VARONIS

WHITEPAPER

Zero Trust
with Varonis

Contents

Today's **Threat Landscape**

Today's cybersecurity threat landscape is everchanging. Long gone are the days where companies operated solely within their own four walls and could be protected by perimeter-based security. As business has moved to the cloud, the concept of a "secure perimeter" has become a thing of the past.

The question is not **"if"** an attacker will get in, but **"when."**

Zero Trust is a security strategy developed by industry analysts at Forrester Research who recognized the shortcomings of perimeter-based security and argue instead that organizations should design their security controls to be data-centric. Understanding what's happening to your data— knowing whether it's sensitive or confidential, over-exposed, or under attack—is a more effective approach for protecting data proactively then relying in perimeter-based security alone.

Organizations should assume hackers will be able to penetrate their network. The question is not "if" an attacker will get in, but "when." All it takes to compromise a network is a subtle misconfiguration or stolen credentials to give bad actors the entry point they need. And, once they're in, it's often not hard for them to gain access to the valuable data they're after, especially on infrastructure that doesn't adhere to a Zero Trust, least privilege model.

To limit the potential damage bad actors can do once inside and proactively detect suspicious activity by insiders or malware, organizations should focus first on defending their data—the asset hackers are ultimately after. Varonis is a pioneer in data security whose capabilities can help organizations implement data security in line with Zero Trust.

Zero Trust as a **Security Strategy**

Zero Trust is a framework designed to help enterprises decrease their attack surface, protect themselves against common attack vectors, and improve detection and response to threats. On why Forrester developed Zero Trust, Forrester analyst Chase Cunningham writes:

> "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, where even the most basic business processes are rarely self-contained within the four walls of the corporation."[1]

The framework involves several layers of defense, including data protection, network segmentation, identity and access management, application stack security, and device management. All of these controls are designed to help enterprises better defend their assets against increasingly stealthy cyber attackers.

- **Secure sensitive data**
  Identify and limit access to sensitive data to limit possible exposure
- **Segment your network**
  Segment your network in order to limit lateral movement of attackers or spreading of malware
- **Limit user access**
  Limit and strictly enforce what users can access
- **Secure application stack**
  Treat every connection, app, and component as a threat vector and ensure Zero Trust principles are applied throughout your technology stack
- **Manage devices**
  Isolate, secure, and control every device that is connected to the network

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

Data-Centric Security

"The average employee has access to 17M files."

At the heart of the Zero Trust framework is data—and for good reason. It's something that all the other areas touch, and it's the most granular level of defense organizations have. Forrester states, "perimeter-based security has failed."

A better security practice, they argue, is to assume attackers will infiltrate your network and set controls up to limit the possible damage when they do. This involves practices like identifying and securing your sensitive data, ensuring that only the people who need access to it have it so that one random entry point can't easily compromise valuable data, or segmenting your network to make it harder for attackers to move laterally or for malware to spread.

One of the challenges with data security is that sensitive information lives everywhere—in files, emails, cloud-based collaboration sites like SharePoint or Office 365. An organization's most valuable data is often unknowingly exposed, buried in files that are open to everyone at a company.

Varonis is a data-centric security company that works with more than 6,900 customers to secure their most sensitive data. Based on thousands of real-world data risk assessments, Varonis compiles an annual Global Data Risk Report that sheds light on the state of data exposure. The findings from 2019 reveal that the average employee can access 17M files—far more than they need to do their jobs. On average, 22% of a business's globally accessible data is sensitive.[2]

Over-exposed data is arguably the biggest problem in data security, both because the challenge and risk compounds as data continues to grow, and because finding and remediating data exposure is a time-consuming and error-prone process that can interrupt business operations. According to Forrester, the average enterprise today has petabytes of data that will continue to grow 15-30% annually.[3] Of that data, approximately 80% of it is unstructured data like files and emails, according to industry estimates.[4] Alan Dayley, Julian Tirsu, Guido De Simoni, Garth Landers, Marc-Antoine Meunier, "Market Guide for File Analysis Software," Gartner Research, March 27, 2018. Imagine all the valuable information within an organization that's saved in files—roadmaps, customer lists, credit card information, personally identifiable information—the list goes on. Today, that information likely lives in hybrid environments—both in on premises data stores and in the cloud, which adds additional complexity, especially with sharing links.

