primarily revolves around the meticulous control of data access, adhering to the “need-to-know” principle, and proactively countering data exfiltration and tampering threats to safeguard the privacy and integrity of sensitive information.

Key controls in this domain encompass:

↳ **Data categorization and tagging:** Establishing processes and automation to appropriately tag sensitive data so that policies can be adapted to data sensitivity rather than general.

↳ **Configuration Logging:** Ensuring that native configuration logging is not only enabled but also properly configured to provide comprehensive insights into the state of your cloud environment.

↳ **Threat Detection and Inventory Tracking:** Leveraging native or external services for threat detection and tracking inventory configuration changes, allowing for early threat identification and responsive action.

↳ **Alerting for Critical Security Events:** Establishing alert mechanisms for critical security events such as unsuccessful management console authentication attempts or significant changes to network configurations, enabling swift incident response.

↳ **Proper Network Segmentation and IAM policies:** Implementing robust network segmentation and IAM access strategies to isolate resources and limit lateral movement, reducing the exposure of sensitive data to potential threats.

↳ **Denial of Unauthorized Communication:** Enforcing stringent controls that deny communication over unauthorized ports or to unauthorized addresses, further minimizing the attack surface.

↳ **Network Activity Logging:** Maintaining comprehensive records of network activity to monitor for any unusual or suspicious behavior, providing valuable insights for threat detection and response.

Audit Logging and Monitoring

Proper collection, management, and analysis of audit events are cornerstones of a robust security posture, serving as the bedrock for effective Incident Response and Management. This critical process enables organizations to not only detect but also comprehend and recover from cyberattacks swiftly and decisively.

Key controls within this domain encompass:

↳ **Comprehensive Configuration Logging:** Ensuring that native configuration logging is both enabled and meticulously configured to capture a comprehensive view of system activities and events.

↳ **Utilization of Threat Detection Services:** Leveraging services tailored for threat detection and the tracking of inventory configuration changes, thus enhancing an organization’s ability to identify and respond to security threats promptly.

↳ **Alerting for Critical Security Events:** Establishing alerting mechanisms for crucial security events, such as unsuccessful management console authentication attempts or significant changes to network configurations, enabling proactive responses and rapid incident resolution.

The Grave Consequences of Mismanaged Controls

Data Loss and Breach

Our CSPM technologies have found that 99% of cloud infrastructure scans conducted thus far revealed security vulnerabilities that could have led to data breaches. Breach of an organization’s systems leading to theft or loss of data is probably the most common public impact of unaddressed security risks in the cloud.

Theft of personal or publicly identifiable information is increasingly common and has the potential for serious reputational and financial implications for organizations depending on the amount and sensitivity of the data that was stolen.

This risk has been exacerbated recently by regulatory developments around privacy like GDPR and other regional equivalents, which has strict disclosure requirements and hefty fines.

Theft of an organization's intellectual property or trade secrets to gain a competitive advantage is another regularly seen but less publicized impact of data breaches, particularly in the case of state-sponsored actors.

Ransomware is another cause of data loss that is often top of mind for IT and security leaders but protection efforts often forget to consider cloud infrastructure. Insufficient security controls can allow malicious actors to encrypt data and systems stored in the cloud and hold it for ransom, without endpoint or network protection tools even having visibility that it has occurred.

If a robust backup and recovery plan was not previously put in place, recovery from such an event can be costly even without paying the ransom.

Compliance Violations

Violations of compliance requirements due to inadequate security controls can have a significant financial and operational impact on an organization.

For organizations in regulated industries such as finance, healthcare, services, or government, breach of compliance can, in very severe cases, lead to losing their license to operate.

Compliance standards like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), NIS2 and DORA in Europe, or the Monetary Authority of Singapore's (MAS) Cyber Hygiene Notices are applicable examples of this.

Some organizations may also have compliance requirements stemming from voluntary certifications such as ISO 27001 or SOC2, which may be a prerequisite for doing business with large enterprises that have strict vendor management processes in place.

