DEEP INSTINCT DATA SECURITY X

# Zero-Day Data Security

PREVENTS

**<0.1%**
FALSE POSITIVE RATE

**>99%**
UNKNOWN ZERO-DAY, AND RANSOMWARE ATTACKS

**<20MS**
REAL-TIME MALICIOUS VERDICTS DETECTED

Data is your organization's most valuable asset. As "Dark AI" drives the exponential growth of sophisticated zero-day attacks, traditional cybersecurity tools fall short, leaving your data vulnerable. Deep Instinct Data Security X (DSX), a purpose-built Zero-Day Data Security (ZDDS) solution, addresses this critical gap by preventing threats no other vendor can find and explaining zero-day attacks in real-time.

## Why Zero-Day Data Security Matters

Deep Instinct DSX leverages the first and only deep learning framework built from the ground up to solve today's most advanced cybersecurity challenges. DSX meets attackers at the point of impact, protecting your environment against malicious files uploaded through web applications, stored in private and public clouds, downloaded from the internet, stored in NAS and cloud storage environments, and transferred into your environment by third-party suppliers.

- **Reduce Liability** – Meet regulatory and internal policy compliance requirements
- **Reduce Threats** – Prevent costly zero-day attacks that can severely damage your business and reputation
- **Lower TCO** – Minimize infrastructure usage and manpower costs associated with attack response

### THE DEEP INSTINCT DSX ADVANTAGE

- **Real-Time Prevention:** Stop zero-day threats with >99% efficacy, with a <0.1 false positive rate
- **Real-Time Analysis:** Provide detailed explainability of zero-day attacks using GenAI (DSX Companion)
- **Secure Data Everywhere:** Comprehensive security across cloud, NAS, applications, and endpoints, at rest or in motion
- **Scalable Solution:** Scan large repositories at enterprise speed and scale
- **Privacy Focused:** Ensure data privacy and compliance – your files and data never leave your environment
- **Self-Sufficient & Cloud-Independent:** Makes malicious vs. benign determinations independently, without cloud threat intel, and requires only 1-2 updates per year

# Deep Instinct Data Security X

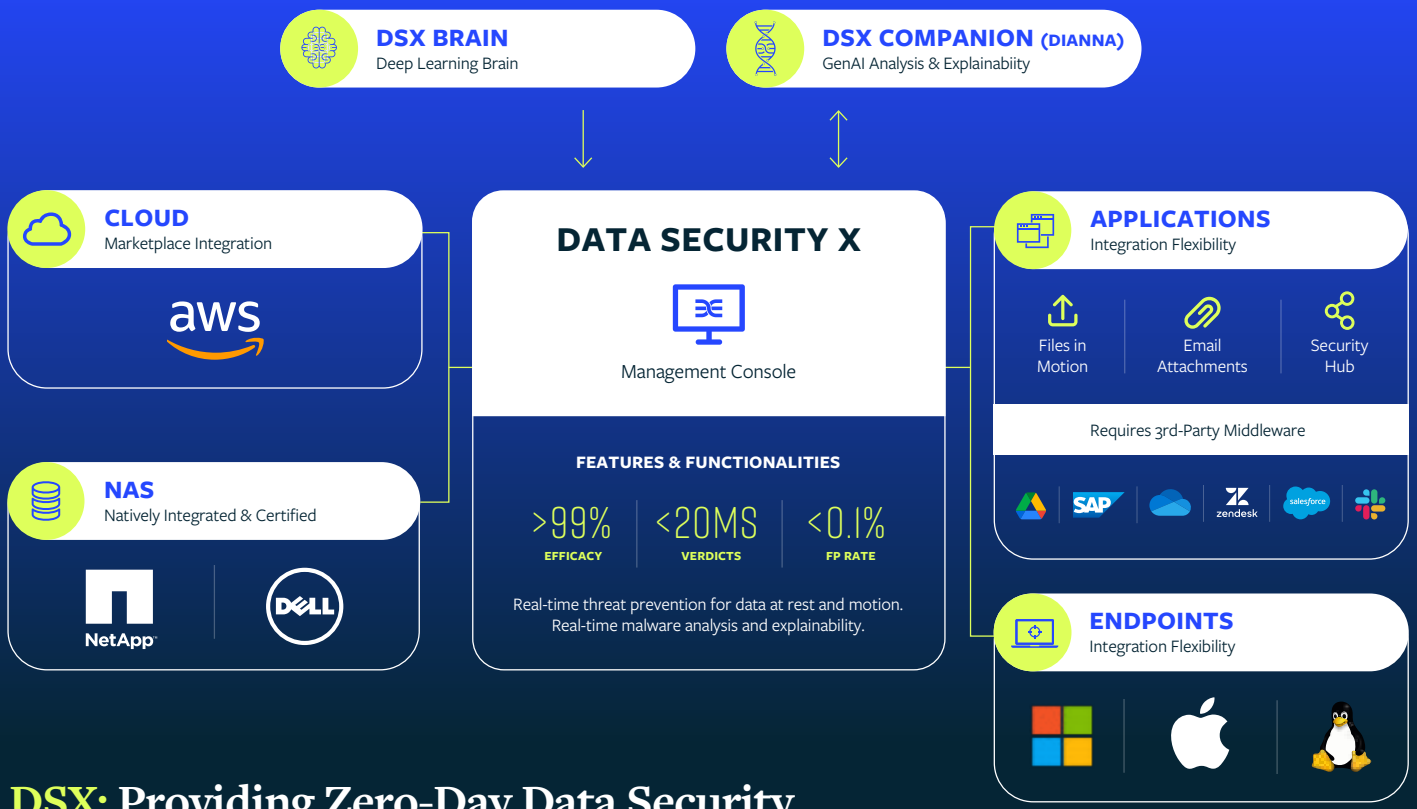
Deep Instinct DSX leverages a purpose-built deep learning cybersecurity framework (DSX Brain) and GenAI (DSX Companion) to prevent and explain zero-day attacks in real-time.

