Brought to you by Informa Tech

Publication date:
03 Oct 2022

Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Cyera offers posture management for cloud data

Summary

Catalyst

Cyera has developed a platform that continually discovers, classifies, protects, and monitors data in any cloud data store.

Omdia view

Cloud adoption was already growing exponentially before the coronavirus pandemic, but COVID definitely turbocharged the process. With millions of knowledge workers adopting home working out of necessity, all forms of cloud computing gained new momentum, a situation that also expanded organizations' attack surface: ever more corporate data finds its way into the cloud, not always with the appropriate governance controls in place. Shadow IT blossoms thanks to the ease of software-as-a-service (SaaS) adoption, test and dev environments leave datastores up and populated after a project is completed, or access controls on these cloud assets are overly lax.

Cloud data security platforms are now emerging to address such issues, offering organizations the ability to discover all cloud data stores in use within their ranks and impose policies on them to reduce their attack surface. Cyera is part of this trend and has the opportunity to gain market share in this still emerging segment, thanks to its agentless, API-based approach and both the speed and accuracy of its classification capability.

Why put Cyera on your radar?

Cloud data security is critically important, given the rate at which corporate data is headed into the cloud, and the ability to be proactive in classifying such data, highlighting potential issues with it, and addressing those issues before an attack takes place is an essential part of cloud governance.

With enterprise cloud adoption continuing to accelerate, just as data breaches and inadvertent disclosures continue to make news cycles, it is clear that infrastructure and application security approaches leave room for focused, data-aware protection to safeguard the data itself. Cyera enables these capabilities and should be on your list of potential suppliers for such technology, given its agentless, API-based approach and the speed at which it can classify data.

Market context

A widely used reference for security in cloud computing, and more particularly for the distribution of responsibility for that security between cloud service provider (CSP) and customer, is the Shared Responsibility Model. Its graphical representation consists of a series of “stacks,” starting with physical security at the bottom and moving up through host, network, application, IAM, and endpoint, before arriving at the data itself.

Some of these images have four stacks with the first one being the on-premises world, where the customer is responsible for everything. The stack for infrastructure-as-a-service (IaaS) shows the CSP assuming responsibility for the bottom few layers, then the platform-as-a-service (PaaS) stack has the provider responsible for a couple more. For the last of the stacks (i.e., SaaS), the CSP is responsible for everything, except the security of the data (this is sometimes further qualified by calling the top box “Data and Access,” since both are the responsibility of the customer. Indeed, the customer’s responsibility for that layer of the stack is the one constant across IaaS, PaaS, and SaaS.

This is an important consideration, as there is a presumption on the part of cloud computing customers that their CSP has shouldered the responsibility for everything, such that any data loss suffered in their environment will be automatically compensated for by the provider. This is not so, however, and Omdia is at pains to disabuse end users of this notion at every opportunity.

This situation favors technology vendors offering some form of data security for cloud environments, whether it be obfuscation technology, such as encryption or platforms such as cloud permissions management (CPM, aka CIEM), which looks at access rights to data and seeks to curtail them whenever they are excessive.

The emerging new technology in this space is what Cyera calls cloud data posture management (CDPM), which sets out to discover all the data stores a customer is using across multiple clouds, parsing and classifying them to provide context on not only the sensitivity/confidentiality of the data they hold, but also how the type of sensitive data represents security, privacy, and compliance risks, based on the identities that can access them, and the type of access that is occurring in the environment. Cyera then prioritizes recommendations and remediation steps to improve the organization’s security posture, and then monitors the environment on an ongoing basis to detect any changes that may adversely impact that posture. Indeed, one way of thinking about Cyera is as a change management platform for the cloud data plane.

Examples of such changes include if a new database has been created and personal identifying information (PII) is not encrypted, or if a new access granted to a given identity elevates the privacy risks or creates toxic combinations of data access to sensitive customer information. Aligned to the cloud security posture management (CSPM) space, Cyera’s technology provides context on alerts for publicly exposed S3 buckets, for example, by highlighting for security teams exactly the type of data that the S3 bucket contains, which helps security teams understand how serious the issue is—benign if the bucket contains public data, or severe if there is PII that is publicly accessible. The technology then delivers recommended actions for the customer’s IT and/or security team to take to remedy the situation.