In addition to the compliance standards listed above, all organizations, regardless of industry or choice, need to comply with a growing number of local privacy regulations. The painful financial impact of compliance violations is not felt by only the organizations hit by data breaches.

Organizations that fail to meet compliance requirements are also liable to be fined. Under the European Union's General Data Protection Regulation (GDPR) law, violators may be fined up to 4% of annual worldwide turnover or €20 million, whichever is greater.

Abuse of Cloud Resources

A weak cloud security posture can also lead to various types of abuse of cloud services and the unsanctioned use of an organization's cloud resources.

Malicious actors that gain access to cloud infrastructure will in some cases use the organization's infrastructure for greater anonymity when carrying out criminal activities such as:

- ↳ Hosting of malware in cloud storage
- ↳ Running command and control servers
- ↳ Storing stolen data after an attack on another organization
- ↳ Launching Distributed Denial-of-Service (DDoS) attacks

These types of misuse may make an organization unknowingly complicit in these activities and potentially liable to prosecution or fines.

Another type of abuse that is frequently seen is the use of an organization's cloud infrastructure to benefit from computing resources without paying. Most commonly, high-performance cloud instances will be launched in large numbers to mine cryptocurrencies for an attacker and racking up large bills with the cloud provider that the organization is left to pay. On a much smaller scale, employees may sometimes provision cloud resources for personal projects in the organization's cloud infrastructure, leading to increased costs and exposure for the business.

99% of cloud infrastructure scans have exposed security vulnerabilities that could have led to data breaches.

Financial Impact of a Data Breach

Data breaches have become a pervasive threat in today's digital landscape, with far-reaching financial implications for organizations of all sizes and industries. Beyond the immediate costs of remediation and legal repercussions, the financial impact of a data breach extends to reputational damage, lost customer trust, and long-term financial repercussions.

Understanding the full scope of these financial ramifications is crucial for organizations to make informed decisions regarding their cybersecurity posture. Preventing data breaches through robust security measures is not only a matter of protecting sensitive information but also safeguarding the financial stability and reputation of the organization in an increasingly data-driven world.

Cost of a Data Breach

According to IBM's Cost of a Data Breach report, the majority (82%) of data breaches in the report involved data stored in cloud environments, and 39% of breaches included data in multiple types of environments. In 2023, the average cost per record involved in a data breach was USD $165, which includes expenses related to the breach response, notification, legal fees, and potential regulatory fines. Moreover, organizations with more proactive and risk-based vulnerability management, such as vulnerability testing, penetration testing or red teaming, experienced lower than average data breach costs.

The report also states that newer technologies such as data security posture management (DSPM) can help find unknown and sensitive data across the cloud, including structured and unstructured assets within cloud service providers, software as a service (SaaS) properties and data lakes. With tools like CSPM, DSPM, CWPP (Cloud Workload Protection Platform), and more, cloud-forward data storage environments can be protected with continuous monitoring, vulnerability assessments, and remediation workflows.

IBM's X-Force is currently tracking over 3,200 cloud-related vulnerabilities, a 540% increase in the last six years, which signifies the scale of the risks associated with cloud computing.

Making The Case For A CSPM

A frequent question Security, Risk and IT leaders ask regarding CSPM is:

Why do I need a new tool for this? Surely my existing resources and tools can cover this.

Simple answer:

It depends.

The Manual Approach

A manual approach to addressing these problems would typically be in the form of quarterly or annual reviews of the configuration of infrastructure. The value of this approach is severely limited due to the scale and dynamism of cloud infrastructure.

What are the limits of a manual approach?

↳ **Scale:** A manual inspection of a single resource's configuration is easily done by a DevOps or Security team via the web console or Command Line Interface (CLI) of Cloud Service Providers (CSPs) but becomes impractical when considering the large number of different services, resource types and resources deployed in most organizations. Frequency of assessment is another.

