

SHOWCASE

Securing the Data for Cloud-native Apps and Data Ingestion Pipelines in AWS

Date: December 2022 **Author:** Jack Poller, Senior Analyst; and Melinda Marks, Senior Analyst

ABSTRACT: While deploying applications to the cloud with modern software development processes helps organizations better serve customers, partners, and employees, organizations need to secure their data as it moves to the cloud. Understanding configurations; whether the data is free of malicious code; and whether it contains intellectual property, financial data, personally identifiable information (PII), or other sensitive information is the key to ensuring data security. Organizations need a solution that can find and tag any sensitive data, scan data for malware, and apply safeguards to ensure data is protected from attacks targeting cloud storage.

Overview

Organizations are moving rapidly to the cloud, and, according to research from TechTarget's Enterprise Strategy Group, the growth of cloud-resident applications will continue. Currently, only 22% of organizations report that more than 40% of their applications are cloud resident; in the next three years, this will increase to 48% of organizations having more than 40% of their applications in the cloud.¹

Leveraging cloud service provider (CSP) services enables these organizations to efficiently deliver and update software applications. Object stores such as Amazon Simple Storage Service (S3) from Amazon Web Services (AWS) provide scalability, data availability, and performance for a range of use cases, including data lakes, websites, and enterprise applications.

Applications need to secure the data in managed storage services like S3. If an infected file is ingested and a user—a customer, partner, or internal user—downloads and opens the file, damage can propagate throughout their system. A common example is ransomware, and the results can be catastrophic, destroying the organization's data, damaging their reputation, and imposing cost penalties from lost business to regulatory fines.

Similarly, applications need to understand the diverse types of data being ingested and used and ensure only authorized users have access to sensitive data. Improper access can lead to data privacy violations, fraud, identity theft, and data exfiltration. As with malware, regulatory fines, reputational damage, and data loss can be debilitating.

CSPs have built their storage services to provide maximum flexibility and utility for applications and developers. This results in a vast and complex set of options and increases the likelihood that misconfiguration can lead to these security issues. Indeed, Enterprise Strategy Group research shows a broad range of common app and cloud service infrastructure misconfigurations (see Figure 1).²

¹ Source: Enterprise Strategy Group Complete Survey Results, [2023 Technology Spending Intentions Survey](#), November 2022.

² Source: Enterprise Strategy Group Research Report, [The Maturation of Cloud-native Security](#), May 2021.

This Enterprise Strategy Group Showcase was commissioned by Cloud Storage Security and is distributed under license from TechTarget, Inc.

Figure 1. Range of Cloud App or Service Misconfigurations

**Within the past 12 months, which of the following issues—if any—associated with the misconfiguration of a cloud application or service has your organization detected?
(Percent of respondents, N=383, multiple responses accepted)**

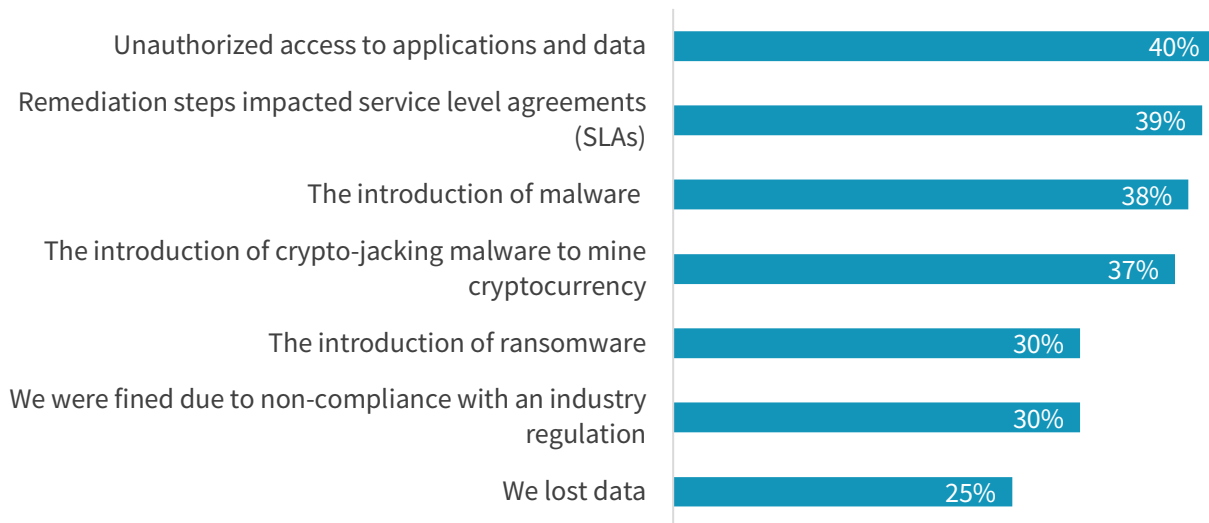


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations have experienced cybersecurity incidents, including unauthorized access, malware, ransomware, and crypto-jacking, as a result of misconfigurations (see Figure 2).³

