

The Quest for Visibility and Control in the Cloud

By Yuri Diogenes - ISSA Senior Member, Fort Worth Chapter 2019-03-20 18:52:29

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. This article will cover important considerations regarding cloud security visibility and control.

Abstract

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. From companies that are still in the process of migrating to the cloud to companies that are already building their infrastructure entirely in the cloud, the governance of cloud workloads can be difficult if not approached correctly and using the right tools. In addition, companies that need to adhere to certain compliance standards must understand the current security controls around their workloads and how they map to the standards that they need to be in compliance with. This article will cover important considerations regarding cloud security visibility and control.

ACCORDING TO “THE 2018 GLOBAL CLOUD DATA SECURITY STUDY” conducted by Ponemon Institute, ¹³ forty-nine percent of the respondents in the United States are “not confident that their organizations have visibility into the use of cloud computing applications, platform, or infrastructure services.” According to Palo Alto’s “2018 Cloud Security Report,” ¹⁴ sixty-two percent of the respondents said that misconfiguration of cloud platforms is the biggest threat to cloud security. What we have here is exactly the lack of visibility and control over different cloud workloads, which not only cause challenges during the adoption, but also slow down migration to the cloud.

In large organizations the problem becomes even more difficult due to the dispersed cloud adoption strategy. This usually occurs because different departments within a company will lead their own way to the cloud, from the billing to infrastructure perspective. By the time security and operations teams become aware of those isolated cloud adoptions, these departments are already using applications in production and integrated with the corporate on-premises network (figure 1).

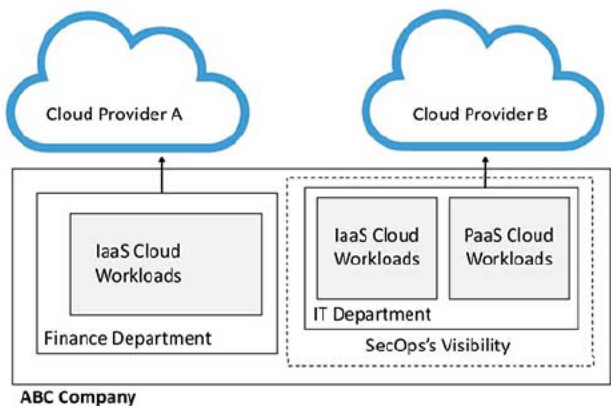


Figure 1 – An unstructured cloud adoption scenario can become a nightmare for the SecOps

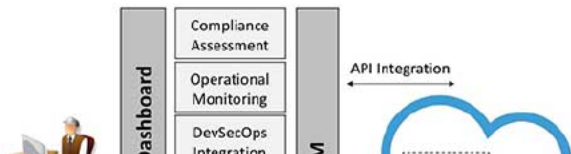
In addition to this unstructured approach, these adoptions usually are done without proper monitoring planning, and many times the attempt to leverage legacy tools to gain viability to cloud resources does not provide an accurate picture of the current security posture of those workloads. According to the Palo Alto Networks report, the “top two security control challenges SecOps are struggling with are visibility into infrastructure security (forty-three percent) and compliance (thirty-eight percent).”

To obtain the proper level of visibility across your cloud workloads, you can’t rely only on a well-documented set of processes; you must have the right set of tools. According to Palo Alto Networks, eighty-four percent of the respondents said that “traditional security solutions either don’t work at all or have limited functionality.” This leads to a conclusion that ideally you should evaluate your cloud provider’s native cloud security tools before even starting to move to the cloud. But many current scenarios are far from the ideal, which means you need to evaluate the cloud provider’s security tools while the workloads are already on it. This brings us to the discussion of two major categories of cloud security tools that are imperative these days:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)

Cloud security posture management

When talking about cloud security posture management, we are basically referring to three major pillars: visibility, monitoring, and compliance assurance. A CSPM tool should be able to look across all these pillars and provide capabilities to discover new and existing workloads (ideally across different cloud providers), identify misconfigurations, provide recommendations to enhance the security posture of cloud workloads, and assess cloud workloads to compare against regulatory standards and benchmarks. According to Gartner, a typical deployment pattern for CSPM has the layers shown in figure 2. ¹⁵



Orca Security Ltd.
Exhibit 2137
Wiz v. Orca
IPR2024-01109, -01190, -01191
Ex. 2137-001

