



STOP RANSOMWARE.

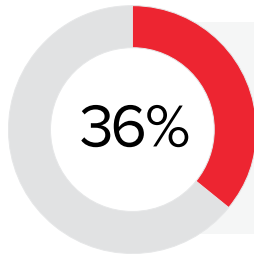
Varonis is a powerful software suite that protects you from insider threats and cyberattacks.

Varonis works across the whole organization – it works with our infrastructure, our active directory, it works on all the hardware and software we have. It's allowed us to see what goes on – and see what's out there.

We were able to detect and disable a ransomware infection within 10 minutes of an attack

– Wade Sendall | Vice President of IT, Boston Globe

The Boston Globe



36% of Varonis customers have detected ransomware with DatAlert

[SEE WHAT OTHER CUSTOMERS ARE SAYING HERE](#)

How does it work?

Varonis detects ransomware on your core IT systems: file servers, NAS and the cloud - where terabytes of your most critical data lives – and stops the attack in its tracks.

Our ransomware defense architecture is designed to protect enterprise data from zero-day attacks – catching ransomware that traditional perimeter security doesn't see.



Detect Ransomware

Spot malware, insider threats, and cyberattacks from the inside.

Monitor and alert on suspicious user activity and behaviors that resemble ransomware with predictive threat models and trigger automatic responses that stop attacks before it's too late.



Prevent Damage

Least privilege means an infected user can't do as much damage in the first place

Reduce the attack surface area by identifying and locking down loose and misconfigured access controls that ransomware and attackers exploit.



Recover Quickly

Simplify recovery with a complete record of everything that was encrypted.

Investigate suspicious behavior and security incidents, and search a comprehensive log of every file touch to see affected files, users and devices.

Why Varonis?

- Analyze behavior and activity across multiple platforms and detect suspicious activity and potential data breaches with a defense in-depth approach.
- Discover overexposed sensitive data and global groups that lead to increased security vulnerabilities and ransomware infections.
- Prioritize remediation by reducing access to sensitive and regulated data, and automate and maintain a least privilege model.
- Utilize threat models specifically designed to fight back against malware: detecting encryption of multiple files, patterns that resemble known ransomware behaviors, and actions that suggest malware (not human) activity.
- Get the latest malware defense with a dedicated research lab of security experts and data scientists who continually develop new threat models to help detect the stealthiest of zero-day malware.

Platform Coverage

Protect your most valuable data wherever it lives.





Live Demo

Set up Varonis in your own environment and see how to stop ransomware and protect your data.

info.varonis.com/demo



Data Risk Assessment

Get your risk profile, discover where you're vulnerable, and fix real security issues.

www.varonis.com/rra

We wanted to ensure that we could prevent and monitor any ransomware or malware attacks: DatAlert has allowed us to do that very easily.

It was demonstrated very quickly that this is a product that works – Varonis does what it says it can do.

– Ron Mark | Innovation & IT Manager, Gas Strategies

We help thousands of customers prevent data breaches.



ING



Nasdaq

CHAMPAGNE
BOLLINGER
MAISON FONDÉE EN 1829

EMC²

TOYOTA

LUXEMBOURG
INSTITUTE
OF HEALTH
RESEARCH DEDICATED TO LIFE

L'ORÉAL