Figure 2. Results of Misconfigurations

You indicated your organization detected at least one misconfigured cloud application or service in the last 12 months. What was the result of the misconfiguration(s)?
(Percent of respondents, N=350, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The publicity surrounding some major data breaches has raised the awareness of cloud misconfigurations, and sophisticated malicious actors are now directly targeting application vulnerabilities and cloud service and infrastructure configuration, with many attacks focused on data in object stores. More than one quarter (27%) have suffered from malware that has moved laterally to cloud workloads, and 25% have suffered targeted penetration attacks or had data exfiltrated from object storage (see Figure 3).⁴

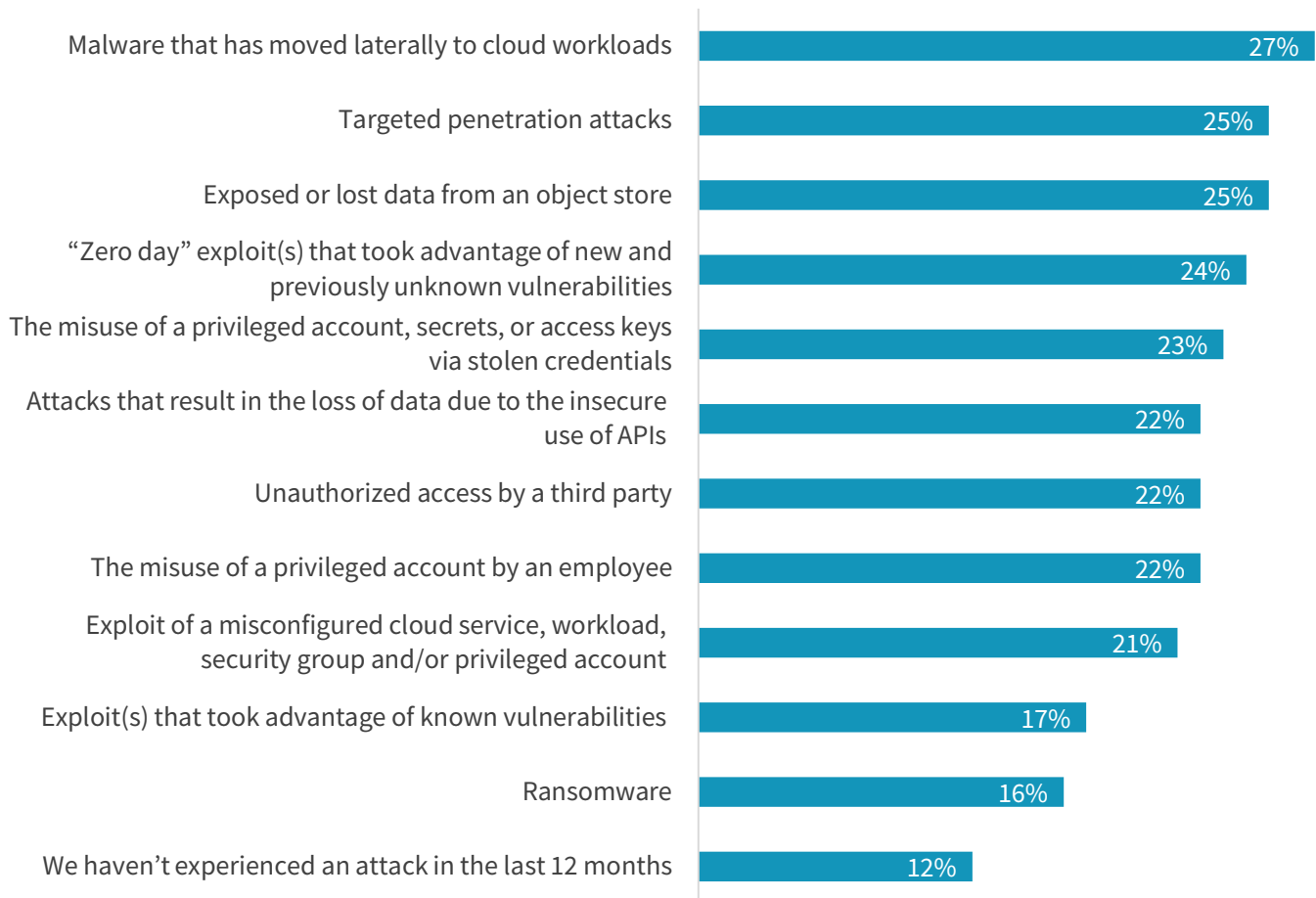
To minimize risks, organizations should incorporate security scanning for all objects in data stores in their development workflows.

³ Ibid.

⁴ Ibid.

Figure 3. Diversity of Cloud-native Application and Infrastructure Cybersecurity Incidents

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure? (Percent of respondents, N=383, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Need for Efficient Data Scanning in AWS Development Workflows

An organization that uses a data scanning solution that is simple, efficient, and flexible enough for multiple use cases is less likely to hesitate before deploying innovative new business processes that rely on cloud-resident data and applications. The chosen solution should be able to answer several key questions:

- **What data do I have and where is it stored?**

Discovery of data and data stores is essential to successfully protecting the data. You can’t protect what you can’t see, and app developers and security teams lack visibility into their company’s cloud-resident data. Organizations that don’t know what data they’re storing or where they’re storing data will have blind spots, making data much more vulnerable.