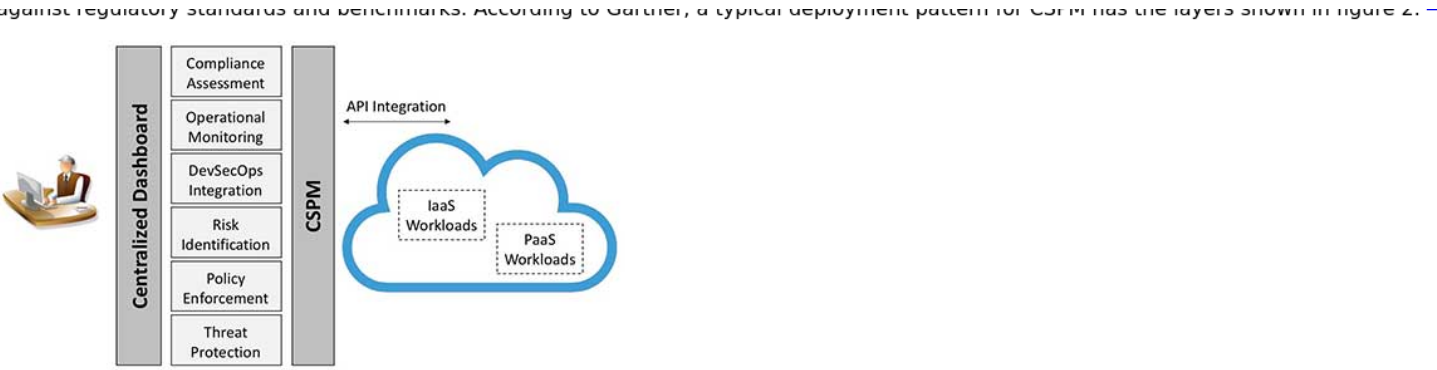


Figure 2 – CSPM capabilities

Each layer is responsible for retrieving the relevant data across the different workloads, rationalize it, and providing the output via a dashboard. Some layers may also have the capability to integrate with external work flows, for example, to send emails or to trigger remediation tasks in case a pre-determined threshold is reached. Table 1 has general considerations for each one of those capabilities of the layered model described in figure 2.

CAPABILITY & CONSIDERATIONS

- **Compliance Assessment:** Make sure the CSPM is covering the regulatory standards used by your company.
- **Operational Monitoring:** Ensure that you have visibility throughout the workloads, and that best practices recommendations are provided.
- **DevSecOps Integration:** Make sure it is possible to integrate this tool to existing work flows and orchestration. If it is not, evaluate the available options to automate and orchestrate the tasks that are critical for DevSecOps.
- **Identification:** How the CSPM tool is identifying risks and driving your workloads to be more secure? This is an important question to answer when evaluating this capability.
- **Policy Enforcement:** Ensure that it is possible to establish central policy management for your cloud workloads and that you can customize and enforce it.
- **Threat Protection:** How do you know if there are active threats in your cloud workloads? When evaluating the threat protection capability for CSPM, it is imperative that you can not only protect (proactive work) but also detect (reactive work) threats.

Table 1 – CSPM general considerations

Some cloud platforms will offer native CSPM solutions that are capable of mapping different regulatory compliance models to your workloads and provide recommendations for security controls. The example shown in figure 3 is from the Azure Security Center regulatory and compliance feature, with the compliance control mapping for the monitored workloads located in Azure.

