How a Resort and Convention Center Operator Reduced Security Alerts by 99.9% and Guards Against Ransomware

CASE STUDY

"When data changes, we know instantly. If ransomware starts to encrypt our data, we see that change in real time. We can dig into the alert to see who owns it. We can make a correlation between the attack and the point of entry. Varonis' monitoring and alerting on file activity is a big plus."

ABOUT THIS CASE STUDY:

Our client is a resort and convention center operator. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Keeping up with 4.5 million events/day was impossible for a small security team
- Protecting PCI and guarding against insider threats was difficult with so much 'noise'
- Cobbling together a security solution from multiple software tools created new vulnerabilities

SOLUTION

Varonis Data Security Platform:

- **DatAdvantage** maps data access activity in Windows and Directory Services
- **Data Classification Engine** finds and classifies sensitive data
- **Policy Pack** enhances Data Classification Engine with CCPA and GDPR patterns
- **DatAlert** monitors and alerts on critical systems
- **Data Transport Engine** to quickly and safely migrate large amounts of data
- **Edge** detects and helps prevent DNS exfiltration attempts

RESULTS

- Averaging 8 security events per day, down from 4.5 million
- Gaining 'incalculable' time savings to focus on other critical tasks
- Safeguarding customer data (and, consequently, brand reputation)

Challenges

Sorting through SIEM 'noise' to isolate potential threats

"I have a million things on my plate," explains the CISO of a resort and convention center operator (anonymous by request).

The company employs U.S. citizens and staff from countries within the EU to support multiple locations across the United States. As such, the company needs to comply with data privacy regulations, including CCPA and GDPR. It's the CISO's job to ensure that compliance rules are met and sensitive customer data—like PCI—is kept safe.

But when the CISO first joined the team, that wasn't easy.

> "When I got here, we had no idea what data we had, where we were keeping it or what sensitive information it contained."

The problem stemmed from a defense stack cobbled together from multiple software solutions.

While the CISO was able to monitor Active Directory for security events, their SIEM system recorded approximately 4.5 million events every day.

With so much 'noise,' it was impossible to keep track of the alerts that might indicate a major security incident. And performing tasks like permissions clean up could take hours or even days.

> “I was spending way too much time looking at the security posture of each individual system. Performing manual audits and reviewing things like permissions sets in Active Directory took a lot of time.”

The CISO was especially concerned by the possibility that being distracted by so much noise might allow malware, ransomware, and malicious insiders to slip by unnoticed.

Hospitality is quickly becoming one of the most-targeted industries, as cybercriminals seek to exfiltrate sensitive data, including PCI and other customer information.

The CISO couldn’t afford to risk the safety of the resort’s visitors.

> “Ransomware keeps me up at night, because I’ve seen it affect other organizations. I don’t want a bad actor to get into our environment and start wiping or locking our data.”

“Performing manual audits and reviewing things like permissions sets in Active Directory took a lot of time.”

Solution

Minimizing alerts that distract from actual security threats

A free Data Risk Assessment shed light on the organization's environment. Varonis reps demonstrated how easily problems could be resolved with products such as:

- **DatAdvantage for Windows and Directory Services,** which helps protect documents in the Microsoft Office suite and Active Directory by mapping who has access to what files.
- **Data Classification Engine** supported by **Policy Pack,** which finds and classifies sensitive data and recognizes data that's protected under regulations like CCPA and GDPR.
- **DatAlert,** which monitors critical systems for unusual behavior and alerts the CISO to the most relevant and potentially dangerous security events.
- **Data Transport Engine,** which makes data migration a breeze. It enables the CISO to quickly and safely move data across servers based on predefined rules.
- **Edge,** which leverages perimeter telemetry to help guard against sneaky data exfiltration attempts.

By adding all of these solutions to their lineup, the resort and convention center operator was able to replace several of their old software tools and streamline their existing security stack.

The CISO says the difference is "night and day":

> "Varonis gives me the ability to see things from a high level without having to dig too deep—but if I need to dig deeper, I can quickly and easily do that without spending days diving through different systems. It saves me a lot of time."

Before Varonis, everything related to data and data permissions used to be done manually. Provisioning, data clean up, rights analysis—everything had to be painstakingly completed by hand.

> "Varonis automated all of that so we didn't have to have people spending hours looking at it. If we didn't have Varonis, admittedly most of it would never be done at all. My team is too busy focusing on system operations and making sure guests are satisfied."

Most importantly, if security teams are buried in alerts and chasing ghosts, it's more likely that they'll miss the threats that matter. That's why Varonis' team worked closely alongside the CISO to fine-tune DatAlert.

> "Varonis' team worked with us to implement and align the solution with our needs. After implementation, it's been very easy to use. One person can effortlessly monitor activity and pinpoint what's going on. So it's a double win: amazing support, plus user-friendliness."

With DatAlert, the CISO has now eliminated **99.9% of the noise** in their environment.

> "Varonis gives me the ability to see things from a high level without having to dig too deep. It saves me a lot of time."

Results

Less time digging through alerts and chasing ghosts

The CISO used to be bombarded by millions of potential security events every day. With DatAlert, they now average **only eight alerts per day**—a significantly more manageable number.

> "SIEMs can be noisy. Varonis gives me a cleaner view of our alerts. The log event is still there for the record, but Varonis minimizes the noise so I get a better and more precise view of what's actually going on. And because Varonis is so granular, it lets me get a close look at what's happening in our environment."

For the CISO, this translates to time savings. Hours that used to be spent tracking down files can now be spent improving the company's overall security posture. Now that they're not manually combing through individual systems, they have time to focus on employee security awareness training.

> "Varonis has given me my time back. I used to spend hours on compliance-related tasks. Now I know that my data is where it needs to be. I can finally focus on the other things I need to focus on."

For the C-suite executives, Varonis quells the fear that bad actors might slip by their defenses and steal customer data unnoticed.

The hospitality sector has been increasingly hit by large data breaches, but this organization is staying one step ahead—and protecting their brand reputation in the process.

> “When data changes, we know instantly. If ransomware starts to encrypt our data, we see that change in real time. We can dig into the alert to see who owns it. We can make a correlation between the attack and the point of entry. Varonis’ monitoring and alerting on file activity is a big plus.”

Now the CISO has just one recommendation for other businesses in the hospitality sector:

> “Get the Data Risk Assessment. It gives you the depth of view to confirm where you’re at risk in your environment. It also gives you a visible, tangible asset to justify the solution to management, so you can say, ‘This is where we are… and this is where we need to be.’”

“Varonis has given me my time back. I used to spend hours on compliance-related tasks. Now I know that my data is where it needs to be.”

Get started with a free Data Risk Assessment.

Shine a light on unknown weak spots and pinpoint your biggest security vulnerabilities.

GET A CUSTOM RISK ASSESSMENT