Between their many data stores, very few organizations know where all their sensitive data exists, who has access to it, and what they're doing with it, which creates considerable risk. Executive boards are no longer willing to stomach this risk, but IT security teams struggle to find sustainable data protection solutions. Varonis is one of the few solutions that can help IT teams remediate over-exposed data, which dramatically reduces their attack surface.

To effectively protect data, organizations need visibility into where they have sensitive data across their different data stores, analytics to be able to identify where that data may be overexposed and when it might be compromised, and the ability to take action to remediate access issues. Zero Trust embeds these concepts into their framework as overarching principles across all areas.

2 "2019 Varonis Global Data Risk Report," https://www.varonis.com/2019-data-risk-report/

3 Andras Cser and Sean Ryan, "Apply Zero Trust eXtended Principles In Your Identity And Access Management Programs, Protect Data And Boost The User Experience With A ZTX IAM Architecture, People, And Process," Forrester Research, November 25, 2019.

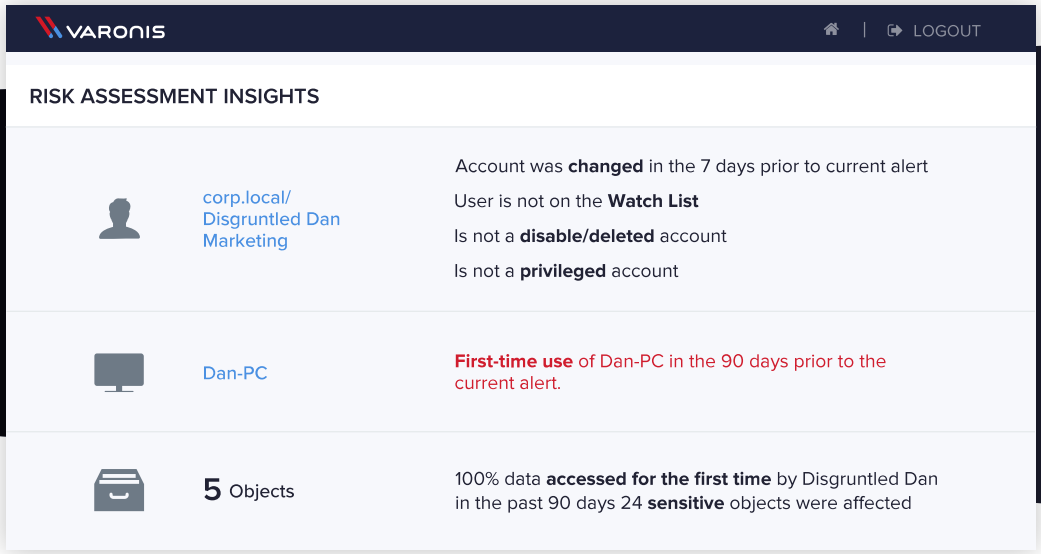
4 Alan Dayley, Julian Tirsu, Guido De Simoni, Garth Landers, Marc-Antoine Meunier, "Market Guide for File Analysis Software," Gartner Research, March 27, 2018.

Visibility & Analytics

Visibility is a big gap for many organizations. You can't protect what you don't know exists. Many teams may think sensitive data only lives in certain applications or databases, but we all know how confidential information often makes its way into email conversations, chats, or personal drives.

Identifying sensitive data is a key first step to protecting it. The challenge with some technologies that provide increased visibility, however, is that they can also create a ton of noise. IT and security professionals are already understaffed and overworked. They need visibility, but more importantly, they need actionable visibility that can help them defend. Chase Cunningham writes:

"Visibility is key in defending any valuable asset. You can't protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the tell-tale signs of a breach in progress and stop it."



High-fidelity alerts enriched with context from data access, Active Directory, and perimeter telemetry

Analytics are a key ingredient for bringing focus to increased visibility. Varonis uses analytics to provide IT professionals with insight into how data is being used and makes recommendations on where a user may have too much access. This helps risk & compliance teams prioritize where they focus for maximum risk reduction.

For security professionals, Varonis can help detect threats by bringing together information from multiple sources, including file activity and perimeter telemetry, and alerting on anomalous activity that could indicate a threat. Visibility and analytics apply to all aspects of Zero Trust as a way to increase threat awareness and defense effectiveness. But even with increased focus on where to prioritize efforts, all of it is useless without being able to act on it.

