How Varonis Helps an Energy Company Safeguard Critical Data in AWS and M365

> “We have a consolidated file system in AWS that has years and years of data. We manage and protect our data across the AWS ecosphere with Varonis.”

About this case study:

Our customer is a leading company in the energy sector that considers Varonis to be a critical piece of their security stack. We have happily accommodated their request for anonymity.

HIGHLIGHTS

Challenges

- Securing data in M365 and AWS
- Addressing high-risk areas in the cloud, email and S3
- Following industry best practices and ensuring compliance with numerous privacy regulations

Solution

The Varonis cloud-native Data Security Platform:

- Automatically discovers and classifies sensitive data
- Audits and remediates access to sensitive data
- Detects and alerts on anomalous activity in real time

Results

- Saved thousands of hours with automation
- Locked down AWS S3 buckets
- Alerted to unusual logins from the CEO for validation
- Cleaned up years of data from disparate file systems and acquisitions into AWS
- Demonstrated compliance with SEC reporting requirements in the U.S. and the GDPR in the EU
- Remain over 85% compliant with the NIST CSF 2.0 standard with automation

CHALLENGES

Data security for M365 and AWS

An energy sector company has a long and successful history of using technology to enhance its operations.

Recently, the company optimized its IT infrastructure by adopting a cloud-first approach. As part of its digital transformation, the company needed to clean up user permissions and stale data and safeguard its critical data from attacks.

According to the CIO:

> **"Our AWS cloud hosts all file servers and systems. Everything is in the cloud. We needed a solution that would address our high-risk areas—our cloud files and servers, email, and S3."**

The energy company's lean IT and security team is responsible for ensuring the security of vast amounts of cloud data for the global enterprise. They needed a solution that could provide the same capabilities across their infrastructure with little management.

The CIO and the CISO sought a solution that could secure their cloud data, help them comply with international standards, and detect and mitigate threats in real time.

The energy company chose Varonis.

SOLUTION

Gaining control of their AWS environment

The Varonis Data Security Platform enables the energy company's IT and security team to secure sensitive data, clean-up permissions, and watch for threats and unusual activity across AWS, Microsoft 365, and Active Directory—all while enabling and executing their cloud-first technology strategy.

The energy company benefits from the capabilities the Varonis Data Security Platform provides while also receiving top-notch expert support.

And the CIO appreciates Varonis' ongoing commitment to ensuring the team gets the most the platform has to offer:

> **"We didn't just want to buy a tool. Varonis makes sure their clients are using the product, which we really like because we have a smaller IT team. The combination of Varonis' team and our team make it work."**

Locking down AWS S3 buckets

Cloud misconfigurations can make sensitive files accessible to unauthorized users and even publicly on the internet. Misconfigured AWS S3 buckets have exposed massive amounts of sensitive data like PHI and PII on millions of individuals at many organizations.

The energy company wanted to ensure they were not the next company to inadvertently expose critical data. According to the CISO:

> **"S3 buckets are a known target in the hacker world because AWS is so prevalent. S3 buckets are exploited all the time."**

Varonis scans the energy company's AWS environment to automatically discover and classify sensitive data in their cloud environment. The platform flags where AWS data is at risk through excessive access and misconfigurations. Varonis also actively identifies and alerts on suspicious activity around data and access.

> **"We have a consolidated file system in AWS that has years and years of data. We manage and protect our data across the AWS ecosphere with Varonis."**

Following best practices and ensuring compliance

The energy company sought to adopt the NIST Cybersecurity Framework 2.0 with a focus on governance. The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should focus on just like they would finance and reputation.

According to the CISO:

> **"We follow the NIST CSF 2.0 standard. Our automation process allows us to stay within these national standards and keep us compliant. We can continuously stay over 85% compliant with Varonis' automation processes."**

Varonis helps the energy company demonstrate compliance with international regulations in the many countries it operates, including SEC reporting requirements in the U.S. and the GDPR in the EU.

The CISO explained:

> **"Cybersecurity is critical, because now, if there's an incident you must respond in hours based on the latest SEC Rulings. We have thousands of employees around the world. Varonis is actively monitoring our environment, giving us real-time intel and closing security gaps for us. Varonis is a huge time saver and helps us reduce our risk tremendously."**

RESULTS

Detecting and alerting on anomalous activity in real time

Varonis connects the dots between sensitive data, permissions, and activity, watching for anything out of the ordinary that could indicate early signs of an attack. With Varonis, the energy company actively monitors its cloud environment and receives real-time alerts on unusual activity.

According to the CISO:

> **"Varonis captured unusual logins from our CEO and one of our board members in places where they're normally not present. Varonis alerted us immediately, and we were able to validate whether it was legitimate. Alerting to unusual logins was something we never had before Varonis."**

Improving data security posture

Varonis helped the energy company clean up years of data from disparate file systems and multiple acquisitions and consolidate them into AWS. Varonis enabled the customer to remove inactive and stale users and unused files from their environment.

According to the CIO, Varonis was pivotal in clearing their environment of this clutter:

> **"Hackers love clutter. Varonis helped identify where the clutter was in our systems in AWS and Entra ID (formerly called Azure AD). It's one thing to say you want to get rid of clutter. It's another thing to identify it so that you can actually get rid of it. Varonis has really helped us become very organized with our cloud data."**

Saving thousands of hours with automation

Data continues to grow, users change roles and leave, and new threats emerge constantly. That's why organizations like the global energy company sees Varonis' automated remediationas critical to maintaining their strong data security posture.