### ZERO-DAY THREAT PREVENTION (DSX BRAIN)

Deep Instinct DSX delivers real-time malicious verdicts in <20 ms, providing the market's fastest and most effective zero-day threat prevention solution — across cloud and NAS repositories, applications, and endpoints. It leverages DSX Brain, the only deep learning framework in the world built from the ground up for cybersecurity to stop threats before they can execute, eliminating the impact of zero-day attacks.

### ZERO-DAY EXPLAINABILITY & ANALYSIS (DSX COMPANION)

Powered by GenAI, DIANNA, the DSX Companion provides comprehensive zero-day malware analysis with unparalleled explainability. DIANNA, the DSX Companion, works alongside the DSX Brain to provide detailed insights into the anatomy of attacks, including their patterns and behaviors, providing comprehensive analysis no other solution can replicate. This enables security and infrastructure teams to understand and respond to threats quickly. This unique combination of deep learning AI capabilities and GenAI-powered explainability enhances overall SOC efficiency and improves your organization's threat posture.




## DSX: Providing Zero-Day Data Security

*Deep Instinct DSX gives your organization a significant edge over attackers. It prevents threats before they execute across cloud and NAS storage, custom applications, SaaS applications, and endpoints.*

## DSX for NAS

DSX for NAS is a prevention-first solution for scanning and securing your network-attached storage (NAS). It prevents ransomware and malware from reaching your storage and executing, preventing >99% of threats, including zero-day and unknown threats. Powered by deep learning, DSX for NAS scans your entire storage environment at lightning-fast speeds (<20ms per file) to ensure the safety of your data.

### EASILY INTEGRATES WITH YOUR NAS STORAGE INFRASTRUCTURE

DSX for NAS prevents threats from entering storage repositories and integrates with leading NAS solutions, including Dell CAVA and NetApp Vscan, for rapid deployment and interoperability.

### PROACTIVELY PROTECT STORAGE

DSX for NAS scans files in storage, whether at rest or in motion, and automatically acts on malicious content, quarantining or deleting infected files before users open them. This proactive approach blocks threats before they spread through storage repositories and to users.

### NO BOTTLENECKING

With an average file scan speed of <20 milliseconds, your teams can spend their time working, not waiting. And when applied to your entire data estate, you can scan your repositories in hours, not days or weeks.

### LOWER TCO

In addition to speed and productivity gains, minimal infrastructure needs help you save even more, delivering a much lower TCO than industry competitors.

## DSX for Cloud

DSX for Cloud applies a prevention-first approach to cloud storage protection, stopping ransomware and malware from reaching your data and executing in your cloud storage environments. DSX for Cloud seamlessly integrates with your cloud storage environment, delivering unparalleled efficacy, accuracy, and enterprise-grade scalability.

### SECURE CLOUD STORAGE IN MINUTES

DSX for Cloud delivers enterprise scalability at a low cost with lightning-fast scanning, preventing malicious files from reaching your storage buckets, ensuring file integrity, and securing access to vital assets. DSX for cloud deploys in minutes using native cloud services.