Product/service overview

Cyera is agentless technology, relying instead on application programming interfaces (APIs) provided by the cloud service providers (CSPs) to access to its customers' entire cloud estate and, as such, can be deployed in a matter of minutes, requiring read-only access to be granted by the customer.

Once that is done, it spends up to a week in observation mode, mapping all the data stores the customer has in the cloud. This includes structured and unstructured data in IaaS (cloud infrastructure like AWS), PaaS (cloud platforms like Snowflake), and SaaS (cloud collaboration platforms like Microsoft 365) environments. Once that process is complete, it parses and classifies this data (including PII and other sensitive types of data) and surfaces the highest priority risks for remediation with suggested courses of action for that purpose. Cyera makes the point that a lot of existing "cloud security" products, such as cloud security posture management (CSPM) and SaaS security posture management (SSPM), manage the security posture of cloud infrastructure, whereas its technology focuses on the data and, as such, provides visibility, intelligence, and insights to remediate potential security risks.

Cyera sees a range of use cases for its technology, including:

The discovery and classification of cloud data

Security teams struggle to keep pace with data proliferation across their cloud environments, and the vendor considers one its key differentiators in this context to be the speed and accuracy with which it can classify data. DLP platform, including legacy approaches like BigID or cloud DLP solutions like AWS Macie or Azure Purview, require users to tell them what to look for, and most often to classify data themselves. Cyera manages hundreds of pre-defined data classes, and automatically creates new classes when it learns from a customer's environment. It works in a way that is similar to Google or iCloud photo—the AI/ML recognizes patterns in the data and suggests the data class to the user.

Part of this differentiation includes understanding when a datastore includes fake data, or de-personalized data. Based on the entropy of the data the engine observes, it makes a determination whether, for example, a field labeled Credit Card holds fake data, rather than throwing up false positive alerts suggesting that sensitive data is exposed. This is critical, given the permissive nature of the cloud and the way enterprises are attempting to enable product, development, and business strategy teams to leverage cloud data to accelerate digital transformation and customer engagement initiatives.

Minimizing cloud data risk

Cloud data sprawl increases the threat surface and exposes the business to increased threat of data compromise or loss, and this use case covers the pervasive challenge of shadow data. Shadow data represents unmanaged cloud data, which includes snapshots, copies, or logs that are not part of a primary data protection or backup and recovery scheme.

This also includes ghost data, which is a case where the data store of record has been removed or deleted, but the snapshots or copies persist in the cloud environment. This can increase a business's threat surface and heighten risk, for a variety of reasons. These can include exploits from ransomware gangs who might take advantage of weak or no security controls on the data, or violations of privacy schemes like GDPR, where ghost data represents ongoing data management requirement, even though there was no longer a viable business justification for it.

Improving cloud data policy management

Lax data management policies expose organizations to data losses, thefts, and breaches. This typically manifests in the form of production data in lower environments. Development teams and business units routinely leverage cloud data, and while best practices dictate that data shared to lower environments have sensitive data obfuscated or removed, this is all too often not the case.

Governing cloud data access

Overly permissive access to data, and a lack of governance over cloud environments violate data access policies and expose sensitive data to risk. This includes pursuing least privileged access to data, only granting access to the explicit data, using the lowest level of access possible to avoid misuse, including inadvertent disclosure.

Managing cloud storage risk and cost

Proliferation of data in cloud environments results in stale, unused, or orphaned data that costs a business money without delivering value, and worse, exposing it to the risk of a breach.

Company information

Background

Cyera was founded in 2021 by CEO Yotam Segev and CTO Tamar Bar-Ilan. Both men spent several years in the Israeli Defense Forces' Unit 8200 military intelligence unit, after which Segev was Senior Director of Cyber Projects at KayHut, a cyber research firm, while Bar-Ilan was Chief Architect at Linxight, a company that adds AI to standard security cameras as a safety measure in swimming pools.

The vendor has raised a total of $64.5m in funding, most recently announcing a $60m Series A round as it emerged from stealth in March 2022, led by Sequoia Capital, with participation from Accel, Cyberstarts, and René Bonvanie, CMO emeritus of Palo Alto Networks.

Cyera's eponymous security platform went on general availability in March 2022, the product launching with several paying customers already.

Current position

Cyera is still at an early stage in its development and is in competition for a bevy of other start-ups who have similarly identified a market opportunity, many of them originating in Israel. These include Laminar Security (founded in 2020), Dig Security, Polar Security, and Eureka Security (all of whom date from 2021). New York-based BigID is a little older, having been around since 2016.