↳ **Dynamism:** Manual reviews of configurations are very time-consuming and therefore can be performed only infrequently. This leaves a large window of opportunity for misconfigurations to go unnoticed and cause damage, as changes to the infrastructure can be introduced at any time during either the standard development process or by an administrator.

↳ **Cost:** Large security teams with highly customized needs and the necessary expertise can certainly consider building CSPM functionalities in-house, but this is generally much costlier than buying an out-of-the-box solution.

Alternative Tools with CSPM Functionalities

Tools like Cloud Access Security Brokers (CASBs), Cloud Management Platforms (CMPs) and Cloud Workload Protection Platforms (CWPPs) may help to address the risk of misconfigured cloud controls. These may already be deployed in existing cloud environments.

CWPPs are software platforms that monitor and protect cloud workloads, designed to address the requirements of server workload protection. CWPP tools may support container-based application architectures and hybrid data center architectures. With the right configurations, CWPPs can provide security and compliance teams the reports they require for internal audits and logging.

Likewise, CASB tools provide organizations with visibility and control across IaaS, PaaS, and SaaS, typically integrated with firewalls, detection capabilities, and traffic encryption. Organizations that already have CASBs may be able to pay an additional license fee to extend infrastructure monitoring services.

The difference in dedicated CSPM tools tends to be the wider range of cloud services assessed, providing more details about security posture in an organization's cloud infrastructure setup. That's why dedicated CSPMs are best suited for teams that process sensitive data in cloud.

What are the Cloud Security Risks?

The security risks in a cloud deployment are not fundamentally different from those in an on-premises infrastructure, however the relative importance of those risks will be very different due to the programmable nature of the cloud.

Lack of Visibility and Transparency

As cloud infrastructure typically follows a self-service model with application or project teams managing their infrastructure directly, centralized visibility into what is deployed can be a challenge. Security teams can't protect what they can't see, leaving invisible resources vulnerable as they may not be managed or monitored for risks.

Weak Authentication

Weak authentication is a key security risk in all enterprises across all IT services, and cloud infrastructure is no exception. Weak password policies or lack of multi-factor authentication are the primary risks to look out for here.

Excessive Account Permissions

Excessive account permissions go against the principle of least privilege access and may significantly increase the impact of a breach by allowing attackers to move laterally inside an organization.

Excessive Network Connectivity

Overly permissive access rules and resources directly accessible from the internet are the security risks behind some of the most publicized data breaches in recent times like cloud storage containers (AWS S3 storage buckets, Azure Blob Storage Container, GCP Cloud storage bucket) or databases publicly accessible. Attackers are continuously scanning IP ranges of CSPs for accessible resources that may be unprotected, and the inherent move away from perimeter security in the cloud has made these risks much more critical to monitor in the cloud than they were on-premise.

Insufficient or Improper Encryption

Lack of encryption can be a significant compliance risk when sensitive application traffic is not protected, opening the door to man-in-the-middle attacks. Equally important, for encryption to be effective in protecting data, organizations must use secure cryptographic schemes and appropriately managed encryption keys that are regularly rotated. This reduces the risk that older encryption standards with known weaknesses can be successfully exploited, giving an attacker only a very small window to take advantage of a compromised encryption key.

Insufficient Logging and Monitoring

If monitoring and logging are not properly set up, organizations will have a high risk of not being able to:

- ↳ Detect an intrusion or abuse early
- ↳ Understand the extent or impact of a breach i.e. which data was exfiltrated, how long an attacker remained in the network
- ↳ Respond to a breach appropriately to stop an attacker
- ↳ Know whether the attacker has retained access to the system

Logging is also essential to provide law enforcement with forensic information to help with a criminal investigation following a breach.

Defining CSPMs

Cloud Security Posture Management (CSPM) tools are security solutions dedicated to the continuous assessment and monitoring of the security and compliance of an organization's public cloud infrastructure.

