VARONIS

How a Major U.S. Energy Provider Uses Varonis as the Heart of their Security Operations Center

> Most solutions focus on threat prevention. But detection, prevention, and investigation are all interrelated. No other solution does all three as well as Varonis.

About this case study:

Our client is a respected U.S. energy provider. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

Challenges

- Protecting sensitive user data from the rising threat of cyberattacks and data breaches
- Building out a SOC for proactive threat detection and response
- Finding a solution that continues to evolve and grow with their company

Solution

The Varonis' cloud-native Data Security Platform:

- Provides visibility and control across all enterprise data in M365 and Windows
- Proactively reduces sensitive data exposure
- Offers real-time behavior-based alerts on potential threats

Results

- Data security both in the cloud and on-prem
- Detailed alerts for everything from ransomware to anomalous file access
- Numerous potential threats detected and eliminated since adopting Varonis

CHALLENGES

Protecting user data from malicious insiders and external threats

Data breaches and cyberattacks affect billions of people every year. In 2017, wormable ransomware like Petya, NotPetya, and Wannacry wreaked havoc on a global scale. And more than 2.3 billion records were leaked in July 2019 alone.

To combat the rising threat, many businesses have onsite SOCs, which act as security "nerve centers" allowing security teams to monitor various parts of the network for threats and suspicious activities.

As one security engineer for a major U.S. energy provider (who requested anonymity) says:

> **"The truth is that a security threat either has happened or will happen to almost every company — be it a malicious insider with too much access or a bad actor infiltrating your network."**
>
> **"We recognize this, which is why we value the ability to catch them in the act and to tell a story after the fact about exactly what they touched or changed when a tripwire goes off."**

This energy provider has built out an onsite SOC to protect its users, and at its heart is Varonis. This company has been a Varonis' customer since 2007 and it understands the importance of threat detection, data security, and user privacy.

According to the security engineer:

> **"We have important things that need to be protected. First and foremost: we represent the power grid for a huge part of the U.S., so we need to keep that secure. We also want our end users to know that we're thinking about them and protecting their data."**

"The truth is that a security threat either has happened or will happen to almost every company — be it a malicious insider with too much access or a bad actor infiltrating your network."

SOLUTION

Security operations center with Varonis at its center

The energy provider adopted Varonis in 2014. Since then, Varonis has become pivotal to their threat detection and response program. The Varonis dashboard is the centerpiece of their SOC and it enables their security group to monitor their network for threats and anomalies.

According to the security engineer:

> **"We leverage around 25–30 Varonis threat models. Some of the models are native and others are exceptionally focused. We have specific alerts that go off if we detect any sign of ransomware, like Petya, NotPetya, and WannaCry."**

They also have alerts set up specifically to monitor user data, which warns them whenever someone accesses sensitive information. Data protection has been the main reason behind each of their purchases.

> **"We want end users to know that we're thinking about them and their data. We get alerts whenever there's suspicious activity in our environment, such as a user accessing a protected file."**

When Varonis directs them to a potential problem, the customer uses the Data Security Platform enables them to understand the full extent of the threat. With these solutions, they're able to follow a comprehensive audit trail, analyze every file touched, and know whether or not the files contain sensitive information.

> **"Most solutions focus on threat prevention. But detection, prevention, and investigation are all interrelated. No other solution does all three as well as Varonis."**

> **"We have found things that were anomalous and we have used Varonis on a number of occasions to tell the story of what this person accessed or that person changed."**

Senior leaders at this company have also found ingenious new ways to use Varonis. For example, they've been using Varonis' analytics to understand the roles and responsibilities of the people working under them.

> **"By using Varonis to understand what files various roles need to access to do their jobs, managers can help their employees — and ensure future employees who might eventually fill that role have access to everything they need from day one."**

"We leverage around 25–30 Varonis threat models. We have specific alerts that go off if we detect any sign of ransomware, like Petya, NotPetya, and WannaCry."

RESULTS

Data-centric security in the cloud and on-prem

The company is scaling data out to the cloud in a controlled fashion. To ensure that their data is protected, the energy company relies on Varonis to provide:

+ Support for their Microsoft 365 environments as well as their on-premises servers, giving them more visibility and control into data access.
+ Help for controlling and keeping track of sensitive data, including who has access to it.

> **"Varonis was already providing value to our on-premises security. We knew we needed to match that level of security in the cloud too."**

With Varonis, the industry leader gained visibility and control over where their sensitive data lives, who can access it, and how it's used. With Varonis, the CISO's team has the visibility and support they need. And they know the Varonis team is available to support them on that journey.

> **"Varonis listens to what their users want. They make earnest efforts to incorporate features that make sense for the solution, and year after year they actively work to make their tool the best solution on the market."**

These ongoing innovations combined with Varonis' commitment to its customers are the two things this security engineer loves most about the platform.

> **"Varonis' customer service is unbelievable. I have never experienced support this good from any other vendor. They have a strong desire to help you use the product to the best of its ability in a way that meets all of your requirements."**

With Varonis at the heart of their SOC, this energy provider is confident their sensitive data is secure and their network is defended from cyberattacks and insider actions alike.

Your Data. Our Mission.

Secure sensitive data, find and eliminate risks, and boost compliance with Varonis.

Request a demo