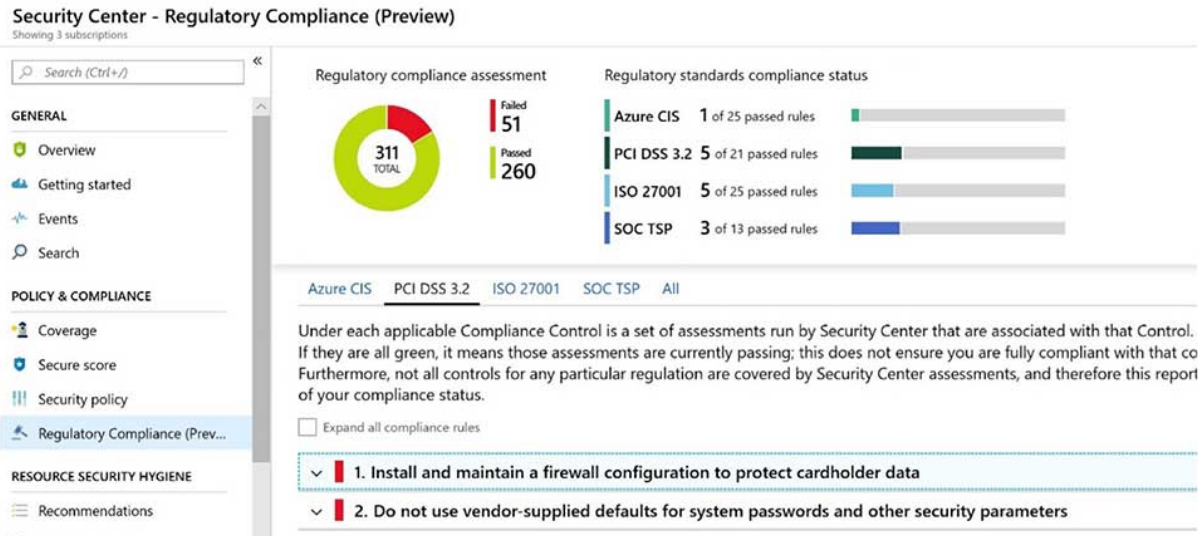


Figure 3 – Regulatory compliance features in Azure Security Center

Cloud workload protection platform

By now you can already conclude that having a CSPM is an important step towards securing your cloud deployment. But there are other aspects of cloud security that need to be addressed including hardening, configuration, network security (firewall, segmentation), protection against exploits, application whitelisting, and other in-depth security capabilities. To address those needs, you will need to use a cloud workload protection platform (CWPP) tool. Gartner also exemplified a typical deployment pattern for CWPP, as shown in figure 4 [16](#).



By now you can already conclude that having a CSPM is an important step towards securing your cloud deployment. But there are other aspects of cloud security that need to be addressed including hardening, configuration, network security (firewall, segmentation), protection against exploits, application whitelisting, and other in-depth security capabilities. To address those needs, you will need to use a cloud workload protection platform (CWPP) tool. Gartner also exemplified a typical deployment pattern for CWPP, as shown in figure 4 [16](#).

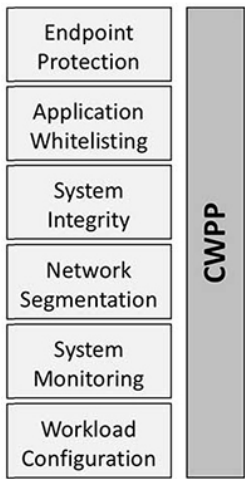


Figure 4 – CWPP deployment patterns

Cloud workload protection platforms that offer these deployment patterns enable customers to have more control and security over their enterprise workloads, containers, and storage across multiple IaaS public cloud deployments and also traditional on-premises data center environments (hybrid cloud scenario). Since CWPP is a more in-depth security protection, it can also have threat detections as part of the system monitoring capabilities. Let’s review some important considerations for each one of those capabilities of the layered model described in figure 4 (table 2).

CAPABILITY & CONSIDERATIONS

- **Endpoint Protection:** Make sure the CWPP can integrate with the current endpoint protection solution that is running on your IaaS workloads.
- **Application Whitelisting:** Ensure that you can whitelist applications that are running in your IaaS deployments.
- **System Integrity:** Make sure it is possible to monitor file integrity in Windows and Linux systems.
- **Network Segmentation:** Ensure you can harden virtual network traffic used by your IaaS workloads.
- **System Monitoring:** How do you monitor active events in Windows and Linux platforms? This is an important question that needs to be addressed by the CWPP. Ideally this should be seamless for IaaS workloads in the cloud, as well as on-premises resources in a hybrid cloud scenario.
- **Workload Configuration:** How to deploy workload configuration in scale by leveraging security best practices, another important consideration that should be covered by the CWPP.

Table 2 – CWPP considerations

Some cloud platforms will offer native CWPP solutions that are capable of mapping all suggested patterns described in table 2. Make sure to evaluate the options, as native cloud tools are usually able to offer some unique capabilities since the cloud provider owns the underlying infrastructure. The example shown in figure 5 is from the Azure Security Center file integrity monitoring capability that can monitor Windows and Linux platforms.

