Cybersecurity from the inside out

The new data-first approach to improve
data security and privacy

INTRODUCTION

They don’t want your devices. They want your data.

When asked why he robbed banks, Willie Sutton famously replied “Because that’s where the money is.” You can’t fault his logic. Willie only wanted to get at what was valuable—the money—wherever it was.

These days, cyber-criminals and bad actors operate with Sutton’s singular focus on the essential: the data—no matter where it is. After all, data has now surpassed oil as the most valuable commodity on the planet; to protect their data, most companies start by securing endpoint devices and their network perimeter.

But there’s a fatal flaw in that thinking.

Devices are the front door to the data—they can always (and, sadly, will always) be defeated. Given the proliferation of connected devices and the disappearing security perimeter, the new threat landscape is immense and ever-changing. It’s predicted that there will be four connected devices for every person by 2020. With each of those devices a potential entry-point to your data, security professionals agree that breaches will happen.

Once inside the network, hackers have access to mountains of critical data—even without escalating privileges. Because companies don’t typically monitor their data for abnormal access, hackers can exfiltrate data undetected, harvest and steal user credentials, and drop ransomware and other types of stealth, persistent malware onto critical systems without sounding an alarm.

While it’s important to secure devices, security teams need to think about the data first. That’s what we’ll talk about in this e-book: how Varonis has flipped security thinking to better protect what hackers are after: the data.

The internal threat—The hazards of transparency

You start a new job and, to get up to speed, you explore SharePoint and Teams for information you might need on the job. Before long, you find yourself—a brand new employee—browsing folders and files full of critical and often confidential company data.

This is not an uncommon experience. Guess how many files the average employee has access to:

Answer: 17 million.

On average, about 1 in 5 folders are exposed or accessible to every single employee.[1] The attack surface for either malicious external, or inadvertent internal breaches in this environment is vast. So how do you stop them?

[1] https://www.varonis.com/2019-data-risk-report/

Protection from the inside out

Here are some quick best practices to protect your data from access overload:

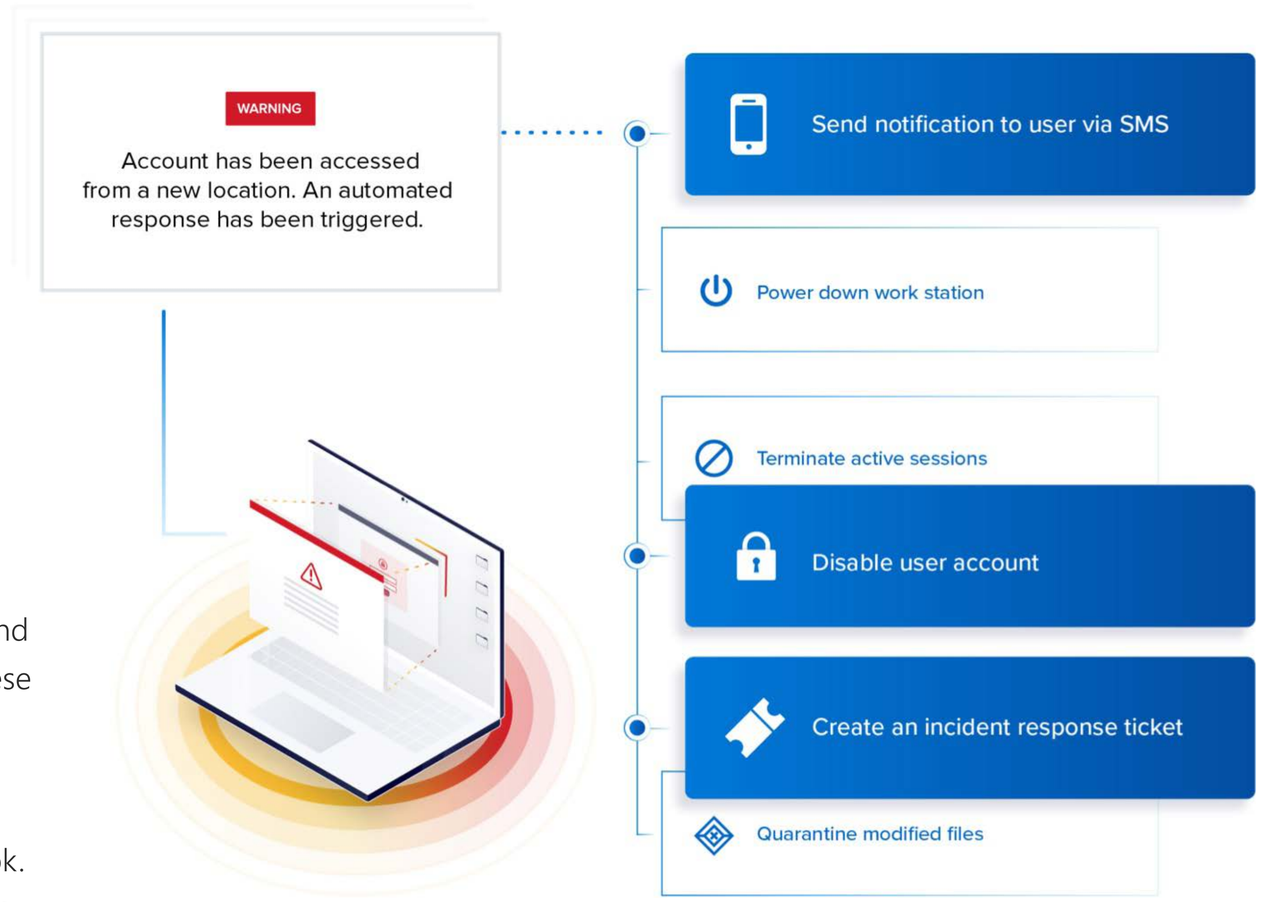
1. **Identify and remediate global access groups** that grant excessive access to critical data
2. **Ensure that only appropriate users retain access** to sensitive, regulated data
3. **Routinely run a full audit of your servers**, looking for any data containers (folders, mailboxes, SharePoint sites, etc.) with global access groups applied to their ACLs
4. **Replace global access groups** with tightly managed security groups
5. **Start with the most sensitive data** and test changes to ensure issues do not arise