At its core, CSPM functionality is the detection of cloud misconfigurations that put an enterprise at risk of security breaches or compliance violations. This is generally done via use of native cloud provider APIs to monitor the configuration of cloud resources against a desired security posture.

CSPM solutions are relatively new in the security market and have quickly gained traction by addressing security gaps left by both traditional on-premises security solutions like firewalls as well as cloud security solutions like CASB or CWPP.

CASBs primarily focus on the data plane and SaaS and are used as visibility and monitoring tools rather than for prevention and compliance. CWPPs focus on the protection of workloads themselves — OS, VM or containers — rather than how the infrastructure running these workloads is managed and configured.

CSPMs — Built for Cloud Security

Purpose-Built for the Cloud

CSPMs are built to address the unique nature these risks pose in a modern cloud deployment. As such, their areas of coverage are aligned with and match the most important risks organizations face in the cloud.

With the understanding that cloud deployments are the business of different functional teams, CSPMs come built-in with a variety of requirements, workflows, specializations, and expertise. This facilitates easier implementation of cloud risk management, with CSPMs handling most of the integration and translating of requirements between Compliance, Security, and Development teams.

Integrated Into the CSP Fabric

The technical approach taken by CSPMs to assess these risks — that of integrating directly with a CSP's APIs, rather than using agents or a proxy — gives them unparalleled visibility into the configuration of the cloud environment. Assessments are based on accurate, trustworthy, up-to-date, and comprehensive data coming directly from the CSP itself, and without affecting what is running in the cloud.

What to Look for in a CSPM

Resource Visibility

How do you protect what you can't see? The importance of visibility into your cloud workloads is without equal. A CSPM should continuously scan cloud environments for services, sensitive data, and instances that would otherwise be invisible and vulnerable to exploits.

Risk Prioritization

If everything is high priority, nothing is. A CSPM needs to recognize and provide comprehensive coverage of the cloud services most used by your organization. It is important for the CSPM provider to flag the areas of excessive risk through continuous scanning. This not only gives a snapshot of security posture, but also provides direction to the respective teams to address the risks.

Authorization and Authentication Checks

No identity in your organization needs more access than the minimum that it requires to perform its role. Anything more is an unnecessary security risk. Look for a CSPM that is able to assess your accounts and services for excessive entitlements and suggest authorization policies based on the principle of least privilege.

Built-In Compliance Reporting

Every organization has different compliance requirements and may face specific regulations in their place of business. CSPMs can extend the compliance support for recognized frameworks and standards including PCI DSS, ISO 27001, NIST, and GDPR. Some CSPMs even provide region or country-specific compliance support, allowing their customers to service their compliance needs in an all-in-one tool.

Some CSPMs go a step further and offer built-in compliance reporting for auditors, providing the auditor with complete mapping to the common compliance requirements.

Risk Management

CSPMs are built on the best practices and well-architected frameworks belonging to CSPs. On top of the risk flagging, CSPMs ought to provide the ability to modify risk ratings and prioritize remediation of these risks according to the organization's specific needs.

Security Posture Over Time

The ability to track historical information and past configurations facilitates digital forensics and incident response initiatives. CSPMs should be able to provide that evolution of security posture over time. Advanced CSPMs identify trends in configuration logs, helping to translate that information into automated risk prioritization.

Bitdefender GravityZone CSPM+

Defeat threats with a comprehensive and straightforward Cloud Security Posture Management Platform with real-time monitoring of threats across your multi-cloud infrastructure, while enforcing the Principle of Least Privilege with GravityZone CSPM+.

Automatically identify and map infrastructure configurations to compliance standards like PCI DSS, NIST, GDPR, SOC2, and ISO27001, in addition to many local standards such as MAS TRM, OJK, Thailand BOT, APRA and Korean ISMS-P, or your custom compliance needs, in a 10-minute no-code setup.

