VARONIS

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

CASE STUDY

"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 Security Operations Center (SOC) for proactive threat detection and response
- Finding a solution that continues to evolve and grow with their company

SOLUTION

The most robust data security platform:

- **DatAdvantage for Windows, OneDrive and SharePoint Online**
- **DatAlert as the pivotal solution in their SOC**
- **Data Classification Engine for Windows and SharePoint**

RESULTS

- Data security both on-premises and in the cloud as they scale out to OneDrive
- Detailed alerts for everything from ransomware to anomalous file access
- Numerous potential threats detected and eliminated since adopting Varonis in 2007

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.

Small wonder that data privacy and protection is front of mind for most companies. To combat the rising threat, many businesses have onsite Security Operations Centers (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 of the matter 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 DatAlert. This company has been a Varonis' customer since 2007 and it understands the importance of threat detection, data security, and user privacy.

> "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 of the matter 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 DATALERT AT ITS CENTER

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

> “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 DatAlert directs them to a potential problem, DatAdvantage for Windows, SharePoint, and OneDrive 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. Recently, for example, they've been using DatAlert 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 ON-PREMISES AND IN THE CLOUD

The company is now in the process of scaling data out to the cloud in a controlled fashion. To ensure that their data is protected, they've added two solutions to their lineup of Varonis' products:

DatAdvantage	Support for their cloud-based SharePoint and Office 365 environments as well as their on-premises servers, giving them more visibility and control into data access.
Data Classification Engine	Helps them control and keep 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."

The company also recently upgraded to Version 7.0. This upgrade features advanced threat detection and response capabilities, new dashboards for at-a-glance visibility, and even more cloud support, including additional context for alerts and investigations.

> "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.

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

VARONIS

Advanced threat detection, prevention, and investigation—all under one roof.

Protect sensitive data, find and eliminate risks, and meet compliance regulations with the help of Varonis.

REQUEST A DEMO