### PROACTIVELY PROTECTS CLOUD STORAGE

DSX for Cloud scans files in storage, whether at rest or in motion, and automatically acts on malicious content, quarantining or deleting infected files before users open them. This proactive approach blocks threats before they spread through storage repositories and to users.

### OPERABILITY AT ENTERPRISE SPEEDS & SCALE

With an average file scan speed of <20 milliseconds, you can quickly scan vast volumes of data contained in your repositories in hours, not days or weeks, ensuring 100% visibility into your cloud storage.

### LOWER TCO

In addition to speed and productivity gains, cloud infrastructure helps you save even more, delivering a much lower TCO than industry competitors.

## DSX for Applications

DSX for Applications is an agentless, on-demand, anti-malware solution that scans files in transit for malicious content. It works at enterprise scale, detecting and preventing zero-day, unknown, and known malware.

### PREVENT MALICIOUS FILES

With an efficacy rate of >99%, DSX for Applications enables you to meet attackers earlier and prevent threats hidden in your files, including ransomware, unknown, and zero-day attacks. Block file uploads through your web applications, scan user downloads from the internet, and restrict third-party suppliers from transferring files into your environment to keep malicious content from traversing your network.

### TAILORED TO YOUR WORKFLOWS

DSX for Applications integrates into your environment with a lightweight, agentless solution that aligns with existing workflows. It offers a flexible and programmable REST API or ICAP that is OS- and device-agnostic.

### SCALABLE TO PETABYTES

Quickly scans tens of millions of files daily and protects any web application or cloud storage environment from malicious content without impacting the user experience.

## DSX for Endpoints

DSX for Endpoints complements your existing EDR and SIEM tools with a multi-layered, prevention-first approach. When an attacker attempts to land a malicious payload on your endpoint, DSX for Endpoints prevents it before it can execute and infect your network.

### PRE-EXECUTION: PREDICT & PREVENT WITH STATIC ANALYSIS

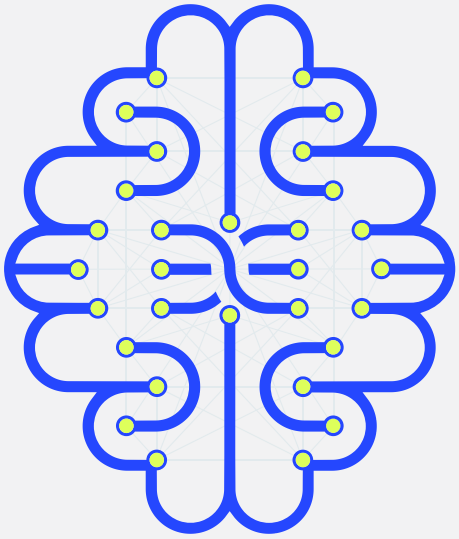
DSX for Endpoints prevents >99% of known and unknown malware, including zero-day exploits, ransomware, and file-based and script-based attacks, using DSX Brain's learning-based static analysis engine.

### ON-EXECUTION: DYNAMIC & BEHAVIORAL ANALYSIS

Employ a multi-layered prevention approach, adding dynamic and behavior analysis to protect and automate responses to the most advanced threats, including fileless attacks like malicious code injection and credential theft, advanced scripts such as unknown shellcode and multi-stage attacks, and active adversarial AI attacks.

### POST-EXECUTION: AUTOMATED ANALYSIS

DSX for Endpoints provides context and analysis to help your security teams understand the severity and tactics of a threat, including suspicious events for threat hunting and MITRE ATT&CK mapping.



## Why is Deep Learning important?

Deep Learning is the most sophisticated form of AI, inspired by the brain's ability to think and learn over time. This ability enables the DSX Brain to prevent attacks before threat actors access your environment.

Deep Instinct's deep learning-based solution provides the following critical advantages:

- Trains on 100% of available raw data, enabling it to make non-linear correlations with greater context, driving faster, more accurate decisions
- Requires just 1-2 updates per year, while preventing all unknown threats
- Understands the DNA of an attack without requiring complete knowledge of the threat or intent, reducing the need for human-fed feature engineering and saving time and effort
- Operates seamlessly without cloud calls or threat intelligence feeds to make decisions, accelerating prevention times
- Greater accuracy than other forms of AI or ML, featuring a <0.1% false positive rate

Deep learning-based cybersecurity helps organizations make prevention a reality by predicting and preventing threats before they can execute. It keeps attackers out of your environment – across endpoints, applications, and NAS and cloud storage. Paired with the DSX Companion, which provides real-time insights and explainability of zero-day attacks utilizing GenAI, deep learning-based cybersecurity will transform your cybersecurity capabilities and the efficiency of the SOC teams you rely on to protect you.