VARONIS NetApp

Fighting Ransomware

with Varonis and NetApp

Storage analytics with deep data context to give you the upper hand

Think of Varonis as User Behavioral Analytics for NetApp ONTAP — customers are using it to fight ransomware and other insider threats. By watching and analyzing access events with NetApp ONTAP FPolicy Zero Trust Engine — Varonis sees ransomware, stops it, and makes recovery simple.

Varonis can alert you to early signs of compromise by ransomware gangs and APTs with behavior-based threat models for each phase of the kill chain. Beyond detection, Varonis can dramatically reduce your attack surface by automatically identifying and removing excessive access to data.

How Varonis Helps

1 Prevention

Reduce your attack surface

- Discover, classify, and label sensitive information so you can prioritize remediation efforts
- Automatically remediate over-exposed sensitive data, including files exposed via shared links
- Simulate a ransomware attack to see which files on your network would be impacted by an infected user or device

2 Behavior-based detection

Fewer alerts, **more answers**

- Enable out-of-the-box threat models that continually learn and adapt to behaviors specific to your organization
- Combine data sensitivity, data access behavior, network telemetry and threat intelligence feeds to uncover advanced threats across the entire kill chain
- Spot tactics that evade AV and EDR solutions by focusing on core data stores and infrastructure
- NetApp can help identify ransomware by comparing the change-of data signature with other antivirus software to show a pattern

3 Automated Response

Don't just detect, **block**

- Stop attacks in their tracks and limit damage by killing user sessions, changing passwords, locking accounts, and powering down systems
- Write your own custom PowerShell response scripts or choose from a shared library of battle-tested actions
- Each alert can have its own custom response so you can right-size the action to the alert severity and type
- Use the NetApp FPolicy solution to filter or block traffic based on file extensions and file metadata.

4 Recovery

Don't go it **alone**

- Search a complete forensic record of all file access (open, move, modify, delete, rename), email activity, network events (proxy, VPN, DNS), and permissions changes makes it easy to identify affected data and remediate quickly
- Call on our world-class incident response and forensics teams for help with any incident, even if it's outside the scope of Varonis monitored systems
- Use NetApp Snapshot to restore from images that are known to be uninfected

Expand your detection window

Varonis helps catch more threats by combining perimeter telemetry with data access, email, and Active Directory behavior. These ingredients fuel machine-learning threat models that are automatically trained and optimized for your unique environment.

Data

- Insider threats
- Ransomware
- APTs & malware

Email

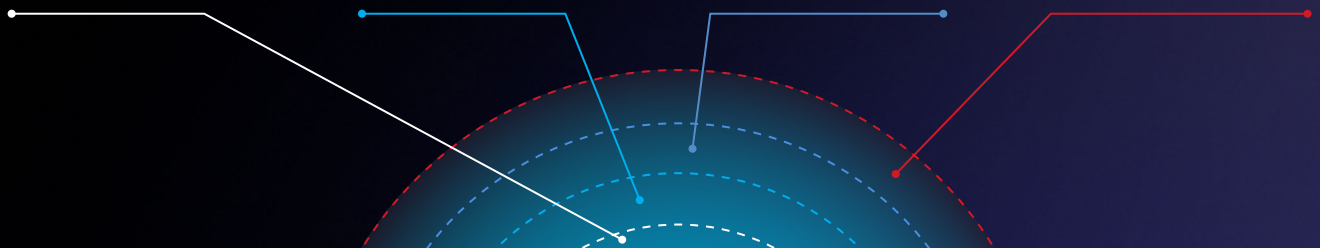
- Phishing
- Infected attachments
- Data exfiltration

Active Directory

- Recon
- Lateral movement
- Privilege escalation

Edge

- Brute-force
- Command & control
- Data exfiltration



Varonis exposes global cyber campaigns

With DatAlert and Edge, our security researchers discovered major classes of malware APTs that other security solutions missed.

Next-gen banking malware (Qbot)

- New strain of Qbot malware designed to steal banking information
- Varonis detected malicious VBS file, C2 comms over DNS, and brute force attempts against domain users

READ THE RESEARCH ›

A stealthy cryptominer (Norman)

- XMRig-based cryptominer — a high-performance miner for Monero cryptocurrency
- Varonis alerted on abnormal web activity alongside correlated abnormal file activities

READ THE RESEARCH ›

Complimentary Incident Response Service

If you're under attack, or just looking for some help to understand what you're seeing, call on the expertise of our Incident Response team. They'll help you investigate and resolve any incident, whether you're a Varonis customer or trial user.

MATT RADOLEC

Security Architecture & Incident Response

Try Varonis Free

All Varonis products are free to try and come with an engineer-led risk assessment. The easiest way to get started is with a short 1:1 demo and discovery conversation.

CONTACT US