SECURE YOUR AMAZON S3 CLOUD STORAGE

DSX for Cloud - Amazon S3

THE CLOUD OPPORTUNITY

The Critical Need to Protect Cloud Storage

Data is the lifeblood of the modern enterprise – a repository rich with insights, strategic value, and sensitive customer information. As cloud transformation has become a strategic imperative for all organizations, the volume of data generated and shared by applications, services, employees, and customers is growing rapidly, with much of it on cloud storage services like Amazon S3. The consolidation of information from various endpoints into data repositories has transformed them into major attack targets, providing a one-stop-shop for attackers. Safeguarding these cloud repositories against increasingly sophisticated cyber threats is paramount. It only takes one infected file to put your enterprise at risk.

More Storage, More Attacks

Amazon S3 is both cost effective and highly scalable, enabling quick and easy data sharing and storage across distributed teams and geographies. But greater accessibility means files can land in storage buckets from virtually anywhere – from anyone, at any time – and the integrity of those files is not ensured by AWS. Bad actors are eager to take advantage of these vulnerabilities.

Attacks are increasing in volume and complexity, aided in part by the ability of Dark AI to generate novel malware that can be deployed quickly to overwhelm defenses. Your cybersecurity solution needs to be able to combat both traditional threats and the growing threats of the future.

> “Storage [is] the backdoor for hackers... requires improved overall security and enhanced cyberprotection.
>
> **JULIA PALMER,**
> **GARTNER ANALYST**
>
> HYPE CYCLE FOR STORAGE AND DATA PROTECTION TECHNOLOGIES, 2023

THE SOLUTION

DSX for Cloud – Amazon S3 applies a zero-day data security approach to S3 protection, stopping bad actors from breaching your cloud perimeter and rooting out existing, unexecuted malware in your storage.

Powered by deep learning (DL), DSX for Cloud – Amazon S3 seamlessly integrates into your AWS environment while delivering unparalleled efficacy, accuracy, and enterprise-grade scalability.

Protecting Your S3 Buckets

Many of the world's largest enterprises rely on Amazon S3 to store their valuable data. They need the right-sized security tools to protect it.

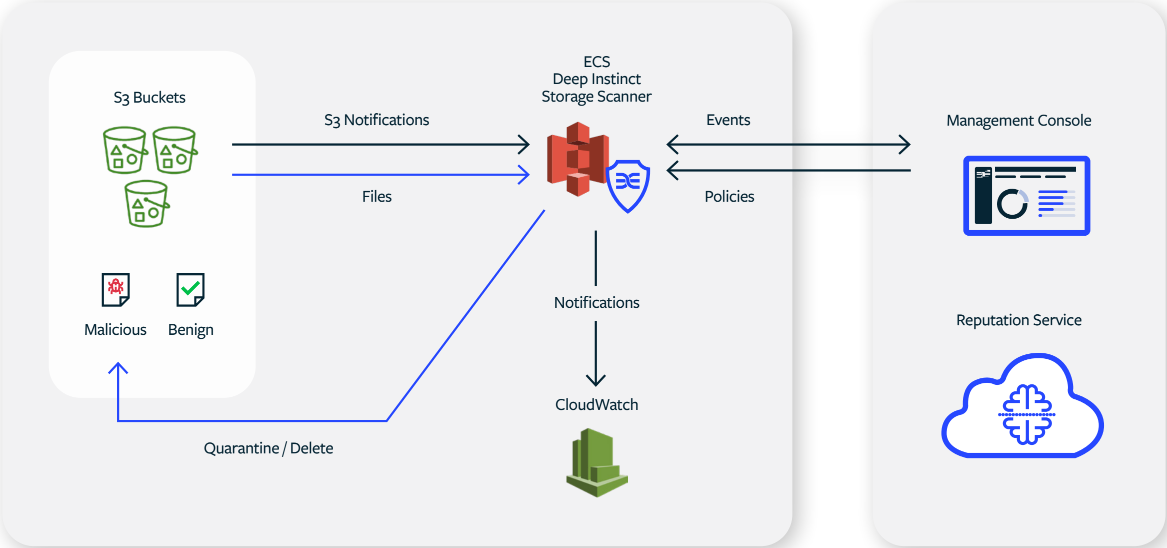
DSX for Cloud – Amazon S3 is a zero-day data security (ZDDS) solution that scans and secures your cloud storage against known and unknown malware, including zero-day threats no one else can find. And it is powerful enough to prevent Dark AI-generated malware.

Using the world's first and only deep learning framework for cybersecurity, DSX for Cloud is the fastest and most effective protection solution purpose-built for cloud storage.

aws + DSX

DSX for Cloud – Amazon S3 is AWS natively integrated and certified. It deploys in minutes and allows you to achieve the following:

- Scan and monitor the Amazon S3 storage buckets of your choice
- Gain full visibility into your entire storage repository, leaving no file unscanned
- Take advantage of flexible remediation options, including file tagging, quarantine, deletion, and restoration of quarantined files
- Securely scan files within your environment, maintaining full control and privacy without letting your data leave your storage
- Scale without interruption, allowing your data and security to grow in tandem, reducing security gaps



DSX for Cloud – Amazon S3 delivers enterprise scalability with lightning-fast scan speeds and a low TCO, providing a comprehensive approach to antivirus scanning. It is natively integrated, giving you the tools to quickly and easily secure your S3 storage.

INTEGRATION SOLUTION

DSX for Cloud – Amazon S3 is a natively integrated solution certified by AWS. After a quick and easy deployment, it proactively prevents malware, ransomware, and unknown and zero-day threats from compromising your storage. Speedy and accurate malware scanning provides visibility into your existing storage, confidence in the safety of incoming files, and the flexibility to prevent new threats.

DSX for Cloud – Amazon S3 allows you to control and manage remediation actions taking place in your storage by supporting easy-to-manage policies. All file scans are logged for easy tracking and reporting. For each malicious file, detailed events can be sent to SIEM and SOAR systems, as well as the DSX console, which allows for enhanced investigation of the prevented attack alongside DIANNA, the DSX Companion.

Improve Security and SOC Operations

- >99% efficacy against known, unknown, and zero-day threats
- <0.1% false positive rate on alerts
- <20ms average file scan speed
- Enterprise scalability and data throughput

Lower TCO

- Minimum infrastructure costs at maximum scale

Ease of Management

- Automated remediation
- Streamlined threat analysis with detailed events
- Integration with SIEM and SOAR

Compliance Ready

- Ensures data privacy
- Logs all file scans

CONCLUSION

Data is your organization’s most valuable asset; protecting it should be your top priority.

As attacks continue to increase in volume and velocity, and emerging technologies like AI expand the threat landscape, a reactive “detect and respond” approach to data security is no longer sufficient. To safeguard your critical data, it is imperative that malicious files are prevented from landing in your storage. Protect your cloud storage with unparalleled efficacy in preventing known and unknown malware, extremely low false positive rates, and a highly scalable implementation.

DSX for Cloud is purpose-built to protect cloud storage and enable zero-day data security.
We prevent what others can’t find.™

DSX for Cloud – Amazon S3 is available now on the AWS Marketplace.