Varonis' automation works in the background, continuously helping the energy company reduce risk and monitor for threats to its data. Varonis frees IT and security team members from manual and time-consuming security processes so they can focus on other work.

According to the CISO:

> **"Varonis' automation is really a game changer for us. The automation Varonis offers has saved us thousands and thousands of hours. Varonis has made us scalable because we don't have to throw manpower at problems. We also eliminated human error that comes with those manual processes."**

With Varonis, the IT and security team sees where all the data in their environment is, knows who has access to it, and what they do with that access, all in one place. Varonis also provides the CISO and CIO with reports showing that the organization has resolved thousands of anomalies in its cloud environment and reduced that number to zero.

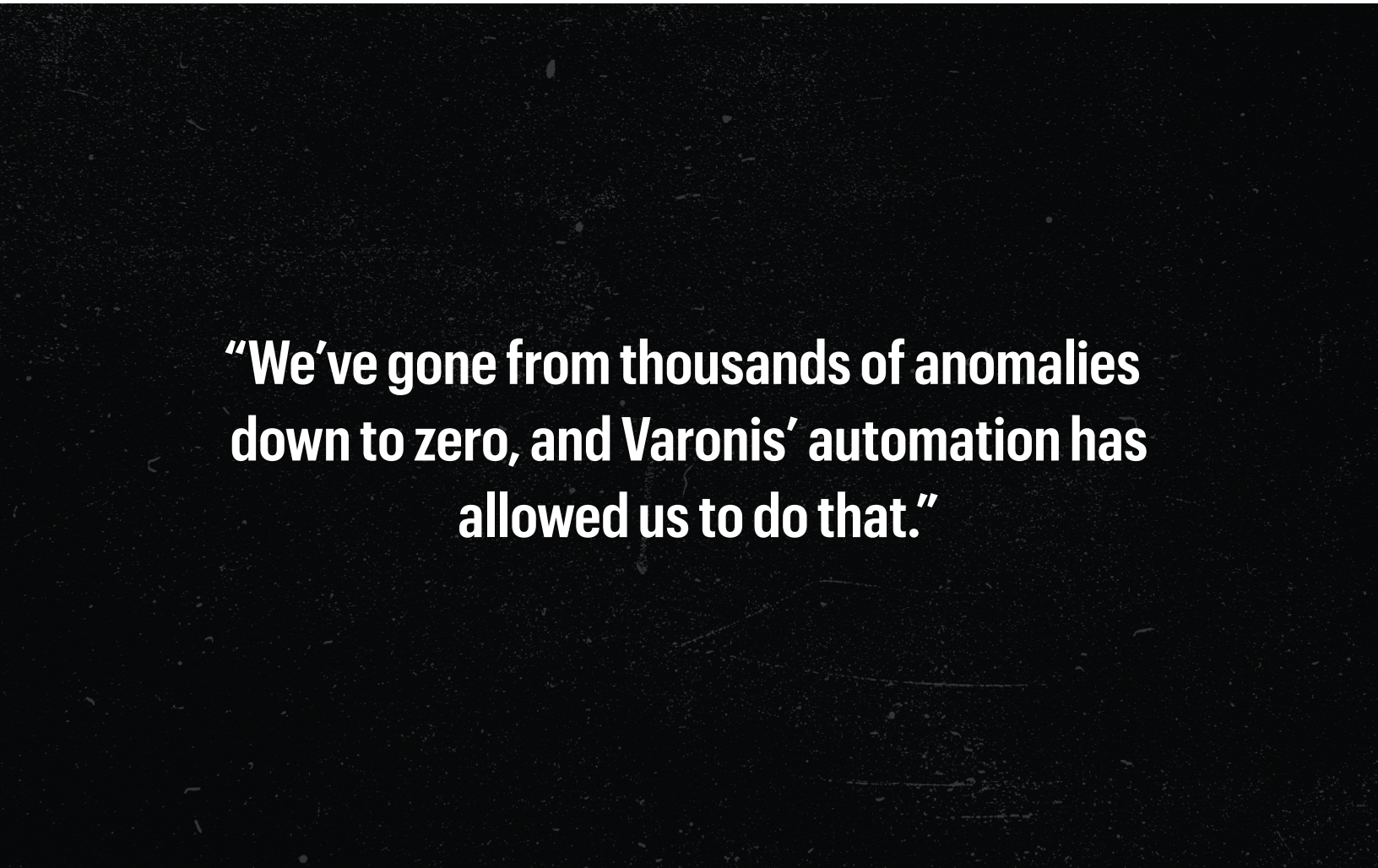
According to the CISO:

> **"With Varonis, we can focus on reporting and analysis. Security is a continuous process. We've gone from thousands of anomalies down to zero, and Varonis' automation has allowed us to do that."**

Demonstrable ROI

With Varonis, the IT and security team can easily gather hard data that demonstrates real outcomes of their cybersecurity investment. The CIO says they can confidently present to the board of directors that the company is following industry best practices for data governance and embracing automation—all while gaining complete visibility into their data estate:

> **"We have an active board concerned about cybersecurity. I present to them each quarter and show how our security posture is maintained with Varonis. We are demonstrating to our executive team that we take cybersecurity seriously, and Varonis is helping do that."**



Your Data. Our Mission.

Varonis provides a unified view of your data across cloud and hybrid environments, with unmatched automation to reduce risk.

Request a demo