External threats.
Don’t think walls.
Think motion detectors.

Bad actors will get in; and you’ve got to have defenses inside when they do. The average security breach worldwide costs over $3 million, and in the US, it’s over $7 million. Why is that? Because once inside, they can take their sweet time stealing data and wreaking havoc. On average bad actors have 196 days between getting in and being identified as a threat.

One of the quietest and easiest ways to get in and move around, are often user and service accounts that are inactive and enabled. These are called “ghost users”. These ghost users can lie dormant, going unnoticed day to day, yet still provide hackers access to your systems and data.

Hunting and eliminating ghost users is a security step organizations often overlook. If these accounts are left unmonitored, attackers can steal data or cause disruption without being detected—placing your organization at risk. It’s essential to be able to detect when one of these ghost accounts starts accessing critical data.



The barriers to data-first protection

Given that bad actors, malicious insiders, or simply careless behavior can result in breaches through any number of vectors, why not focus on protecting the data? It's not as simple as flipping a switch. Organizations face an array of challenges to securing their data, including:

Lack of a comprehensive understanding of access. This includes basics like establishing which data is sensitive, regulated, active or stale. You'll also want to know who has access to data across all your important data stores and whether they actually need it for work purposes. Sometimes employee functions, roles, or projects change and their permissions roll forward unnecessarily. You'll need visibility into that as well.

Granular and comprehensive permissions visibility can be difficult to manually analyze on a large scale. Varonis automates the process, giving you a way to visualize, prioritize, and reduce exposure.

Inability to identify and limit access to sensitive data. With many organizations migrating to cloud, multi-cloud, and hybrid-cloud systems, finding and securing sensitive data has become more complex. Even if administrators can locate sensitive data, they often lack the ability to roll back permissions in an efficient manner without generating complaints from business users.[2] To accomplish all this often requires cumbersome workflows for systems and personnel to keep up with everchanging permissions and security landscapes. And that can be expensive, especially when you consider the costs to purchase and maintain software to achieve it all.

Limited visibility of security incidents when they happen. Security analysts often rely on end users to alert them to issues. When they don't, malware can run undetected for several hours, days, or months. Given that so many sensitive files are open to anyone, this is open season for hackers. Then, after the fact, security teams will have a hard time figuring out which data was exposed and taking necessary steps. The most important question, "Is our data safe?" often goes unanswered without a searchable audit trail of data activity.

Finally, multiple point solutions that require management and coordination. Currently, organizations lack an integrated solution to handle multiple scenarios leaving vulnerabilities.

If you take a step back, all of these challenges can be overcome. Let's talk about how to do that.

[2] Forrester: The Total Economic Impact™ Of The Varonis Data Security Platform, 2018

What’s needed to overcome the challenges

Varonis has developed an approach and solution to each of these challenges with a data-first strategy. As you’re considering any security solution for on-premises, cloud, or hybrid data, make sure it delivers on these critical elements the way Varonis solutions do:

