NEWS RELEASE

Varonis Announces Trailblazing Features for Securing Sensitive Data in Salesforce

4/26/2022

New capabilities identify excessive permissions and misconfigurations, classify sensitive data in files and attachments, and detect data exfiltration attempts

NEW YORK, April 26, 2022 (GLOBE NEWSWIRE) -- **Varonis Systems, Inc.** (Nasdaq: VRNS), a pioneer in data security and analytics, today **announced** groundbreaking new features to help companies close critical security and compliance gaps in Salesforce.

These enhancements are part of DatAdvantage Cloud, which gives customers a single pane of glass to protect critical data across Salesforce, Google Drive, Box, AWS, Okta, Jira, Slack, GitHub, and Zoom.

Salesforce can be a blind spot for security and compliance teams. Over time, permissions sprawl out of control, misconfigurations arise, and countless apps connect to Salesforce via APIs to read and write data.

Most organizations can't see where sensitive data lives within Salesforce, who has access to it, or who uses it, making it difficult to maintain a strong security posture and comply with regulations such as GDPR, HIPAA, SOX, and PCI-DSS regulations.

This new release of Varonis for Salesforce represents a breakthrough in SaaS data protection, with capabilities to address a broad range of security and compliance use cases:

- Quickly understand exposure: Varonis radically simplifies permissions analysis by revealing a user's net effective permissions and how they got them — so you can finally answer the question, "Who can access sensitive data?"

- Classify sensitive files and attachments: Varonis scans files attached to objects in Salesforce and auto-tags sensitive items using patented data classification technology.
- Right-size sprawling permissions: Fix compliance gaps and reduce exposure — from former employees and ex-contractors with active logins to regular users allowed to export every record.
- Detect anomalous activity: Out-of-the-box alerts can detect internal and external threats, such as users accessing an unusual number of Salesforce objects or an admin deactivating a critical update.
- Pinpoint misconfigurations: The SSPM dashboard helps detect problems with organization-wide settings, discover shadow instances, and spot vulnerabilities such as misconfigurations that can expose data publicly.

"I'd heard horror stories about Salesforce permissions and how literally hundreds can be applied in a manner of different ways, but I didn't realize how complicated our permission sets had grown," said Tony Hamil, Senior Cybersecurity Engineer at a top real estate organization. "DatAdvantage Cloud is a single pane of glass that not only helps us secure data in Salesforce, but also gives us cross-cloud visibility that we couldn't get otherwise."

"Salesforce is one of the biggest and most complex repositories of confidential and regulated data," said David Bass, Executive VP of Engineering and Chief Technology Officer, Varonis. "This new release gives customers critical visibility and protection they simply can't get natively. Varonis' platform approach helps companies unify their cloud security controls and detect threats across their SaaS environment within a single, easy-to-deploy product."

Varonis for Salesforce is available now to customers and trial users. Sign up for a complimentary **SaaS Data Risk Assessment** to evaluate your security posture, lock down overexposed data, and remediate risks.

Additional Resources

- Read about **today's news** on our blog.
- Learn about **Varonis for Salesforce**.
- Request a **demo** from the Varonis team.
- For more information on Varonis' solution portfolio, please visit **www.varonis.com**.
- Visit our **blog**, and join the conversation on **Twitter**, **LinkedIn**, and **YouTube**.
- **Watch and subscribe** to SecurityFWD, Varonis' YouTube show covering the latest infosec tips, tricks, and tools.

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property. The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a

secure state with automation. Varonis products address additional important use cases including data protection, data governance, Zero Trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Investor Relations Contact:
James Arestia
Varonis Systems, Inc.
646-640-2149
investors@varonis.com

News Media Contact:
Rachel Hunt
Varonis Systems, Inc.
877-292-8767 (ext. 1598)
pr@varonis.com

Source: Varonis Systems, Inc.