File Integrity Monitoring

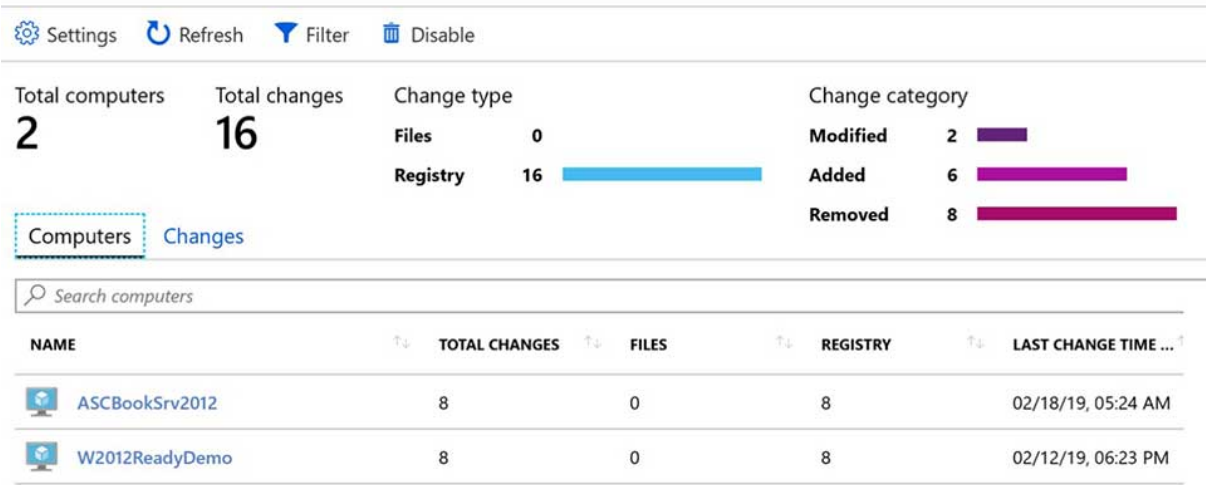


Figure 5 – File integrity monitoring in Azure

In order to provide in-depth security for your workloads, it is common that CWPP implementations are agent-based solutions. In a recent blog post published by Palo Alto Networks [17](#) they reported that analysis done in cryptominer code used by Berke group [18](#) identified that the malicious code was able to evade

Figure 5 – File integrity monitoring in Azure

In order to provide in-depth security for your workloads, it is common that CWPP implementations are agent-based solutions. In a recent blog post published by Palo Alto Networks ¹⁷, they reported that analysis done in cryptominer code used by Rocke group ¹⁸ identified that the malicious code was able to evade detection by uninstalling the cloud security protection and monitoring products from compromised Linux servers. Since this has the potential to become a new attack vector against CWPP, it is imperative to verify with your CWPP vendor if they have the capability to detect this attempt to evade detection.

Conclusion

Cloud security should be tackled from different angles, and as demonstrated in this article, a single approach may not cover all aspects that will enhance the security posture while keeping in-depth monitoring of the different cloud workloads. For this reason, CSPM and CWPP are solutions that should be prioritized during the planning phase of your cloud migration. For existing cloud deployments, it is important to review the design patterns of existing workloads, and ensure that the CSPM and CWPP solutions are capable of addressing current and future needs.

References

¹³ "The 2018 Global Cloud Data Security Study," Gemalto (Jan 2018) – <https://safenet.gemalto.com/resource/partnerasset.aspx?id=64424542279&langtype=1033>.

¹⁴ "2018 Cloud Security Report," Palo Alto Networks (May 2018) – <https://www.paloaltonetworks.com/resources/research/2018-cloud-security-report-palo-alto-networks>.

¹⁵ Richard Bartley, "Comparing the Use of CASB, CSPM, and CWPP Solutions to Protect Public Cloud Services," Gartner (August 2018) – <https://www.gartner.com/doc/3886773/comparing-use-casb-cspm-cwpp>.

¹⁶ Ibid.

¹⁷ Xingyu Jin and Claud Xiao, "Malware Used by 'Rocke' Group Evolves to Evade Detection by Cloud Security Products," Unit 42, PaloAlto Networks (Jan. 17, 2019) – <https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/>.

¹⁸ Ed Targett, "This Malware Turns Off Your Cloud Security Tools," Computer Business Review (Jan. 1, 2019) – <https://www.cbronline.com/news/rocke-group-malware>.

About the Author



Yuri Diogenes, CISSP, MS in Cybersecurity Intelligence & Forensics Investigation, currently works for Microsoft as Senior Program Manager for Azure Security Center. Yuri is also a Professor for the Master of Science in Cybersecurity course from EC-Council University. You can follow Yuri on Twitter @yuridiogenes or his website yuridiogenes.us, yurid@microsoft.com.

©ISSA. [View All Articles](#).

