VARONIS

How Varonis Helps HomeServe Secure the Sensitive Data on Millions of Customers

“Don’t just think of Varonis as time-saving; think of it as risk-reducing. It finds problems you otherwise wouldn’t even know existed.”

Matthew Mudry,
VP AND GLOBAL HEAD OF CYBERSECURITY, HOMESERVE

CASE STUDY

HomeServe

HomeServe has a simple mission: to free people from the worry and inconvenience of home emergency repairs. Since 2003, they've been doing just that.

HIGHLIGHTS

CHALLENGES

- Coping with a massive spike in VPN usage during COVID-19
- Ensuring sensitive customer data remains secure while employees work from home
- Increasing perimeter awareness to detect signs of attack on the network, including the VPN

SOLUTION

The most robust data security platform:

- **DatAdvantage** to audit every file touch both on-prem and in Active Directory
- **Data Classification Engine** to identify sensitive data
- **Data Classification Policy Pack** to identify and classify sensitive CCPA data
- **Data Transport Engine** to automate data migration and help enforce data privacy regulations, including CCPA
- **DatAlert Suite** for fast threat detection and response
- **Edge** to monitor and secure the huge spike in users logging in through the VPN

RESULTS

- Data protection for millions of customers
- Actionable insight into at-risk areas that can be proactively addressed
- Unprecedented visibility into Active Directory and VPN activity

Challenges

Protecting employee and customer data during COVID

As a precaution under COVID-19, HomeServe, like many companies, rapidly transitioned to a mostly remote workforce. With over 2,000 employees in North America, this resulted in a massive spike in VPN usage.

For Matthew Mudry, Vice President and Global Head of Cybersecurity, this presented a logistical challenge: how do you protect your employees' and, in turn, your customers' information with so many people working remotely?

He knew it would be impossible without full transparency into who was connecting to the VPN and from where. He also needed visibility into sensitive data—no matter where it lived.

> "In addition to understanding who is connecting to our VPN and from where, we need to be aware of where our PCI and PII (or sensitive data) lives so it can be protected—especially if it shows up in an unexpected location," Matthew says.

Fortunately, he had a solution. Since 2019, Varonis has provided HomeServe with unparalleled alerting and visibility into its data stores. It helps them maintain least privilege and streamline basic regulatory needs, like maintaining PCI compliance.

Now Varonis was going to help protect their remote workforce. With Edge, HomeServe would gain real-time awareness into their top remote work risks and even the subtlest compromise indicators.

> “Varonis gives us transparency around VPN activity. With it, we can monitor who’s connecting or attempting to connect to our network at certain times and correlate that information to events taking place on our network,” Matthew explains.

Determined to do everything in its power to keep networks and customers as secure as possible, HomeServe also began rolling out **DatAdvantage for Directory Services**, to gain a single, unified audit trail of activity in Active Directory.

> “In addition to understanding who is connecting to our VPN and from where, we need to be aware of where our PCI and PII (or sensitive data) lives so it can be protected—especially if it shows up in an unexpected location.”

Solution

Varonis had a clear vision to solve the problem

The first solutions HomeServe rolled out were designed to give them more control over their on-premises environments.

DatAdvantage for Windows enables them to audit every single file touch and monitor permissions. It also helps them execute a retention schedule by identifying stale data that's long past its retention requirements and safe for removal.

> "We brought in Varonis to help us understand who the last person is to touch data, so we can paint a picture of what data can truly be deleted without negatively impacting the business," Matthew says.

Data Classification Engine looks inside files to identify sensitive data that's at risk. Together with **Data Classification Policy Pack**, Matthew is able to easily discover and secure at-risk CCPA data.

If anything's out of place, **Data Transport Engine** automatically archives, quarantines, or deletes data based on predefined rules, without compromising existing permissions structures.

> "Varonis not only helps us identify sensitive data but it takes it a step further, showing us where it lives and who has access to those files. From there, we can easily isolate it, quarantine it, or just execute an alert to protect the data," Matthew explains.

When Varonis detects a potential problem, DatAlert Suite provides advanced threat detection and response so that Matthew and his team can quickly assess possible issues and take remedial action.

> “We had a penetration test recently and Varonis was the first alarm that went off. That real-time alerting is essential,” Matthew says.

These solutions laid the foundation for protecting HomeServe’s newly mobilized remote workforce. Security Analyst Jeremy Diaz worked closely with the Varonis Incident Response (IR) team to set up alerts and get them up and running with **DatAdvantage for Directory Services** and **Edge**.

> “From my perspective, it’s a lifesaver knowing that I can get security alert notifications about my data in real time. Varonis is always on,” Jeremy says.

By combining knowledge of Active Directory, file server activity, and perimeter telemetry, Varonis can detect threats to Active Directory long before they become full-blown data breaches. It’s the key to the entire kingdom, and maintaining its security is paramount.

“We had a penetration test recently and Varonis was the first alarm that went off. That real-time alerting is essential.”

Results

Data protection for millions of customers

Varonis enabled HomeServe to mobilize its remote workforce with confidence. Active Directory transparency, advanced perimeter telemetry, and alerting on their VPN allows Matthew to rest easy because they’re doing everything they can to keep employee and customer data secure.

With Varonis, he is always finding small things to improve and potential security risks to address. But he’d rather be armed with knowledge than fall victim to a bad actor.

> He says, “Don’t just think of Varonis as time-saving; think of it as risk-reducing. It finds problems you otherwise wouldn’t even know existed.”

> “Tackling data protection at scale is hard. But it’s comforting that I know where my problem is and it’s not a needle in a haystack. Having that visibility with a click is mind-blowing,” Jeremy agrees.

DatAdvantage for Directory Services provides Matthew and team with visibility into the Active Directory space. This visibility makes it possible or them to track VPN activity—and resolve issues before they could escalate.

> Matthew says, “Before Varonis, we were using another tool that provided limited visibility into our Active Directory environment. Now we have actionable and intelligent information that allows us to quickly identify and respond to things such as misused service accounts, inactive domain accounts, and changes to sensitive and protected Active Directory groups.”

With Varonis, Matthew can follow a clear audit trail to track and—if necessary—undo changes to Active Directory. He can see who logs into the VPN and where they’re logged in from. He’s already used this insight to shore up potential risks to HomeServe’s data security.

> “We have the capability to dive in and see the thousands of people connecting to our VPN and identify those who are not. This is important because it allows us to figure out why they’re not connecting, solve their issue, and ensure that they’re getting the necessary updates and patches,” Matthew says.

> “It’s comforting that I know where my problem is and it’s not a needle in a haystack. Having that visibility with a click is mind-blowing.”

VARONIS

How you work is evolving. Is your data security keeping up?

Get data protection, threat detection, and compliance that fits the way you work.

REQUEST A DEMO