VARONIS

Zero Trust Extended Ecosystem

The Zero Trust security model focuses on creating security controls that place data at the center of it all and ensures that organization's are prepared for an inevitable security breach. Every aspect of an IT environment needs to be inspected, monitored, and secured, starting with the data itself, and building out from there.

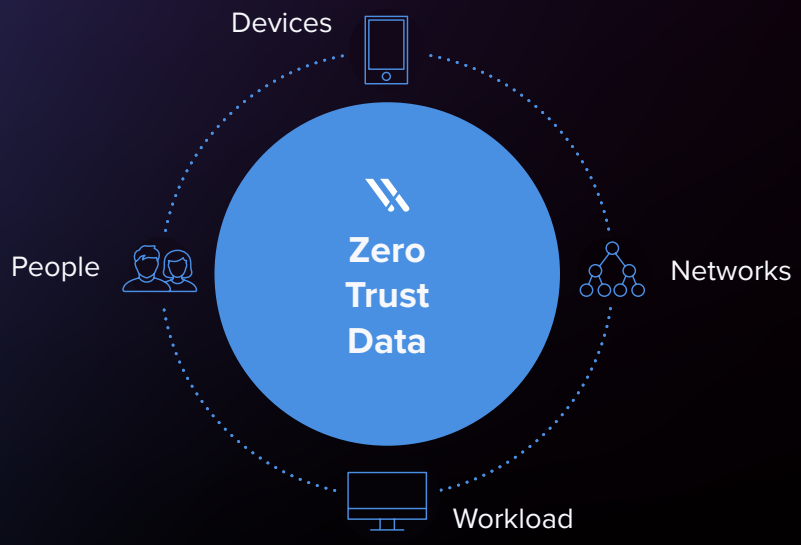
Varonis is a data-centric security solution that correlates data activity to users, devices, and network telemetry to present a complete record of cybersecurity incidents.

Varonis can help agencies:

- Automatically identify confidential information
- Pinpoint data exposure and spillage
- Revoke unneeded access
- Automate attack surface reduction
- Detect and stop APTs, ransomware, and insider threats

"The driving force behind Zero Trust was to move security pros from a failed perimeter-centric approach to security to a model that was much more data- and identity-centric and better adapted for today's digital business."[1]

Zero Trust Security Model

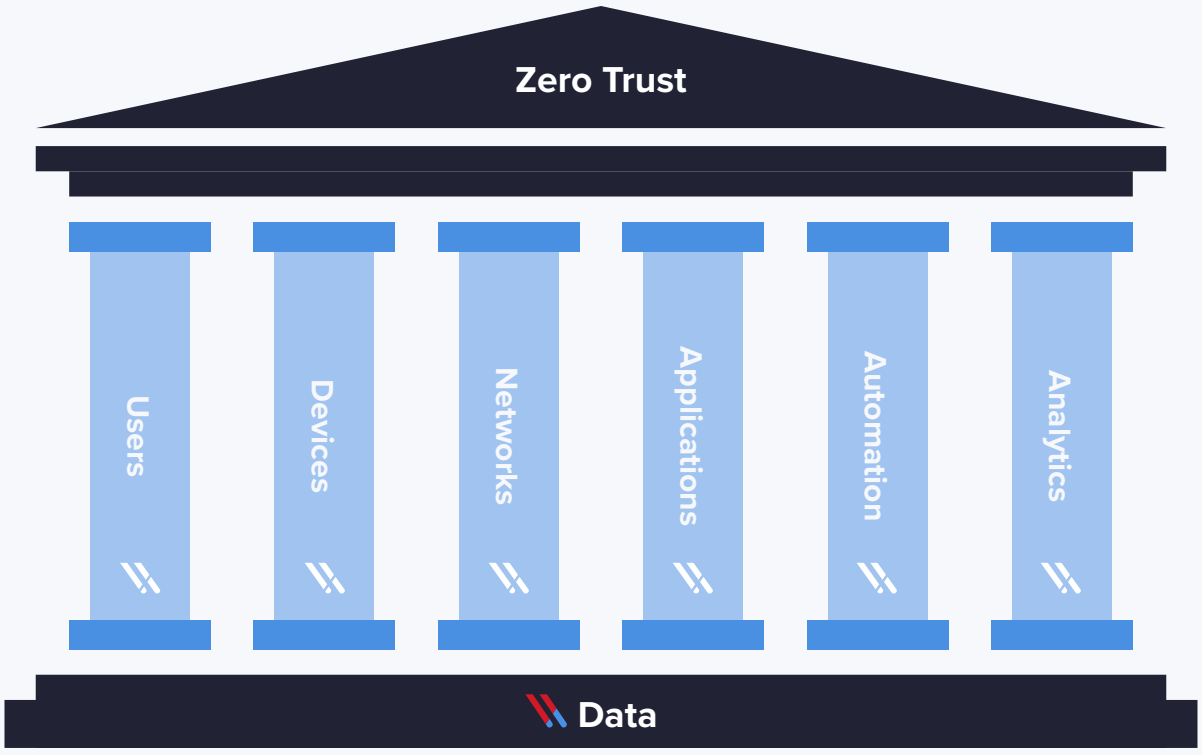


[1] Chase Cunningham, "The Zero Trust eXtended (ZTX) Ecosystem, Strategic Plan: The Zero Trust Security Playbook," Forrester Research, July 11, 2019.

The Structure of the Zero Trust Framework

The foundation of the Zero Trust framework is data — and for good reason. It's ultimately what attackers want to steal. Protecting the perimeter alone is not an effective strategy when defending against modern day attacks. Instead, agencies should focus on securing the center of it all — the data.

The pillars of the Zero Trust framework have been built upon the foundation of securing data to support a complete Zero Trust security model. These pillars consist of securing users, devices, networks, and applications, along with effectively utilizing automation and analytics. Aligning with this structure, Varonis helps create a comprehensive security solution.



Zero Trust Pillar	Varonis Capability
Users	• Automatically flag where users have excessive access • Strictly limit and enforce users' access to data • Use machine learning algorithms to learn how users behave and alert on any abnormal or suspicious behavior • Determine data owners by looking at data activity and automatically assigning owners
Devices	• Gain insight into a device's trustworthiness through information gathered from Active Directory, perimeter telemetry, and activity on the file system — without deploying an endpoint agent • Automatically pair users to devices, aiding in detecting suspicious behavior
Network	• Block easy entry-points by automatically fixing misconfigurations in Active Directory, Exchange, SharePoint, and file servers • Analyze VPN, DNS, and web activity in context with data, email, and Active Directory behavior to detect potential threats • Visualize and report on indicators of compromise hiding in your network traffic
Applications	• Monitor AD groups to gain visibility into who has access to an application and give an automated workflow for owners to monitor and manage this access • Track file integrity and alert on changes to configuration files that could weaken the security posture of an application • Monitor and alert on access to applications from unsanctioned, blacklisted, or unreasonable locations around the world
Automation	• Identify and classify sensitive data automatically • Use automation to provide insight into where data is overexposed • Detect threats based on data activity using machine learning algorithms • Automatically remediate overexposed files and folders • Enforce privacy policies automatically
Analytics	• Monitor and analyze data access events, Active Directory events, and network telemetry in real-time • Perform real-time data risk assessments to measure exposure, track vulnerabilities, and constantly assess your Zero Trust posture • Run continuous data classification scans to ensure your inventory of sensitive data is current • Use a unified audit trail to know who has been opening, creating, deleting, or modifying important files

Get started.

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

CONTACT US