



May 4, 2017

Varonis Unveils New Automation Engine to Reduce File Exposure in Minutes; Presents at Dell EMC World 2017

Extends the Varonis Data Security Platform with Automated Remediation, Enhanced Forensic Investigations and Account Hijacking Prevention

NEW YORK, May 04, 2017 (GLOBE NEWSWIRE) -- [Varonis Systems, Inc.](#) (NASDAQ:VRNS), a leading provider of software solutions that protect data from insider threats and cyberattacks, today announced the upcoming release of the Varonis [Automation Engine](#), new threat models within [DatAlert](#) and DatAlert Analytics Rewind: advanced forensic intelligence that allows customers to analyze past user and data activity.

Expected this quarter, Version 6.3.170 of the Data Security Platform (DSP) introduces the Automation Engine that automatically finds and fixes some of the most dangerous file system security issues so that organizations are less vulnerable to attacks, more compliant and consistently enforcing a least privilege model. Varonis will showcase the Automation Engine at Dell EMC World, May 8-10, in Las Vegas, Nevada in booth #641 in the expo hall.

"A common misconception about data breaches is that they are sophisticated attacks, but in reality they are frequently opportunistic, where insiders or attackers that have bypassed perimeter defenses take advantage of excessive user access through global groups. In the recent [Varonis Data Risk Report](#), we found that 20% of all folders on average within an organization were open to every employee, and in 47% of the cases analyzed, at least 1,000 files containing sensitive data and falling under compliance regulations like PCI, HIPAA or GDPR were open to all users," said Ken Spinner, VP of Field Engineering at Varonis. "We are excited to launch the Automation Engine to help organizations close a serious audit gap and reduce an attacker's ability to exploit misconfigured permissions hidden many levels down in a directory tree."

"Terrorists, spies and crooks motivated by money and malice are in pursuit of intellectual property or damaging personal information and exploit vulnerabilities in U.S. companies' information systems," said John P. Carlin, former Assistant Attorney General for National Security and current Chair of Morrison & Foerster LLP's Global Risk and Crisis Management Group. "Companies have to prepare to mitigate risk from a breach by safeguarding sensitive files and eliminating unnecessary access. The [Varonis Data Risk Report](#) highlights what I have seen in government and in private practice: that too many companies and governments today are relying on firewalls and not taking basic steps to reduce risk once the bad guy is inside the perimeter. We need to get better at this if we hope to keep pace with the rapidly evolving threat landscape and defend against increasingly sophisticated actors." John Carlin will present with Varonis at Dell EMC World, Wednesday, May 10 from 12:00 — 1:00 p.m. PT in Palazzo I in the session titled: "Lessons from the trenches: What investigating cyber incidents at DOJ taught me about where cybersecurity preparedness falls short."

Organizations must address global access — access that includes every user and service account in the organization — and fix inconsistent Access Control Lists (ACLs) in order to eliminate unnecessary access. A manual remediation project of these two issues that does not disrupt employee productivity requires at least three to six hours of work per misconfigured folder. With the Automation Engine, customers will be able to automatically remediate entire servers — thousands of shares and folders — in minutes after initial setup.

The Varonis Automation Engine:

- | Discovers and automatically repairs broken and over-permissive access controls
- | Automatically fixes hidden vulnerabilities that hackers and insider threats will exploit, such as overly accessible confidential files that can be accessed by everyone, without introducing business disruption
- | Safely automates necessary remediation steps to achieve and sustain a least-privilege model, where employees only have access to files they need to do their jobs

Other highlights of the upcoming release:

- | DatAlert Analytics Rewind allows customers to analyze past user and data activity to identify attacks that may have occurred in the past and pre-emptively tune out false positives
- | New DatAlert Threat Models detect suspicious mailbox and Exchange behaviors, password resets and unusual activity from personal devices
- | Support for NetApp ONTAP Cloud Data Storage

Learn more about the upcoming release at booth #641 in the expo hall at Dell EMC World, May 8-10, 2017 in Las Vegas, Nevada and attend one of our sessions:

- | **Wednesday, May 10, 12:00 p.m. — 1:00 p.m., Palazzo I: John P. Carlin**, Partner and Chair, Global Risk and Crisis Management, Morrison & Foerster LLP; Former Assistant Attorney General for National Security, presenting with Varonis at the session: "Lessons from the trenches: What investigating cyber incidents at DOJ taught me about where cybersecurity preparedness falls short."
- | **Monday, May 8, 7:30 p.m. and Wednesday, May 10, 2:00 p.m., Connect Tech Booth #1722 in the expo hall: Brian Vecci**, Technical Evangelist for Varonis, discussing how Varonis DSP and Dell EMC Isilon mitigate and stop ransomware attacks.

Additional Resources

- | Watch a video to learn about the benefits of the Varonis Automation Engine:
<https://www.varonis.com/products/automation-engine>.
- | For more information on Varonis' solution portfolio, please visit www.varonis.com.
- | Visit our [blog](#) and join the conversation on [Facebook](#), [Twitter](#), [LinkedIn](#), [Podcast](#) and [YouTube](#).

About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through its innovative Data Security Platform, Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search, and file synchronization and sharing. With offices and partners worldwide, Varonis had more than 5,500 customers as of March 31, 2017, spanning leading firms in financial services, healthcare, public, industrial, insurance, energy and utilities, media and entertainment, consumer and retail, technology and education sectors.

News Media Contact:
Jennifer LuPiba
614-338-9889
jlupiba@varonis.com