
VARONIS
DATALERT SUITE

VARONIS DATALERT SUITE

Detect and alert on suspicious activity on your file and email systems.

DATALERT:

- Monitor critical assets for suspicious activity and unusual behavior
- Cross-platform event monitoring on Windows, UNIX/Linux, NAS, Active Directory, SharePoint, or Exchange
- Trigger alerts across multiple platforms, helping you detect potential security breaches, misconfigurations, and other issues
- Detect critical events and compromised assets
- Reduce the amount of time it takes to find and assess a real issue

DATALERT ANALYTICS:

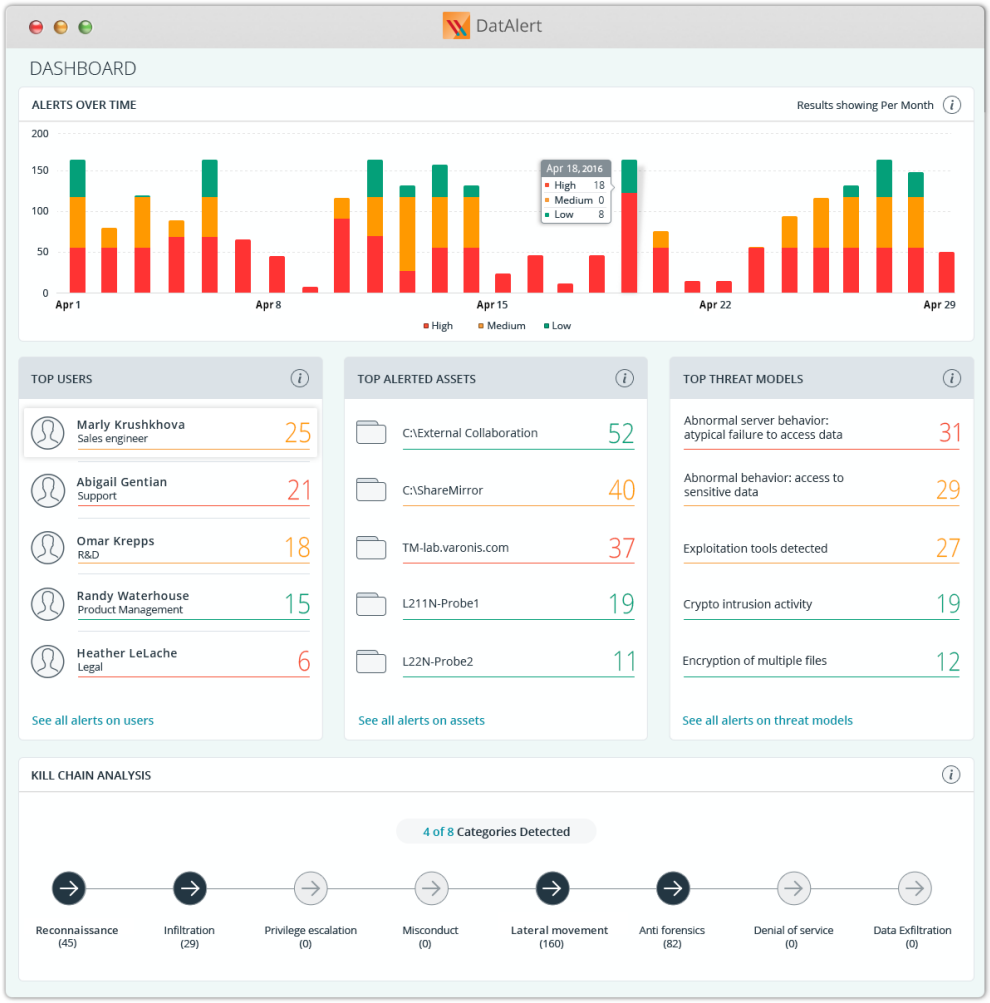
- Automate threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning
- Profile user roles and service accounts and baseline how they use file and email systems and interact with Active Directory
- Get meaningful insights into user and data patterns, security risks, and social connections
- Defend against insider threats, ransomware, and potential data breaches

VISUALIZE, INTERPRET, AND ANALYZE YOUR DATA:

- Use the DatAlert web-based dashboards to help score, triage, analyze, and prioritize alerts and take action to resolve incidents
- Configure alert criteria and output the way you need it
- Trigger custom actions with command line execution
- Easily integrate with SIEM and network management solutions

VARONIS BEHAVIOR RESEARCH LABORATORY:

- A dedicated team of security experts and data scientists from Varonis continually introduce new behavior-based threat models
- Stay up-to-date on the latest security issues, APTs, and insider threats, and how to defend against them



MONITOR, ANALYZE, AND DETECT:

- Ransomware behavior
- Unusual file activity
- Unusual mailbox and email activity
- Access to sensitive data
- Unauthorized access attempts
- Unusual encryption activity
- Accumulative analysis on idle and sensitive data
- Unusual access to system files
- Unauthorized data access
- Unusual encryption activity
- Misconfigurations
- System intrusion
- Unauthorized privilege escalations
- Mass delete behaviors
- Abnormal lockout behaviors
- Attempts to damage and destroy operational files
- Exploitation tools
- Membership changes
- Modifications to critical files and units
- Modifications to critical GPOs
- Suspicious access activity
- Permission changes
- Brute force attacks
- Attempted data exfiltration