DATA-CENTRIC SECURITY WITH ISILON & VARONIS

Security that covers your biggest assets

ESSENTIALS

- Dell EMC Isilon provides a robust suite of features to ensure data protection and regulatory compliance.
- Varonis provides a data security platform that works in conjunction with Isilon OneFS to protect against insider threats and cyberattacks
- File System Auditing strengthens compliance by providing a Chain of Custody to prove Data Authenticity
- Varonis can detect suspicious behavior and alert data administrators of potential threats
- Isilon SnapshotIQ™ can be used to protect against business outages caused by Ransomware or internal threats

REGULATORY COMPLIANCE, INSIDER THREAT AND RANSOMWARE PROTECTION

CIOs and CSOs are facing unprecedented challenges with ensuring their data is both authentic, confidential and protected from malicious activities that may make their data inaccessible and put their business at risk. Their situation is exacerbated by the rapid growth of unstructured data—from a never-ending number of sources—landing in their data centers. Ever-advancing hacking techniques, ransomware, and insider threats present additional challenges.

Through sophisticated analysis of permissions, content and file system audit activity, many potential sources of data loss -- including fraudulent activities, inappropriate entitlements, unauthorized access attempts are detected and mitigated.

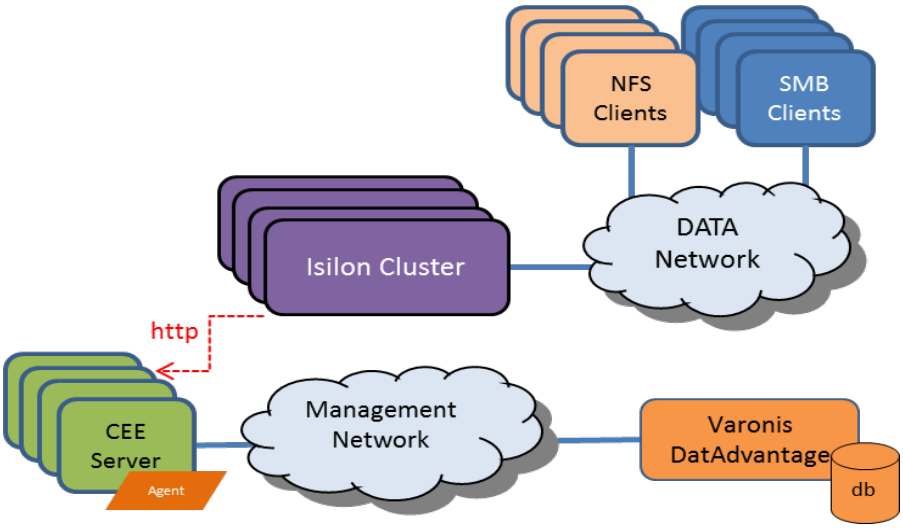
Auditing, classification and least privilege enforcement are key components of meeting regulatory requirements. Features like Isilon SmartLock can provide Write Once Read Many (WORM) to lock down data and make it immutable, but auditing of the file system is still a necessity to provide a Chain of Custody to prove the data is authentic. A good compliance strategy must contain additional security features in addition to auditing and WORM. Here are some examples of markets that require compliance.

Example Regulatory Requirements

SEGMENT	KEY BUSINESS DRIVERS
Financial Services	Compliance requirements for the Sarbanes-Oxley Act (SOX)
Healthcare	Compliance requirements for the Health Insurance Portability and Accoutabilty Act (HIPAA) 21 CFR (Part 11)
Life Sciences	Compliance requirements for the Genetic Information Non-discrimination Act (GINA)
Media & Entertainment	Security requirements for Motion Picture Associaton of America (MPAA) content movement
Federal Agencies	Securith requirements for Security Technical Information Guide (STIG) & Federal Informaton Security Management Act (FISMA)

ISILON AND VARONIS SOLUTIONS FOR AUDITING

Isilon has a feature for CIFS/SMB and NFS that enable file system auditing. This feature allows all changes to the file system to be tracked and logged and made accessible to Varonis DatAdvantage via the Dell EMC Common Event Enabler (CEE). Below is the logical data flow for CEE processing to Varonis.



Isilon and Varonis provide a powerful and complete solution to understand by whom and how the data is being accessed, capturing statistics on file system activity and providing a mechanism to prove data authenticity.

ISILON AND VARONIS SOLUTIONS FOR RANSOMWARE DETECTION AND PREVENTION

Varonis analyzes access events from Dell EMC CEE to detect and alert on suspicious activity like ransomware and other insider threats that are traditionally difficult to spot and put your organization at even greater risk.

DatAlert performs user behavior analytics to automatically profile the entities that use data – employees, executives, administrators, and service accounts – and baselines how every user uses data and alerts on suspicious activity. Varonis user behavior analytics-based threat models utilize thresholds, statistical analysis and machine learning to trigger alerts on what looks unusual and uncover potential security issues. DatAdvantage provides an interactive interface for charting accessibility, and usage by date, by user, by department, and more. Data Classification Framework classifies files to identity regulated and sensitive content. If malware such as CryptoLocker does hit your servers, DatAdvantage can help pinpoint exactly which files and folders were impacted, making recovery much easier. Admins can drill down to see a highly granular audit trail of every single file or email touch (who did, what they did, and when) — extremely helpful for finding misplaced files or doing forensics.

Isilon also has a number of features that help protect against ransomware in conjunction with Varonis. In addition to the auditing feature, Isilon has File Blocking capability which prevents unwanted or illegal content from being placed on the cluster in the first place. Isilon SnapShotIQ is a great way to protect against ransomware by maintaining a clean copy at a remote site.

The process is straightforward:

- Create Snapshot Copy of the data at the Primary Site
- Replicate Second Copy to Secondary Site
- Create Snapshots at Secondary Site
- Keep Snapshots for a specific period time to meet your RPO

SNAPSHOT PROTECTION WITH AN OFFSITE COPY

To be prepared for a ransomware or other attack you should ensure that AV scanning is enabled and that regular backups are created and a well-designed snapshot policy, for example hourly, and snapshot retention policy is established to prove multiple recovery points should an attack occur.

If an attack does occur the obvious first step is to stop the attack. Varonis DatAlert can execute commands to automatically stop the attack in progress. Next leverage the auditing features of Varonis and Isilon to isolate where the attacks are coming from and exactly which files were affected and when.

Then recover to a pre-attack state from the Snapshots. It may require walking through multiple Snapshots to find the ones that address the scope of the attack and then use Isilon SnapRevert to convert the active data set back to a known good point in time.

SUMMARY

Dell EMC Isilon and Varonis are a great combination to keep your data lake regulatory compliant and protected from insider threats and ransomware. As market leaders and longtime partners enterprise class solutions are a given and CIOs, CSOs and IT Managers can all rest assured that they have the most robust solution available to help them protect their business.

CONTACT US

To learn more, contact your local representative or authorized reseller.