Of course, the older generation of data discovery and security vendors such as Varonis are aware of the need to address cloud data, and against those players, Cyera and all the other cloud data security vendors highlight the fact that they are cloud-native in their approach, and as such as not shoehorning legacy technology into a cloud environment.

In addition, cloud platforms have all created their own DLP services. However, as previously noted, the shared responsibility model will limit the degree to which they invest in classification, and they have little incentive to perform discovery outside of their cloud environment. Microsoft Azure's Purview offering is marketed as supporting hybrid cloud environments, but classification is currently limited to native Azure data stores. As with BigID and Varonis, this leaves an opportunity open to the cloud data security startups like Cyera to differentiate their value proposition to enterprises.

As a SaaS platform, Cyera bills based on a subscription model. Pricing is managed in tiers, based on the volume of data and the number of data stores an enterprise connects the solution to.

Future plans

Cyera's platform is available globally and can scale to consume and classify massive volumes of cloud data. The team is growing rapidly, investing across product, engineering, and go-to-market teams to continue their rapid growth. From a technology perspective, investments are being made across three axes: providing context across more data stores and data, showcasing the identities that can access that data and the actions those identities are taking, and providing insight into the data usage and flows.

Data and Data Stores

Cyera is continuing to invest in automated discovery and classification to ensure customers gain visibility into the "unknown unknowns" in their environment. Additional data store support will include MongoDB Atlas, SAP HANA, Google Workspace, and additional collaboration tools including Salesforce and Slack as the platform matures.

Identities and Access

Cyera will continue to expand access graph capabilities to include security, privacy, and governance framework reporting, and "what if" scenarios to help security and privacy teams understand the risks of overly permissive access, and how to govern access requests to sensitive data.

Data Movement and Data Flows

Cyera customers have benefitted from the platform highlighting when sensitive data has been moved without prior security measures including encryption, tokenization, or obfuscation being applied. Cyera is focused on making the insights it provides actionable by integrating with third-party solutions that can apply data protection, manage identity and access management, and make Cyera's data context an integral part of an enterprise's cloud security process.

Key facts

Table 1: Data sheet: Cyera

Product/Service name	Cyera	**Product classification**	Cloud Data Posture Management
Version number	N/A (full SaaS)	**Release date**	March 2022
Industries covered	Financial services, Healthcare, Manufacturing, Business Services, Commerce	**Geographies covered**	North America, EMEA
Relevant company sizes	Enterprise and SME	**Licensing options**	SaaS/Subscription
URL	cyera.io	**Routes to market**	Direct, Channel, AWS Marketplace
Company headquarters	Tel Aviv, Israel	**Number of employees**	65

Source: Omdia

Analyst comment

Cyera has emerged from stealth this year at a time when cloud data security is a hot topic, as evidenced by the fact that several of its competitors were founded in 2021, like Cyera itself.

They all seek to address a need for proactive security around cloud data (i.e., finding all the cloud datastores in use and addressing any perceived issues making them susceptible to attack.) Indeed, Cyera's choice of the term cloud data posture management is itself a nod to the broader trend towards proactivity, with other platforms such as CSPM and SSPM vying for space in the growing market for cloud security (Omdia refers to the entire field of proactive security as security posture management, or SPM).

One risk that some of those platform face is that the CSPs themselves could move into the market. Indeed, Microsoft Azure already has a CSPM capability in place for a few years and is now developing SSPM. Could the same happen with cloud data security?

This eventuality cannot be ruled out, though to be fair, the CSPs have by and large avoided getting deeply into data security (at least beyond encryption, which they all offer). Some observers speculate that this may be reluctance on the CSPs' part to come more into scope (i.e., put themselves in the firing line of the multiple regulations covering data breaches.) If a customer loses data from their cloud and they were providing posture management for that data, the rationale goes, they might be liable for damages.

It remains to be seen whether the CSPs will stay out of CDPM, but for now at least, Cyera has a clear opportunity in this emerging market. Perhaps a more serious threat might come from established security players such as Palo Alto Networks, who have been buying up cloud security start-ups at a rate of knots in recent years. CDPM might well be an attractive addition to their portfolio, which of course could turn a threat to Cyera into an opportunity.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Cloud security – IaaS and PaaS (December 2019)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia’s consulting team may be able to help you. For more information about Omdia’s consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com