Solution Brief

NetApp DefendX Insider Threat Solution

Key Benefits

Identify Threats and Anomalous Behavior

By creating a baseline for your environment, you can identify unusual or nefarious activity.

Provide Visibility— Answer the Question "Why?"

You cannot protect what you cannot see. Identify who has access to resources and at what level, and confirm that you understand why they have access.

Combat the Rising Cost of Data Loss and Data Breaches

Identify the files in your environment to understand the value of your environment, to assess risk, and to more efficiently derive security budgets and costs.

Address Privacy Through Compliance

Getting specific details and keen insight on user access activities and resources also helps you meet current compliance challenges, such as GDPR, PCI standards, HIPAA, and others.

The Challenge

Insider threats continue to increase—in fact, they already have access to your critical files

Every year, countless businesses and government organizations are attacked and robbed of valuable assets. With the ongoing digital transformation, more and more of these assets are taking the form of digital files that are stored in vast file repositories. The loss of the intellectual property (IP) that these files represent can result in staggering consequences if the IP is not properly protected. Although many attacks originate from outside the organization, some of the most notable and damaging attacks are committed by insiders—the very people who are trusted to access and manage these critical files.

As a leading provider of enterprise-class file storage solutions, NetApp has partnered with DefendX Software to provide proven protection from these insider threats.

The Solution

Protecting your most valuable resource: data

Protecting your file data is paramount for your organization. Together with enterprise-class NetApp® storage systems that help meet your various deployment needs, the NetApp DefendX Insider Threat Solution provides the secure, enterprise-class file storage architecture that you need for today's digital environments. An outline of this architecture is depicted in Figure 1. DefendX extends NetApp technology capabilities with integrated software that helps you understand who has access to critical file assets and what permissions or levels of access they have. DefendX also provides a complete solution for event logging, activity monitoring, threat intervention, and forensic auditing.

The NetApp DefendX Insider Threat Solution uses the following four capabilities to meet the challenges of insider threats.

- Permission mapping
- Real-time event tracking
- Alerting and intervention
- Forensic auditing

Permission mapping

Take care of the obvious problems first! Securing your digital file environment starts with assessing the status of your file permissions. The file security reporting component of the NetApp DefendX Insider Threat Solution helps you answer a question that is fundamental to protecting your key assets: Who has access to file assets but shouldn't? Finding and closing these security holes are the first steps to better file security.

NetApp®

Real-time event tracking

The NetApp DefendX Insider Threat Solution is tightly integrated with the NetApp FPolicy™ component to log relevant events that are associated with files, directories, shares, and groups of files. This real-time logging capability enables DefendX to monitor for suspicious behavior and to perform forensic audits of protected file assets.

Alerting and intervention

A central function of the DefendX security package is alerting and intervention. The NetApp DefendX Insider Threat Solution supports two types of alerting:

- **Event-based.** Alerts can be issued and acted upon with real-time logging of specific events. Examples include blocking an attempted directory delete, notifying specified authorities through email, and locking out the offending user.
- **Trend-based.** Trend-based alerts enable the creation of Business Overwatch Tasks (BOTs) to monitor logged events for suspicious trends or threshold situations over time. For example, the accrual of a certain number of file deletes over a set period might represent a deviation from normal behavior.

Forensic auditing

With a comprehensive log of all relevant file operations that is available for analysis, the NetApp DefendX Insider Threat Solution features a powerful reporting engine to perform deep forensic audits. An audit can focus on the protected file asset, or it can focus on a particular user or group, which provides context to address current security challenges.

This solution is primarily designed to help you handle insider threats. However, functions such as audits help you adhere to internal file management policies and to comply with regulatory programs. You can comply with programs such as ISA, Defense Federal Acquisition Regulation Supplement (DFARS), Federal Acquisition Regulation (FAR), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR). Audits are also crucial for the investigation of policy violations and threat events.

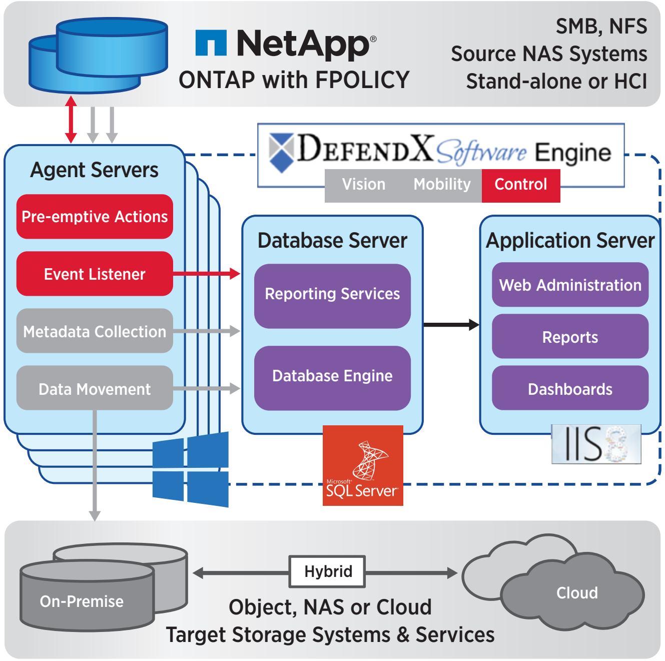

Figure 1) NetApp DefendX Insider Threat Solution architecture.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven