NASUNI | VARONIS

Solution brief

Nasuni + Varonis: integrated file storage and data protection

Ransomware vulnerability of unstructured data

Only 20% of data resides in highly protected, secure databases for most enterprises. The other 80% is unstructured data in file systems scattered across multiple NAS devices and file servers. This creates two severe challenges for modern organizations.

First, traditional NAS, remote office file servers, and backup can no longer keep pace with the rapid growth of unstructured data, which, for many organizations, is doubling every year. File storage capacity and performance issues, ineffective multi-site file sharing, inadequate recovery points and recovery times, high costs, and complex administration are now commonplace.

Second, 80% of unstructured data is vulnerable to threats because of its distributed nature and the number of users accessing it daily. Ransomware and other types of cyberattacks can be launched – intentionally or not – by internal users who have complete access. The result can be devastating, including data breaches, sensitive data exposure, privacy violations, destruction of intellectual property, and more.

Two best-in-class solutions
For integrated file storage and security that delivers robust protection against the latest cybersecurity threats

Consolidated files
On a scalable platform with limitless capacity, access from any location, and continuous file versioning

File activity monitoring
In real-time to detect insider threats, ransomware, security violations, and cyberattacks

Audit file data
To assist in meeting security and compliance requirements

Private or public cloud
Storage reduces on-premises storage by up to 70%

Automatically map permissions
Structures and remediate excessive access to data at scale

> We need to prevent malware, ransomware, and other threats from compromising our file data. The joint Nasuni-Varonis solution gives us **best-in-class capabilities** for file storage and file security.
>
> **Dennis DiPalma**, MIS Project Leader, PJ Dick

Nasuni® and Varonis® team up

The joint Nasuni and Varonis solution offers a highly scalable, tightly integrated solution that overcomes both challenges. Nasuni provides the modern file data services platform that stores files in limitless private or public cloud object storage, with edge caching appliances in any location for high-performance file access. Varonis provides a data security platform that protects files from ransomware, cyberattacks and insider threats by analyzing the behavior of the user and machines accessing the data, alerting on misbehavior, and enforcing a least privilege and a zero-trust model. Together, Nasuni and Varonis provide a solid strategy to detect, protect, and recover against ransomware for unstructured file data.

Case study

PJ Dick – Trumbull – Lindy is a top 100 general contracting and construction management firm, providing services for large-scale projects such as the CONSOL Energy Center in Pittsburgh, the first LEED Gold certified NHL arena in the US, and The Tower at PNC Plaza, the world's greenest skyscraper. Faced with the need to store and collaborate on fast-growing CAD, LIDAR, and other unstructured data across offices and remote worksites and proactively detect threats to mitigate the impact of cyberattacks, PJ Dick's IT team turned to Nasuni and Varonis. With Nasuni, the firm consolidates all its file data from multiple sites into limitless Microsoft Azure object storage, caching actively used files on-premises for high-performance access and improving RPOs and RTOs. With Varonis, PJ Dick monitors file access patterns on Nasuni Edge Appliances to detect suspicious activity and alert on misbehavior.

Explains Dennis DiPalma, MIS Project Leader at PJ Dick, "Our goal in IT is to deliver efficiency and performance in support of our large-scale contracting projects. With CAD and other types of unstructured data growing and playing a critical role in every project, a scalable file infrastructure that enables us to store, collaborate, and recover files quickly is essential. At the same time, we need to prevent malware, ransomware, and other threats from compromising our file data. The joint Nasuni-Varonis solution gives us best-in-class capabilities for file storage and file security and enhances our ability to maintain tight schedules while keeping IT costs down."

Key capabilities

- **Automatically and accurately classify sensitive and regulated data** with Varonis' sophisticated classification rules that go beyond regular expressions.
- **Varonis continuously maps out permission structures** and pairs them with classification results, revealing where data is overexposed and at risk. Unique automated remediation capabilities help organizations dramatically reduce their attack surface by eliminating excessive permissions at scale – all without affecting production data.
- **Varonis monitors data access activity**, authentication activity, and perimeter telemetry, employing behavior-based threat models to detect suspicious activity like privilege escalation or unusual access to data.
- **Speed up investigations** with a complete audit trail of events that help organizations better understand how data is accessed and used. Utilize dozens of built-in reports to report on incidents and demonstrate compliance to regulatory officers quickly.