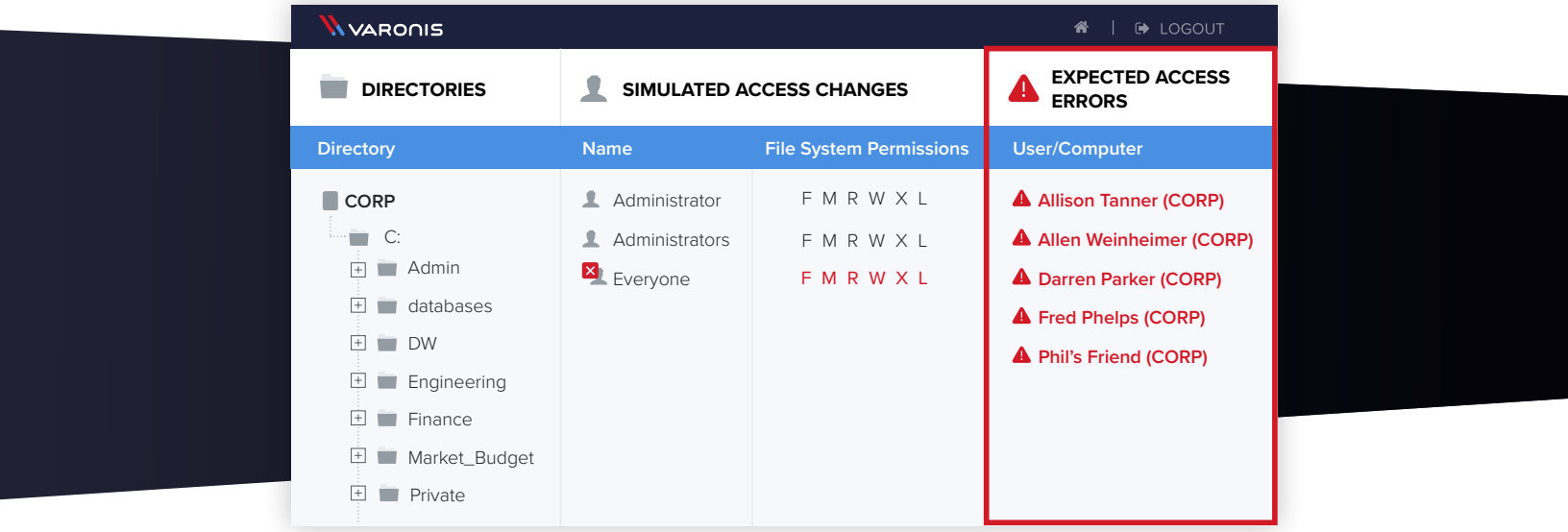
Automation & Orchestration

On top of visibility and analytics, Forrester adds automation and orchestration as the outermost layer of their Zero Trust model. With the right visibility and analytics, IT and security teams know where to focus, and with the help of automation and orchestration, they can tackle the scale of many of the problems that they're facing today.

From a data security perspective, automation is a necessary approach for remediation. The scale at which data grows and the complexity of managing access to it is too cumbersome to do manually. "Fixing" one access problem can inadvertently cause more problems, not to mention the business disruptions that can also result. Automation is the only realistic way to tackle global access groups and other examples of overexposure. When sensitive information is only accessible to the people who absolutely need access, it's a lot harder for attackers to gain access to it, even if they penetrate your network.

Varonis harnesses automation both to remediate access issues, which can help organizations reduce their attack surface, and to limit the damage of potential attacks with automated response. Cyber attacks happen around the clock. A Chinese APT doesn't care if your U.S.-based security team is sleeping—in fact, they'd prefer it. Varonis has automated methods to shut down accounts that exhibit anomalous and potentially malicious behavior which can limit damage dramatically and save organizations millions of dollars in remediation costs. To take on today's security challenges, organizations need the help of automation to act on the increased visibility and analytics that technology vendors can provide.

Several technology vendors can provide visibility into which users can access what data, but few can enable the actions that are needed at scale to remediate these risks. Varonis believes security should start with data and provides the visibility, analytics, and automation necessary to help organizations limit their attack surface, reduce risk, and detect and respond to threats.