[The Quest for Visibility and Control in the Cloud](#)
<https://issa.mydigitalpublication.com/articles/the-quest-for-visibility-and-control-in-the-cloud>

Menu

- [Page View](#)
- [Contents View](#)
- [Issue List](#)
- [Advertisers](#)
- [ISSA.org](#)
- [YouTube](#)
- [Facebook](#)
- [Twitter](#)
- [LinkedIn](#)
- [Instagram](#)

Issue List

[January/February 2025](#)

[November/December 2024](#)

[September/October 2024](#)

[Julv-August 2024](#)

[January/February 2025](#)
[November/December 2024](#)
[September/October 2024](#)
[July-August 2024](#)
[March-April 2024](#)
[February 2024](#)
[January 2024](#)
[December 2023](#)
[November 2023](#)
[October 2023](#)
[September 2023](#)
[August 2023](#)
[July 2023](#)
[June 2023](#)
[May 2023](#)
[April 2023](#)
[March 2023](#)
[February 2023](#)
[January 2023](#)
[December 2022](#)
[November 2022](#)
[October 2022](#)
[September 2022](#)
[August 2022](#)
[July 2022](#)
[June 2022](#)
[May 2022](#)
[April 2022](#)
[March 2022](#)
[February 2022](#)
[January 2022](#)
[December 2021](#)
[November 2021](#)
[October 2021](#)
[September 2021](#)
[August 2021](#)
[July 2021](#)
[June 2021](#)

[September 2021](#)
[August 2021](#)
[July 2021](#)
[June 2021](#)
[May 2021](#)
[April 2021](#)
[March 2021](#)
[February 2021](#)
[January 2021](#)
[December 2020](#)
[November 2020](#)
[October 2020](#)
[September 2020](#)
[August 2020](#)
[July 2020](#)
[June 2020](#)
[May 2020](#)
[April 2020](#)
[March 2020](#)
[February 2020](#)
[January 2020](#)
[December 2019](#)
[November 2019](#)
[October 2019](#)
[September 2019](#)
[August 2019](#)
[July 2019](#)
[June 2019](#)
[May 2019](#)
[April 2019](#)
[March 2019](#)
[February 2019](#)
[January 2019](#)
[December 2018](#)
[November 2018](#)
[October 2018](#)
[September 2018](#)
[August 2018](#)
[July 2018](#)

[October 2018](#)
[September 2018](#)
[August 2018](#)
[July 2018](#)
[June 2018](#)
[May 2018](#)
[April 2018](#)
[March 2018](#)
[February 2018](#)
[January 2018](#)
[December 2017](#)
[November 2017](#)
[October 2017](#)
[September 2017](#)
[August 2017](#)
[July 2017](#)
[June 2017](#)
[May 2017](#)
[April 2017](#)
[March 2017](#)
[February 2017](#)
[January 2017](#)
[December 2016](#)
[November 2016](#)
[October 2016](#)
[September 2016](#)
[August 2016](#)
[July 2016](#)
[May 2016](#)
[June 2016](#)
[April 2016](#)
[March 2016](#)
[February 2016](#)
[January 2016](#)
[December 2015](#)
[November 2015](#)
[October 2015](#)
[September 2015](#)
[- - - - -](#)

- [November 2015](#)
- [October 2015](#)
- [September 2015](#)
- [August 2015](#)
- [July 2015](#)
- [June 2015](#)
- [May 2015](#)
- [April 2015](#)
- [March 2015](#)
- [February 2015](#)
- [January 2015](#)
- [December 2014](#)
- [November 2014](#)
- [October 2014](#)
- [September 2014](#)
- [August 2014](#)
- [July 2014](#)
- [June 2014](#)
- [May 2014](#)
- [April 2014](#)
- [March 2014](#)
- [February 2014](#)
- [January 2014](#)
- [December 2013](#)
- [November 2013](#)
- [October 2013](#)
- [September 2013](#)
- [August 2013](#)
- [July 2013](#)
- [June 2013](#)
- [May 2013](#)
- [April 2013](#)
- [March 2013](#)
- [February 2013](#)
- [January 2013](#)
- [December 2012](#)
- [November 2012](#)
- [October 2012](#)

