VARONIS

How an NFL Team Prevents Ransomware and Protects PCI with Varonis

> We have everything set up the way we need to prevent large issues from happening from a security standpoint, a file standpoint, and a directory services standpoint. So we're really satisfied with Varonis.

About this case study:

Our customer is an NFL team. We have happily accommodated their request for anonymity.

Highlights

Challenges

- Proactively minimizing their ransomware blast radius
- Enforcing PCI compliance
- Gaining advanced threat detection and response

Solution

Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **DatAlert** monitors and alerts on abnormal behavior on critical systems
- **Edge** detects and helps prevent threats on the perimeter

Results

- Time savings for the IT team taking mitigative action
- Peace of mind thanks to advanced threat detection and alerting
- On-prem and cloud environments that are PCI compliant

Challenges

Threat detection and PCI compliance issues

In 2013, a Major League Football (NFL) team faced a serious threat. An intern was using a company computer when it suddenly locked up. The IT team scrambled in response, but the ransomware had already started to spread.

> **"It crippled some of our file systems. But thankfully the files weren't important and we caught it quickly. Nobody got anything from us," says an IT admin, who requested anonymity.**

Even though the threat was quickly neutralized, the IT team didn't want to rely on good luck the next time they faced an attack. It was time to up the ante on their cybersecurity.

> **"After that, we definitely took a more proactive approach to ransomware. We chose Varonis because they're very active in the alerting space and we needed insight into potential threats that change daily. Varonis is always updating their dictionaries and threat reporting and they do a good job being proactive."**

VARONIS

But the NFL team didn't choose Varonis just for threat detection and response. They also needed to enforce Payment Card Industry (PCI) compliance—and they knew Varonis could help.

Pro sports teams collect credit card information in a variety of ways: ticket sales through online portals, marketing events, deals brokered between advertising agencies, and more.

Having visibility over PCI and locking it down is crucial. The NFL team's top executives wanted assurances that all sensitive data—and, by extension, the team's brand reputation—was safe.

> **"You never want to see potentially sensitive data leave the environment or used against us in any way, like given to a rival or brought to another company. We always want to prevent those things."**

"We chose Varonis because they're very active in the alerting space and we needed insight into potential threats that change daily. They do a good job being proactive."

Solution

Smart threat detection + compliance automation

Learning from the ransomware attack, the NFL team has since used the Varonis Data Security Platform to fortify their on-premises and cloud cybersecurity.

They use **DatAdvantage** for Windows, Directory Services, OneDrive, SharePoint Online, and Exchange to gain visibility into their environment, limit open access, and gain a clear forensic trail of who is accessing files and folders.

> **"The DatAdvantage GUI has gotten better with each new software release. It's super easy for me and other team members to look at alerts, analytics, and all the products we have on the left-hand pane. We can just click on each one to bring up a more granular dashboard. That's been fantastic."**

Data Classification Engine provides the next piece of the puzzle. It identifies sensitive data (such as PCI) stored in file shares, SharePoint, OneDrive, and SharePoint Online. Armed with this insight, the IT team can focus their remediation efforts on the most at-risk areas first.

> **"We use Varonis to scan our corporate file systems for Social Security Numbers, driver's licenses, credit card numbers, bank account routing numbers, and all of that PCI compliance data. When we find those files, we can ask the owner of the file to strip out the sensitive information, or we can monitor the file going forward if we give the owner time to clean it up."**

For threat detection and response, the NFL team adopted **DatAlert**. DatAlert uses behavioral analysis to alert on suspicious activity that may indicate a compromised account. Professional sports teams and the people who work with them travel a lot, so having this visibility is critical.

> **"We get alerts for a lot of different scenarios, such as warning signs if a computer has been compromised. Varonis also has what's called a 'watchlist,' and if you know someone is leaving the company you can put them on the watchlist to ensure that they don't suddenly copy a large amount of data."**

Finally, the company adopted Varonis **Edge**, which uses perimeter telemetry from VPN, DNS, and web proxies, to expand the detection window. When employees need to travel frequently, Edge helps ensure that their data is safe—even abroad.

With Edge hooked into their VPN, the IT team receives an alert whenever anyone uses their phone or personal device to log into a Microsoft 365 app. When Edge detects that they're logging in from another country, it issues an alert.

> **"It's a really good one for us, because we get a lot of logins from abroad. Sometimes we think a user is on-site and then their IP address pops up in another country. Then we can reach out to them and ask, 'Are you really in Kenya?' or 'Are you really in China?' It gives us peace of mind."**

"We use Varonis to scan our corporate file systems for Social Security Numbers, driver's licenses, credit card numbers, bank account routing information, and all of that PCI compliance data."

Results

Fortified security on prem and in Microsoft 365

Today, the IT team has proof in place that they have the ability to stop malicious activity across their hybrid environments. With Varonis, they rest easier knowing that sensitive PCI and personal identifiable information is being protected, even when employees are abroad.

> **"We know where our data lives. We can show that it's being monitored. It's a way to prove to upper management and executives that we have the tools in place to protect us."**

The benefits of Varonis for the IT team are threefold:

1. They have an early warning system when they're under attack, and the means to resolve issues quickly.
2. They have visibility that helps them focus remediation efforts and proactively remediate the most at-risk areas.
3. They have tools to help them lock down sensitive data quickly and decisively vs. a drawn-out manual process.

> **"It's been a lot more time-saving on my end. I don't need to deep-dive into all of the potential issues and dread fixing them when Varonis does it behind the scenes."**

As for the NFL team's owners and executives, Varonis provides peace of mind that their environment is secure and the company is PCI compliant.

> **"We have everything set up the way we need to prevent large issues from happening from a security standpoint, a file standpoint, and a directory services standpoint. So we're really satisfied with Varonis."**

“We know where our sensitive data lives. We can show that it’s being monitored. It’s a way to prove to upper management and executives that we have the tools in place to protect us.”

Gain airtight PCI compliance.

Varonis helps you pass annual compliance audits and lock down your environment.

Request a demo