USE CASE: STOPPING RANSOMWARE BEFORE IT'S TOO LATE

An employee of a large hospital clicked on a well-crafted phishing email and downloaded Locky. The employee had access to terabytes of NAS data via mapped SMB drives.

DatAlert sent a critical event to security operations after detecting abnormal file modified events. They were able to disable the account and restore the affected files with minimal headache.

See www.varonis.com/ransomware for more.

How does Varonis protect your file servers and NAS from ransomware and cyberattacks?

Varonis catches ransomware when it gets past your endpoints — protecting file and email servers, where terabytes of your most critical data lives.

Varonis has been collecting and analyzing file system activity and other metadata unavailable to traditional security products UBA systems for over a decade, and we've learned to distinguish between human and machine activity -- they look different. We do the threat analysis and send hi-fidelity alerts via email, syslog, to your SIEM, and even allow you to automate a response to lock out the offending user account and stop further damage.

Our DatAlert Threat models are designed to detect zero-day attacks and fight back against malware: detecting encryption of multiple files, patterns that resemble ransomware behaviors, and actions that suggest malware (not human) activity.

Relevant DatAlert Threat Models

- Pattern detected: user actions resemble ransomware
- Crypto intrusion activity
- Encryption of multiple files