Cloud Automation On the Rise

The more organizations move their services to the public cloud, the more pertinent it is to leverage scalable solutions for secure configurations. When infrastructure and data is spread out across hundreds of different services, the need for automation of cloud configuration checks is stronger than ever.

CSPM tools from both CSPs and third-party vendors will continue to rapidly develop, and the many acquisitions of CSPM startups by vendors across the security landscape are a testament to this critical market. Organizations who already own CASB or CWPP solutions need to assess if the basic features there are sufficient for their growing infrastructure needs.

We hope this whitepaper has shed light on the important role of CSPM tools and the features organizations need to look out for in their purchase consideration. Continuously take stock of your security risks and your cloud needs down the line in order to pick a vendor that you can establish a long-lasting relationship with.

Afterword

In the rapidly evolving landscape of cloud computing, the importance of Cloud Security Posture Management (CSPM) cannot be overstated. As organizations across the globe continue to embrace the limitless potential of the cloud, they are also exposed to a growing array of security challenges. This whitepaper has elucidated the critical role that CSPM solutions play in safeguarding cloud environments, reducing risk, and enhancing overall cybersecurity.

CSPM goes beyond mere protection; it ensures regulatory compliance, automates security processes to minimize human error, and provides centralized visibility into cloud security. With CSPMs in place, organizations can effectively manage the risks associated with cloud infrastructure, prevent potential exploits, and mitigate financial and reputational damage caused by data breaches.

As we look ahead, the adoption of CSPM solutions is not just a cybersecurity imperative but a strategic necessity for any organization leveraging the cloud. With CSPM, organizations can confidently navigate the complexities of the cloud while fortifying their defenses against an evolving threat landscape.

CSPM is not just necessary; it is a cornerstone of modern cloud security.

Why CSPM?

Cloud Security Posture Management (CSPM) is an essential component of modern cybersecurity for several reasons.

- Firstly, the rapid adoption of cloud computing has expanded the attack surface for organizations, making it more challenging to ensure security. CSPM solutions play a pivotal role in continuously monitoring cloud environments to identify misconfigurations, vulnerabilities, and compliance gaps.

- Secondly, human error remains a significant contributor to security incidents. CSPM automates security policies, reducing the likelihood of misconfigurations and other human-related security lapses.

- Thirdly, regulatory compliance is a critical concern for many businesses. CSPM tools help ensure adherence to industry-specific regulations and standards, protecting against potential fines and reputational damage.

- Finally, in an era of sophisticated cyber threats, CSPM provides a proactive defense by detecting and responding to emerging security risks promptly. In conclusion, CSPM is necessary to secure the cloud, mitigate risks, maintain compliance, and fortify organizations against the evolving threat landscape.

In Conclusion

The trajectory of cloud adoption in recent years has been nothing short of remarkable, as organizations of all sizes have embraced a cloud-forward strategy. However, this rapid transition to the cloud has outpaced the development of the necessary skills and expertise, particularly in the realm of cloud security.

To bridge this divide, automation and robust tooling have emerged as vital allies to supplement human security teams. Automation not only augments the capabilities of security professionals but also accelerates the scaling of security measures. Recognizing the dynamic nature of cloud security, organizations are well-advised to automate wherever feasible, ensuring that security keeps pace with the ever-evolving threat landscape.

The transition to the cloud has reshaped infrastructure management and security paradigms, ushering in a shared security responsibility model between Cloud Service Providers and their customers. As organizations navigate this new landscape, traditional security controls must adapt to the unique challenges posed by cloud-based environments. Key security domains, such as Identity and Access Management, Network Protection, Data Protection, and Audit Logging and Monitoring, remain foundational pillars in securing Infrastructure as a Service (IaaS) cloud environments.

In sum, the journey towards securing the cloud is an ongoing evolution, demanding adaptability, automation, and a holistic approach that engages multiple teams within an organization. By recognizing these imperatives, organizations can effectively safeguard their cloud investments while fostering a resilient and agile security posture.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com