VARONIS

Embracing a Zero Trust Security Model

The U.S. National Security Agency (NSA) recently issued guidance strongly recommending a Zero Trust security model for all critical networks, including NSS, DoD, and DIB systems. Varonis aligns with NSA guidance.

NSA Guidance	Varonis Capabilities
Define mission outcomes — Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).	• Automatically identify and classify secret, top secret, confidential, and CUI data within your environment • Apply labels to critical data to enforce policies such as obfuscation, encryption, etc.
Architect from the inside out — First, focus on protecting critical DAAS. Second, secure all paths to access them.	• Map out an environment's permission structure to visualize and understand where critical data lives, who has access, and who uses their access • Pinpoint where data is overexposed and automatically flag users who no longer need access
Determine who/what needs access to the DAAS to create access control policies — Create security policies and apply them consistently across all environments.	• Set organization-wide policies that only allow users with certain credentials to access specific sensitive or regulated data • Require users to submit data access requests before they are granted access to specific sets of data • Make access changes at scale and maintain least-privilege access over time
Inspect and log all traffic before acting — Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.	• Comprehensive audit logs let administrators track file and email activity both on premises and in the cloud • Behavioral threat detection automatically alerts on abnormal user behavior and can trigger responses to shut down user sessions and change passwords to limit damage

Reach Zero Trust Maturity with Varonis

	Zero Trust Roadmap	Varonis Capabilities
Without Zero Trust	**Preparation**	• Conduct a free risk assessment to understand where sensitive data is overexposed and at-risk to potential threats
With Zero Trust	**Basic**	• Identify and classify regulated data across the entire environment and map out permission structures to understand how data is stored, accessed, and used • Learn where data is overexposed and remove excessive access to ensure only those that require access have it
	Intermediate	• Automatically create baseline behavioral profiles to flag and alert on suspicious behavior • Use a unified audit trail to see who's been opening, creating, deleting, or modifying critical data
	Advanced	• Use automated responses to shutdown user sessions and change passwords when abnormal behavior is detected • Automatically find and safely remediate global groups and inconsistent permissions on entire servers • Expand the detection window by combining network traffic with data access activity • Require users to submit requests to access data

Get started.

To learn more about how to implement Zero Trust in your environment, contact our U.S. Public Sector team.

CONTACT US