Access changes simulated based on actual activity to minimize business disruption when committing changes

VARONIS

Varonis and Zero Trust

For any organization pursuing a Zero Trust strategy, data security is a key first step. Protecting data is one of the most foundational concepts of Zero Trust, but it's a concept that's easier to understand than implement. Varonis is a pioneer in data-centric security. Our inside-out approach to security helps organizations limit their attack surface and proactively detect threats, by surfacing where their sensitive data lives, allowing them to control who has access to it, and monitoring activity for suspicious behavior.

At its core, the Zero Trust framework is meant to provide organizations with a practical way to think about attacks and how to protect themselves against them. If there's one thing in common among cyber attacks, it's that they're aimed at stealing data. By implementing security practices in line with Zero Trust, organizations can make their data difficult to steal, resulting in better security no matter how the attack is carried out.

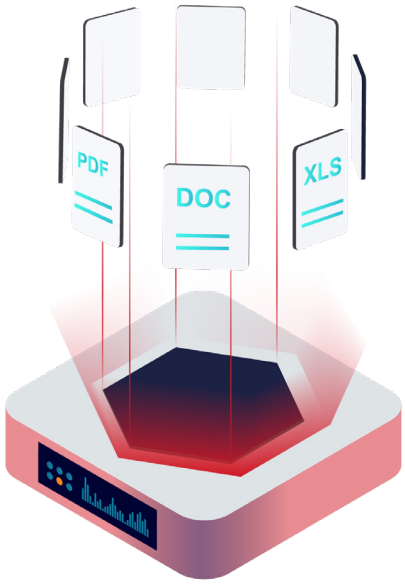
Forrester outlines these 5 steps for getting started with Zero Trust. Here's how Varonis can help.

VARONIS

Forrester's 5 Steps to Zero Trust Information Security

1 **Identify** your sensitive data

Data is what hackers want to steal. To protect it, you need to know where it is and who has access to it so you can limit the avenues through which this data could be compromised.



How Varonis can help:

- **Automatically discover and classify** sensitive on premises and in the cloud at petabyte scale
- **Leverage a library of hundreds of pre-built, always-updated classification rules** (HIPAA, PCI, GDPR, CCPA, etc.) with sophisticated validation algorithms to ensure accuracy and reduce false-positives
- **Prioritize data in terms of risk—**where sensitive data is concentrated and exposed at both file and container levels
- **Report on exposure** through global groups, external links, and excessive group memberships
- **Identify stale sensitive data** and quickly archive, quarantine, or delete at-risk files that are no longer needed
- **Apply labels to classified files and enforce DRM policies** and automate encryption though integration with Microsoft Azure Information Protection (AIP)

To ensure speed and scale, Varonis leverages its file activity audit trail for true incremental discovery of new and modified data. Scanning is distributed and multi-threaded, so scanning is performed in close network proximity to the monitored nodes and multiple servers can be scanned at once. Files are streamed, not copied, to reduce disk I/O and increase performance. Our classification engine prioritizes what to scan first, based on exposure and other factors to get actionable results quickly.

To ensure accuracy, Varonis uses flexible condition matching, algorithmic verification, proximity matching, smart filtering, and more. Matches are compared against databases of valid values (e.g., medical terms). Varonis also identifies various structures within documents and can target the search to these areas.

VARONIS

2

Map the flows of your sensitive data

Knowing what's happening with your data can help you identify whether an attack is underway. By understanding typical user behavior and monitoring for suspicious activity or common attack patterns, like command-and-control attacks, you can quickly identify potential threats and respond quickly. Furthermore, understanding how data is flowing throughout your business can better equip you to meet privacy regulations.

How Varonis can help:

- **Create a visual map of your data estate—**both on premises and in the cloud—and identify who has access to it and whether they should have access
- **Record a searchable & sortable forensic record** of all file access (open, move, modify, delete, rename), email activity, network events (proxy, VPN, DNS), and permissions changes—scalable to billions of events per day
- **Continuously monitor** data access, email behavior, Active Directory events, and network activity to detect and respond to potential threats
- **Detect and respond to abnormal behavior** with out-of-the-box threat models that baseline access patterns, perform peer analysis, learn working hours, device usage, geolocation, logon behavior
- **Easily comply with privacy regulations** by storing PII properly, ensuring data is shared appropriately, and being able to quickly complete data subject access requests (DSARs)

Varonis also has visibility from DNS, VPN, and proxies to spot attacks or exfiltration at the perimeter. We put this telemetry in context with data access, giving analysts meaningful alerts. Inspection is available for on-premises and cloud data, email servers, and network devices.