[January 2013](#)
[December 2012](#)
[November 2012](#)
[October 2012](#)
[September 2012](#)
[August 2012](#)
[July 2012](#)
[June 2012](#)
[May 2012](#)
[April 2012](#)
[March 2012](#)
[February 2012](#)
[January 2012](#)
[December 2011](#)
[November 2011](#)
[October 2011](#)
[September 2011](#)
[August 2011](#)
[July 2011](#)
[June 2011](#)
[May 2011](#)
[April 2011](#)
[March 2011](#)
[February 2011](#)
[January 2011](#)
[December 2010](#)
[November 2010](#)
[October 2010](#)
[September 2010](#)
[August 2010](#)
[July 2010](#)
[June 2010](#)
[May 2010](#)
[April 2010](#)
[March 2010](#)
[February 2010](#)
[January 2010](#)
[December 2009](#)
[November 2009](#)

[February 2010](#)

[January 2010](#)

[December 2009](#)

[November 2009](#)

[October 2009](#)

[September 2009](#)

[August 2009](#)

[July 2009](#)

[June 2009](#)

[May 2009](#)

[April 2009](#)

[March 2009](#)

[February 2009](#)

[January 2009](#)

[December 2008](#)

[November 2008](#)

[October 2008](#)

[September 2008](#)

[August 2008](#)

[July 2008](#)

[June 2008](#)

[May 2008](#)

[April 2008](#)

[March 2008](#)

Library



< Contents View

The Quest for Visibility and Control in the Cloud

By Yuri Diogenes – ISSA Senior Member, Fort Worth Chapter

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. This article will cover important considerations regarding cloud security visibility and control.

Abstract

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. From companies that are still in the process of migrating to the cloud to companies that are already building their infrastructure entirely in the cloud, the governance of cloud workloads can be difficult if not approached correctly and using the right tools. In addition, companies that need to adhere to certain

The Quest for Visibility and Control in the Cloud

By Yuri Diogenes – ISSA Senior Member, Fort Worth Chapter

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. This article will cover important considerations regarding cloud security visibility and control.

Abstract

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. From companies that are still in the process of migrating to the cloud to companies that are already building their infrastructure entirely in the cloud, the governance of cloud workloads can be difficult if not approached correctly and using the right tools. In addition, companies that need to adhere to certain compliance standards must understand the current security controls around their workloads and how they map to the standards that they need to be in compliance with. This article will cover important considerations regarding cloud security visibility and control.

ACCORDING TO “THE 2018 GLOBAL CLOUD DATA SECURITY STUDY” conducted by Ponemon Institute, ¹³ forty-nine percent of the respondents in the United States are “not confident that their organizations have visibility into the use of cloud computing applications, platform, or infrastructure services.”

According to Palo Alto’s “2018 Cloud Security Report,” ¹⁴ sixty-two percent of the respondents said that misconfiguration of cloud platforms is the biggest threat to cloud security. What we have here is exactly the lack of visibility and control over different cloud workloads, which not only cause challenges during the adoption, but also slow down migration to the cloud.

In large organizations the problem becomes even more difficult due to the dispersed cloud adoption strategy. This usually occurs because different departments within a company will lead their own way to the cloud, from the billing to infrastructure perspective. By the time security and operations teams become aware of those isolated cloud adoptions, these departments are already using applications in production and integrated with the corporate on-premises network (figure 1).

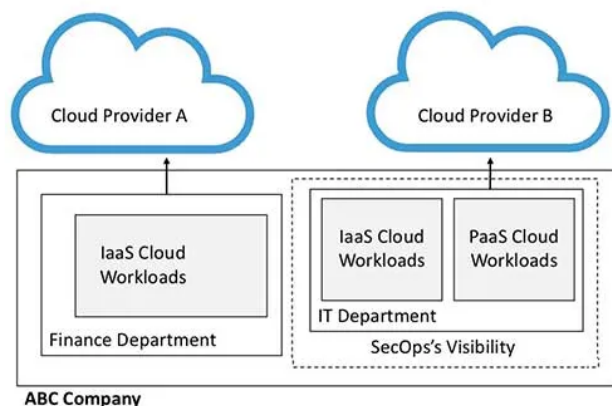


Figure 1 – An unstructured cloud adoption scenario can become a nightmare for the SecOps

In addition to this unstructured approach, these adoptions usually are done without proper monitoring planning, and many times the attempt to leverage legacy tools to gain visibility to cloud resources does not provide an accurate picture of the current security posture of those workloads. According to the Palo Alto Networks report, the “top two security control challenges SecOps are struggling with are visibility into infrastructure security (forty-three percent)

and compliance (thirty-eight percent).”

To obtain the proper level of visibility across your cloud workloads, you can’t rely only on a well-documented set of processes; you must have the right set of tools. According to Palo Alto Networks