deep instinct

KEEP YOUR STORAGE REPOSITORIES SAFE

Deep Instinct Prevention for Storage

THE CHALLENGE

The Critical Need to Protect Storage Repositories

Data is the lifeblood of the modern enterprise—a repository rich with insights and strategies along with sensitive and protected customer information. As organizations continue to digitally transform, applications, services, employees, and customers are generating and sharing more data than ever before.

The consolidation of information from various endpoints into data repositories has transformed them into major attack vectors, providing a one-stop-shop for attackers. Safeguarding these repositories—whether they are in Network Attached Storage (NAS), hybrid, or public cloud environments—against increasingly sophisticated cyber threats is paramount. It only takes one infected file to put your enterprise data at risk.

Legacy Tools Falling Short

Many organizations believe that their data is protected by traditional solutions such as legacy AV, immutable backups, and content disarm and reconstruction (CDR). Unfortunately, these solutions are insufficient to stop ransomware, zero-day threats, and other known and unknown malware from infiltrating your storage environments—whether data is stored on-prem or in the cloud. To effectively combat this new breed of cyber threats, a next-generation cybersecurity solution that harnesses the power of AI is required.

> “
>
> 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

Fight AI with Advanced AI: Predictive Prevention for Data Security

Deep Instinct Prevention for Storage applies a prevention-first approach to storage protection, stopping ransomware and malware from reaching your data and executing in your environment. Powered by deep learning (DL), Deep Instinct Prevention for Storage seamlessly integrates into your storage environment while delivering unparalleled efficacy and accuracy along with enterprise-grade scalability.

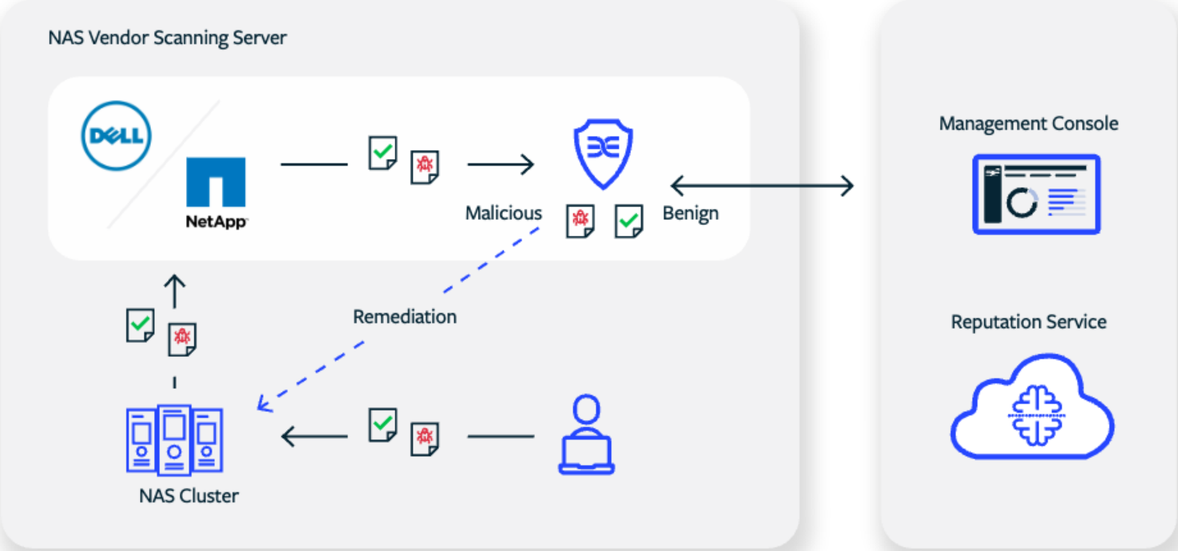
DPS for Network Attached Storage (NAS)

DPS for NAS is a natively-integrated solution that proactively shields your data from cyberattacks including ransomware, zero-day threats, and other known and unknown risks. Leveraging the unique power of our deep learning framework, it prevents malicious files and malware from landing in your storage quickly and effectively.

NAS repositories store business-critical information while NAS devices are used as file-sharing platforms where multiple users access and retrieve files.

If malware-infected files are stored in the NAS they can be downloaded or opened leading to infections, compromised devices, and business disruption.

- Traditional approaches have long scan times, causing delays and increasing TCO.
- They have low detection rates for zero days and unknown variants, leading to complexity and false positives.
- Deep Instinct scans files in <20 milliseconds, revolutionizing data protection and malware prevention.
- DPS for NAS triggers a scan whenever a file is accessed, preventing users from accessing infected files.
- Malicious files are quarantined or deleted by the system.
- DPS for NAS seamlessly integrates with leading NAS vendors like Dell CAVA and NetApp Vscan for smooth deployment and interoperability.