Integrated file storage and data protection

The Nasuni UniFS® global file system stores the gold copies of all files and metadata in private or public cloud object storage platforms like Nasuni virtual Edge Appliances intelligently cache just the active files anywherefile access is needed.

Each Nasuni Edge Appliance looks like a traditional NAS device or file server, using existing Active Directory or LDAP authentication infrastructure and standard file sharing protocols (e.g., CIFS, NFS) to provide file access. Nasuni appliances require a much smaller storage footprint – typically 80% less capacity – since they are optimized to cache only the active files.

Varonis Collectors can be installed in the cloud or wherever Nasuni Edge Appliances are located to provide centralized security monitoring, auditing, analytics, and remediation.

When a user or program accesses file data cached on a Nasuni Edge Appliance, Nasuni automatically sends audit tracking data to a Varonis Collector. The Varonis Data Security Platform analyzes the behavior of users and machines accessing data and provides real-time alerting and notification of any suspicious activity.

IT administrators can use Varonis to identify compromised accounts, privilege escalations, GPO changes, and malware attacks like ransomware – and deploy automated responses to stop them before they lead to a data breach.

Varonis can also identify and lock down sensitive data at scale, set permissions, capture detailed audit trails for compliance and forensics, and produce reports.

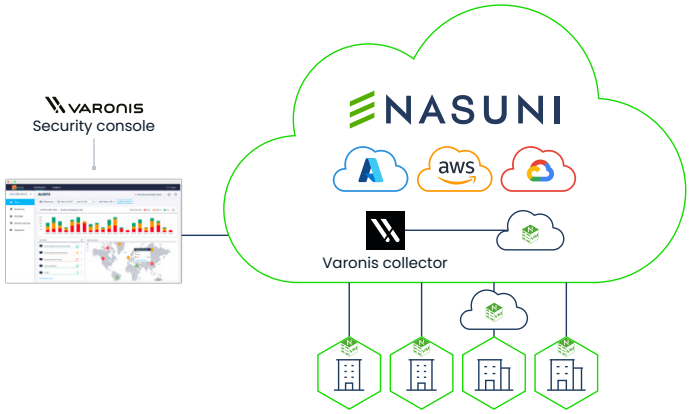
> "Nasuni and Varonis provide joint customers with a comprehensive solution for storing, sharing, protecting, and defending their data on-premises and in the cloud – while also addressing GDPR and other requirements by discovering and classifying personal identifying information."
>
> **David Bass**, EVP of Engineering and CTO, Varonis

Benefits of Nasuni + Varonis

- Highly secure and scalable platform for storing and protecting unstructured data on-premises, in the cloud, or in hybrid cloud implementations
- Unlimited file storage capacity for user home drives, department shares, and project directories, with no limits on volume, directory, file size, or the number of locations accessing the same data
- Security analytics with deep data context, combining advanced data classification and access governance with continuous monitoring, alerting, and locking down core data stores at scale
- Custom dashboards to help identify and prioritize risk, enabling you to get started with remediation efforts and resolve misconfigurations quickly
- Keep critical business data safe with immutable and infinite snapshots in low-cost cloud object storage
- Recover millions of files in minutes with Rapid Ransomware Recovery
- Restore entire volumes, or individual files for specific users with recovery points as recent as one minute prior to an attack
- Detect and alert suspicious activity and prevent further damage with automated responses

LEARN MORE

To learn more about Nasuni and Varonis click here.



About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases, including data protection, data governance, zero trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

NASUNI

sales@nasuni.com
+1.857.444.8500

nasuni.com

Nasuni is a scalable data platform for modern enterprises in an AI world.

The Nasuni File Data Platform delivers effortless scale in hybrid cloud environments, enables control at the network edge, and meets today's expectations for highly protected and insight-ready data.