- **Is the data sensitive?**

Just discovering data stores is insufficient. Organizations need to classify the data, as knowing the type of data they're storing helps developers ensure that the correct security controls are in place, only authorized users can access sensitive data, and all standards and regulations are being applied.

- **Is the organization in compliance with regulations?**

The plethora of standards and regulations regarding data continues to grow, and existing and new standards control both data storage and data access. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires organizations to restrict access to PII and personal health information (PHI), while the Payment Card Industry Data Security Standard (PCI DSS) requires the organization to protect cardholder data.

- **Is the storage configured properly?**

Misconfigurations, especially access and permission-related misconfigurations, can result in inadvertent data exposure and data loss. Organizations need a quick and simple way to ensure that cloud storage infrastructure configuration doesn't lead to data exfiltration.

- **Is the data safe to use?**

As organizations shift workloads to the cloud, they move workload-associated data in bulk transfers. This ingested data could contain long-dormant or stealthy, persistent malware and ransomware. Likewise, as users interact with cloud apps, they may upload files containing malware and ransomware. Organizations need to ensure that all data is clean, and this needs to occur as soon as data is ingested or uploaded to avoid the data becoming a vector for malicious payloads, including malware, viruses, ransomware, trojan horses, and more.

Organizations may try to answer these questions in house, assigning personnel to each of these tasks or creating scripts and other functions to help. However, the automation, programmability, and flexibility of the cloud enables app developers and admins to create and copy data stores quickly and easily. And, to deliver this automation, programmability, and flexibility, the CSPs provide fine-grained access controls and infrastructure configurations.

The result is hundreds to thousands of different data stores with billions of possible permutations for configurations and access. For many organizations, the scale is beyond what a human can comprehend and beyond what a team can manage without turning to specialized tools.

To quickly and easily answer these questions, organizations need a solution that is integrated with AWS and that automates key processes to scan and protect data in AWS managed storage services in real time.

Optimizing Efficiency

Modern software development and digital transformation is about increasing efficiency, and organizations need to prioritize efficiency in application development and security tools. Key efficiency considerations include:

- Is the solution an easy-to-deploy solution and does it work seamlessly in development workflows by automating security scanning?
- Does it help the security team more efficiently gain visibility, set policies and controls, and reduce security incidents from exposing data or transmitting infections?
- Does it minimize costs from adding multiple separate security solutions?

Introducing Data Classification and Antivirus for Amazon S3

Cloud Storage Security, an AWS Partner with AWS Security Competency, provides two cloud-native solutions available in AWS Marketplace to help organizations easily and cost-effectively incorporate data scanning into their workflows; they may be used together or independently from within the same console:

- **Data Classification for Amazon S3** helps organizations find and classify sensitive data to gain visibility and oversight of data for better security and compliance with industry regulations.
- **Antivirus for Amazon S3** discovers and scans data to minimize the risk of ingesting and transmitting malware.

The benefits of deploying Data Classification and Antivirus for Amazon S3 include:

- Fast and easy acquisition and deployment entirely within the AWS environment via AWS Marketplace.
- Quick, simple, private, and secure scanning. Cloud Storage Security's applications run inside the customer's AWS instance. Data never leaves the AWS account and Cloud Storage Security has no visibility or access to the customer's data.
- The ability to assess the volume and type of data ingested, where the data resides, and if the data is clean (i.e., the data doesn't contain ransomware or other malware).
- Automatic discovery of all S3 buckets. Dashboards provide an at-a-glance overview, summary statistics, and analytics of restricted, sensitive, and public data by AWS region, enabling organizations to organize and manage their repository of data.
- Cross referenced classification to assess data risk, prioritize vulnerability management, and protect storage systems.
- Efficient scanning—the solutions employ multiple scanning models, including event-driven scanning as files are written, API-driven scanning in real time, Amazon S3 proxy, and retro scanning—to keep data clean and rapidly address security issues.
- Flexibility and scalability, with the ability to scan any number of files, in any format, ensuring that even the largest files can be scanned for ransomware, trojans, and viruses.

Together, Data Classification for Amazon S3 and Antivirus for Amazon S3 help organizations answer the key questions about data: What data do I have, where is it, is it sensitive, and is it safe to use?

The Bigger Truth

Unsecured data creates risk for organizations as they adopt cloud-native application development. These organizations can effectively manage their data security risk by understanding the data across their data stores and ensuring they apply the correct policies and configurations to protect sensitive data. To be proactive, they should regularly scan data to prevent infection and transmission of malware.

Cloud Storage Security offers two solutions—data classification and antivirus detection—that provide an easy way to incorporate security scanning into workflows so organizations can protect their data in dynamic cloud environments as their applications are used and data is transmitted. Organizations looking to incorporate data scanning into their AWS environment should take a closer look at these solutions from Cloud Storage Security.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188