Deep Instinct ensures proactive, real-time scanning, detection, and prevention of malware, safeguarding the integrity and security of stored data.

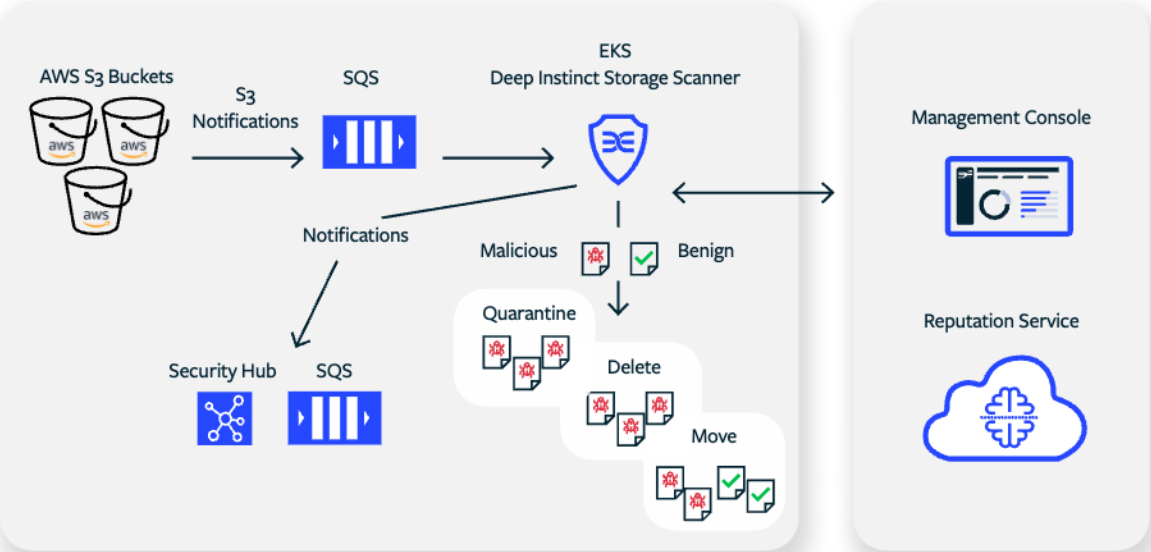
DPS for Cloud Storage

DPS for Cloud Storage is a natively-integrated solution that leverages our deep learning framework to perform highly efficient malware scanning on files whenever they are added or changed within your cloud storage. This stops malware from ever entering your hybrid or public cloud storage environment, protecting the integrity of your data.

Cloud repositories are both cost effective and highly scalable, enabling easy and quick sharing of data. But files can land in storage buckets from virtually anywhere by anyone at any time, which makes them an easy target for bad actors. While cloud vendors protect the cloud storage itself, they do not ensure the integrity of files stored.

Cloud vendors do not scan files before storing them, leading to a high risk that malware infected files are being stored in the cloud and spreading malware to production systems.

- DPS for Cloud Storage deploys in minutes using a CloudFormation template and utilizes native AWS services.
- It seamlessly integrates with Amazon Security Hub, enabling rapid threat notifications.
- The solution supports monitoring of existing buckets and discovery and monitoring of new buckets.
- Flexible remediation options include file tagging, quarantine, deletion, and restore of quarantined files, all controlled through policies.
- Files are scanned within your environment and never leave it, ensuring full data privacy and confidentiality.



INTEGRATION SOLUTIONS

Proactively prevent malware and other threats—including unknown and zero-days—from reaching your data wherever it is stored.

Deep Instinct Prevention for Storage is managed via a single console alongside Deep Instinct Prevention for Endpoints (DPE) and Deep Instinct Prevention for Applications (DPA).

Deep Instinct allows you to control and manage remediation actions taking place in your storage by supporting easy-to-manage policies. These include quarantine or deletion of malicious files, as well as restoring from quarantine, if needed.

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 Deep Instinct's management console which allows for further investigation of the prevented attack.

Easily Integrate with Your Storage Infrastructure

- Dell and NetApp native integration
- AWS S3 cloud storage integration

Improve SOC Operations and Lower TCO

- > 99% efficacy preventing unknown threats
- < 0.1% false positives rate
- < 20ms file scan time
- Minimum infrastructure costs at maximum scale

Ease of Management

- Single console experience spans all Deep Instinct products
- Automated remediation
- Streamlined threat analysis with detailed events
- Integration with SIEM, SOAR and AWS Security Hub

Compliance Ready

- Ensures data privacy
- Logs all file scans

CONCLUSION

Data is an 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 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. In an ever-evolving, AI-driven digital landscape, Deep Instinct can protect you. With unparalleled efficacy in preventing malicious files, extremely low false positive rates, reduction in TCO, and a highly scalable implementation, Deep Instinct Prevention for Storage ensures that your data remains secure, and you can achieve peace of mind.