How Varonis Helps a Global Law Firm Safeguard Sensitive Client Data

CASE STUDY

> "It's really about making quick decisions. With Varonis, I have everything I need within a half hour. Without Varonis, it would take me at least five times longer."

ABOUT THIS CASE STUDY:

Our client is a global law firm. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Meeting various compliance requirements for clients across different industries
- Understanding the big picture: who can and who does access data
- Finding and fixing security blind spots after a Purple Team exercise exfiltrated dummy data

SOLUTION

The most robust data security platform:

- **DatAdvantage** maps user access and provides an audit trail when sensitive files are moved or copied
- **DatAlert Suite** monitors and alerts on critical data and systems
- **Edge** detects signs of attack on the perimeter, including DNS exfiltration attempts

RESULTS

- Increased visibility into server and perimeter activity
- More mature incident response procedures to detect and stop DNS exfiltration attempts
- Enhanced data security to help meet even the strictest client compliance requirements

Challenges

Meeting client compliance requirements

Despite the fact that they were using leading solutions (Microsoft for DNS, Palo Alto for VPN and web proxy), a global law firm (anonymous by request) wasn't taking any chances with sensitive client data. As their information security director explains:

> “As a law firm, we have no direct regulatory oversight. What we do have are contractual obligations with our clients. If we have a client in financial services, our terms are written around their PCI requirements. If we have a client in healthcare, we need HIPAA compliance. Essentially, we're beholden to none but have to comply with all.”

To test the maturity of their security response procedures, the firm engaged Varonis to perform a **Purple Team exercise**.

Purple Teaming combines the focused penetration testing (“pentesting”) of Red Teaming with training and education for the Blue Team (i.e., ‘the defense’ led by a cybersecurity team) to improve incident response procedures. In other words, it tests their ability to cope with an “ethical hack” that simulates a real-world attack and coaches them on how to improve.

The goal of this exercise was to weed out vulnerabilities and find ways to improve incident response.

If a malicious insider or external attacker decided to access non-public information for inappropriate use (e.g., for stock market trading) or exfiltrate protected information disguised as normal web traffic, would their team be able to detect and prevent the threat using the tools in their existing security stack?

The Purple Team exercise was about to find out.

After staging dummy data on one of the law firm's servers, Varonis' Red Team attempted to sneak in, locate the dummy data, and exfiltrate it by exploiting a blind spot in the firm's security.

> "There's a recent and scary method that attackers use to steal data—DNS exfiltration. That's exactly what Varonis came in to test. We wanted to see if they could exfiltrate our data through our DNS."

The only solutions in the firm's technology stack that even detected the attack—and let the Blue Team know they had a problem—was Varonis.

The test results were grim. For the first time, the information security director had a clear view of the firm's vulnerabilities. Something had to change—and it had to change quickly.

> "We thought we were safe—right up until someone came in and demonstrated we were wrong. It was time to take action."

“There’s a recent and scary method that attackers use to steal data—DNS exfiltration. That’s exactly what Varonis came in to test.”

Solution

Introducing perimeter threat analytics to the security stack

During the Purple Team exercise, the Blue Team used **Varonis Edge** to detect exfiltration attempts that the law firm’s other solutions missed. Edge analyzes metadata from perimeter devices (DNS, VPN, and web proxies) to detect attacks and expand the security team’s field of vision.

Combined with **DatAlert Suite**, Edge enables DNS events to be pulled in and monitored while DatAlert functions like an early alarm system that lets security teams know about unusual activity taking place on the perimeter.

When Edge + DatAlert detected unusual DNS requests coming from the Purple Team exercise, it sent a detailed alert to the information security director about the possible threat.

“Varonis alerts tend to be richer [than other security solutions]. Every alert includes a clickable link that takes you into the console to get additional detail and see exactly what’s happening in your environment.”

Before the Purple Team exercise, the law firm hadn't given a lot of thought to perimeter defenses; they'd focused all of their efforts on improving the security of core systems and folders.

> “We have over 20 offices. Each office has its own server and each server has many folders. Before Varonis, nobody really knew who owned that data or who was accessing it.”

The Varonis solutions they rely on are DatAdvantage and DatAlert Suite. With **DatAdvantage**, they have unparalleled visibility into their core systems. Following audit trails and remediating permissions for on-prem data stores, SharePoint, and Active Directory is a breeze.

> “When you are looking at a file share, it's easy to click on a folder and see who has access to that folder. What's more difficult is figuring out exactly who's responsible for a change or tracking everything that user has accessed. That's where Varonis comes in.”

The Purple Team exercise demonstrated the value of having equally high-level analysis and visibility into perimeter activity. With the help of Varonis' Forensics Team, the Blue Team assessed their biggest vulnerabilities and developed an improved incident response plan built around Edge.

Now the company has 360-degree visibility. Regardless of whether a threat originates from an insider (e.g., an attorney saving sensitive data to an external drive) or an outsider (e.g., APT intrusions or data exfiltration attempts), this firm has the ability to quickly detect and deal with it.

> “If you have twenty different tools in your stack, you probably could go in and stitch all of that information together… but investigations are time sensitive. Varonis collects all of the need-to-know threat information and puts it into one tidy package.”

> “Varonis alerts tend to be richer. Every alert includes a clickable link that takes you into the console to get additional detail and see exactly what’s happening in your environment.”

Results

5X faster incident response and added peace of mind

Getting buy-in for a new security solution isn’t always easy, but the information security director says that decision-makers understood the urgency when they reviewed the Purple Teaming results and learned how much damage DNS exfiltration had done to other firms.

> “Varonis has helped guide the firm in best practices for user management, incident response procedure, and handling unstructured data.”

More importantly, the firm is taking every possible step to protect its attorneys, employees, and clients. Client trust depends heavily on the firm’s ability to prove compliance and protect their sensitive data—earning and maintaining that trust is paramount.

> “Many of our clients require us to maintain least privilege when it comes to who can access their data. On a regular basis, they will check in with us and ask for evidence that we are compliant. It’s easy for me to hop into Varonis and create a report of all the people who can access that data and everyone who has accessed it in the past 90 days.”

The security team now has the visibility they need to monitor their servers for both insider and outsider threats. They keep a watchful eye on who’s accessing, moving, and changing sensitive data.

> “Now we have a myriad of tools and good environmental awareness of what’s going on in our servers. Varonis is one of our top solutions.”

Should the worst-case scenario occur—a bad actor attempting to gain access and exfiltrate sensitive data—they won't be caught off guard. With Varonis, they have the requisite insight to take quick and decisive action.

> "It's really about making quick decisions. With Varonis, I have everything I need within a half hour. Without Varonis, it would take me at least five times longer."

> "Varonis has helped guide the firm in best practices for user management, incident response procedure, and handling unstructured data."

VARONIS

Level up your threat detection and alerting.

Stop intrusion and data exfiltration with Varonis.

REQUEST A DEMO