Forensics investigations features allow analysts to search & filter activity from any user, device, IP, etc. with many built-in searches (e.g., "Sensitive data access by users on a watch list").

VARONIS

3

Architect your Zero Trust microperimeters

The concept of microperimeters is essential to Zero Trust. It's based on the principle of segmenting your network to limit an attacker's ability to move laterally through it and limiting data access to make it more difficult for attackers to gain access and steal data. Being vigilant about access control minimizes your attack surface and helps you limit damage.

How Varonis can help:

- **Get a comprehensive view of what people can access** by correlating user and groups to access control lists on data repositories on prem and in the cloud
- **Ensure data is not over-exposed** by resolving all user & group memberships and access levels, including complex and deeply nested relationships
- **Automatically detect when a user no longer requires access to a resource** based on usage activity and cluster analysis
- **Automatically revoke permissions** to a resource, group, or data based on a time window or change in policy
- **Identify abnormal events in your VPN or proxy traffic—**such as brute force activity, connections to suspicious URLs or hosts, and geo-hopping
- **Analyze DNS traffic** to detect behavior such as DNS tunneling or reverse DNS queries that may signal exfiltration or reconnaissance
- **Identify, alert, and remediate on access control changes to critical resources** (e.g., CEO's mailbox) or configurations (e.g., GPO change, user added to Domain Admins)

4

Continuously monitor your Zero Trust ecosystem

Data isn't static, and neither are permissions; data is constantly being created and shared, and people's roles and need for access change. Having an ongoing process to manage access is key for maintaining a least-privilege model that thwarts hackers' ability to get to what they want. Understanding users' typical behavior and monitoring for anomalies can also help you quickly identify when something is amiss.

How Varonis can help:

- **Run continuous data classification scans** to ensure your inventory of sensitive data is current
- **Perform daily crawls of access control lists and user/group repositories** so that visualizations and mappings reflect up-to-date effective permissions
- **Monitor and analyze** data access events, Active Directory events (logons, permissions changes, GPO changes, password resets), and network telemetry in real-time
- **Alert on suspicious activity** by determining users' typical behaviors, including normal working hours, geolocation, user-device pairs, and peer analysis
- **Establish a process for ongoing access management** by identifying data owners and giving them control of access control decisions
- **Perform real-time data risk assessments** to measure exposure, track vulnerabilities, and constantly assess your Zero Trust posture
- **Ensure business processes aren't interrupted** by modeling access control changes in a sandbox before implementing them

5

Embrace security automation and orchestration

Manually remediating data access issues is a time-consuming process that inevitably leaves gaps. Automation and orchestration are necessary in today's threat landscape not only to bolster organizations' defenses, but also to enable them to more quickly respond to threats.

How Varonis can help:

- **Automatically discover and remediate over-exposed sensitive data,** including data exposed via shared links–like automated patching, but for your data
- **Block easy entry-points** by automatically fixing misconfigurations in Active Directory, Exchange, SharePoint, file servers, etc.
- **Trigger automatic responses** based on the type and severity of an alert (e.g., ransomware alerts can lock a user account or unmount a file share)
- **Uncover and auto-quarantine sensitive files** that spill into unapproved locations
- **Automate access control approval workflows and entitlement reviews** to enforce a least privilege / Zero Trust model
- **Enforce data security and privacy policies with automated rules** that report policy violations and revert them instantly

VARONIS

Conclusion

As the cybersecurity landscape changes, traditional defenses are no longer enough. New approaches to cybersecurity, like Forrester's Zero Trust strategy, are a necessary evolution.

Zero Trust was designed to help organizations navigate the data- and identity-centric security strategies that are necessary in today's digital business world. While not the only tenant of Zero Trust, data security is a fundamental aspect of the framework that can dramatically improve risk reduction and threat detection.

When starting a security program or evaluating how to strengthen it, evaluating the state of data security is a wise place to start. In today's hybrid world where perimeter security falls short, data security offers organizations another line of defense against cybercriminals.

Live Demo

Set up Varonis in your own environment.
Fast and hassle free.

info.varonis.com/demo

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 on premises and in the cloud: 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 insider threats and cyberattacks 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. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and, as of December 31, 2018, had approximately 6,600 customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.