Comprehensive threat detection

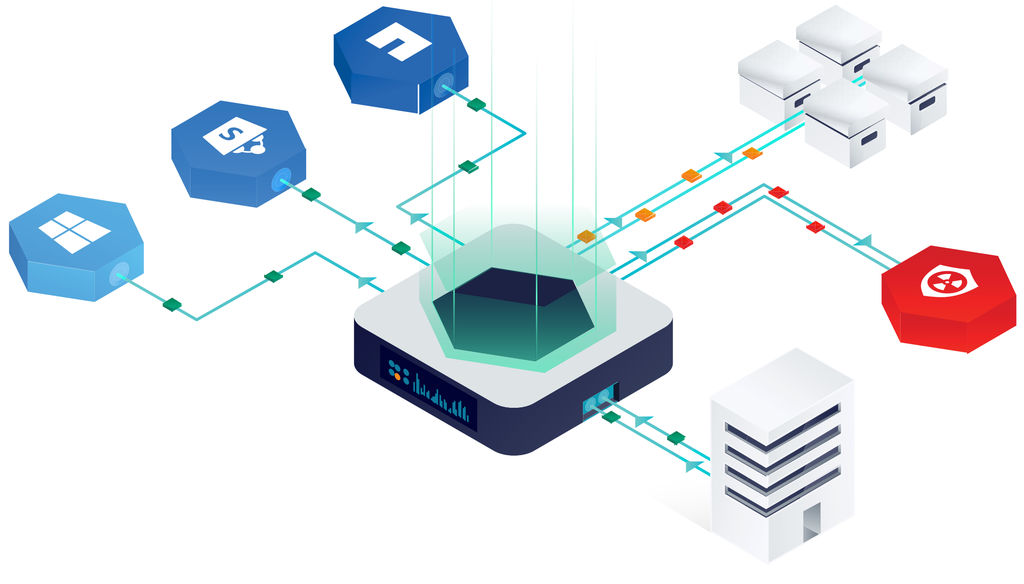
By combining visibility and context from both cloud and on-prem infrastructure, Varonis customers get 90% reduction in incident response times, out-of-the-box threat models for the entire kill chain, and the top-reviewed UEBA solution on Gartner Peer Insights.

Increased IT productivity

No organization, no matter how large, has resources to waste on doing labor-intensive tasks that could be done automatically. Varonis uses behavior-based automation to intelligently remediate risk on a massive scale without disrupting anyone. We recommend you only consider solutions that automate manual tasks like authorization, attestations, data migration, and disposition.

True Integrated multi-cloud abilities

Whatever solution you choose, you must be confident that it helps you identify and locate the most valuable data whether it is on-premises or in the cloud. That’s what the cyber-Willie Suttons will be after. To do that, your security solution must provide integration of multiple inputs from file activity, emails, directory services, DNS, VPN, and more to correlate user behaviors on each account, including file system permissions, AD structure, data classification and access activity.



A better solution—for security and productivity.

What have organizations found when they've implemented a data-first approach with Varonis?

A drastic reduction in risk associated with a data breach

With the help of Varonis solutions, it's possible to automatically remediate and protect millions of files without significant staff time impacts. One large U.S. insurance company recently used the Varonis Automation Engine to remediate 3 million globally exposed folders in just two weeks time—a project they estimated would take years to complete.

Improved security workflows

Varonis helps keep risk low by automating thousands of manual tasks. Access requests are routed to the proper stakeholders based on workflows you define, automatically granting access on approval without relying on IT intervention.

Smarter, more efficient retention and archiving

When retention and archiving is more streamlined, it allows organizations to better identify stale data and choose to retain or archive it based on business needs. Varonis makes it easy to create custom rules to move, tag, archive, or delete data based on content type, age, access activity, and more. Varonis also helps legal and compliance teams automate data subject access requests required by many privacy laws.

The numbers on data-first security

(Spoiler alert: It pays off.)

Forrester Research conducted a Total Economic Impact study on Varonis' data-first approach and found it not only effective, but a smart financial choice.

Time savings and cost avoidance on Remediation and permissions management: 4.5 hours per server folder

Reduced risk profile exposure: 65%

Total Return on Investment: 346%

Payback time: Less than 6 months

CASE STUDY

Landing a more secure solution

Situation

When a top U.S. airline adopted Varonis, they needed a solution that would help them protect their data and monitor all of their on-premises file servers.

Challenge

The main problem was that file shares would often be modified and no one would know who had done it. No one could see who was changing sensitive files or where they were located. Each time the team was blindsided by surprise alterations.

As the company continued to grow, senior leaders had also decided to switch from on-premises storage to the Microsoft Office 365 cloud in order to facilitate collaboration and protect sensitive data.

They had no way of knowing how much sensitive data was unsecured. This is a serious problem—especially in a highly regulated industry like aerospace. If they'd run afoul of a security breach and were found to be noncompliant, they could have faced fines of up to $100,000 every month.

Solution

The first thing the airline did was use Varonis DatAdvantage and Data Classification Engine to clean up data in their physical servers. It automatically catalogs all user accounts, group memberships, and their permissions to data and resources. It also tracks account activity, allowing monitoring and immediate response whenever someone accesses or modifies sensitive files. Wherever it resides—on-premises, in file shares, NAS devices, SharePoint, or Office 365—the Varonis solution scans and classifies all sensitive and regulated information.

Results

- Confidence to make the transition to OneDrive (down to 10 on-premises servers)
- Increased file integrity and data security onsite and in the cloud
- Insights needed to prepare for stricter compliance regulations (CCPA)

Fight threats on your terms

Don’t fight the cybersecurity battle on the hacker’s playing field. Move it to yours with the help of Varonis and Microsoft. Together, we’re relentlessly focused on protecting your most critical data first, not last.

CHANGE THE EQUATION

VARONIS

Microsoft 365