VARONIS

How Varonis Helps a Large U.S. Law Firm Combat Insider Threats and Ransomware

CASE STUDY

“When it comes to potential insider threats, Varonis provides a lot of peace of mind. Every morning, I review a list of all the file accesses that took place over the last 24 hours. Varonis tells me if users accessed anything abnormal.”

ABOUT THIS CASE STUDY:

Our client is a large U.S.-based law firm. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Enforcing least privilege to protect client data
- Monitoring anomalous user behavior for hundreds of attorneys and paralegals
- Fixing permissions on millions of folders open to everyone

SOLUTION

The most robust data security platform:

- **DatAdvantage** maps data access activity across file and email systems
- **Data Classification Engine** finds and classifies sensitive data
- **DatAlert** monitors and alerts on critical systems
- **Automation Engine** automatically repairs and maintains file system permissions

RESULTS

- Open access reduced by 5,144,800 folders
- Remediation that would have taken a team 10+ years finished in 6 months
- Visibility and alerting help the firm protect client data against insider and outsider threats

Challenges

Monitoring potential insider threats on folders with long lifespans

A study published by the American Bar Association revealed that most law firms are shockingly underprepared to protect client data. At least 29% of firms have experienced a security breach and only 34% of firms have any sort of incident response plan in place.

But one well-established U.S. law firm (anonymous by request) partnered with Varonis in 2012 to proactively protect client data. As one of the firm's security engineers explains:

> "Protecting confidential client information is a number-one priority. 90% of what we actually maintain on our network requires visibility as to who, what, and when files were accessed or modified."

Law firms guard a lot of sensitive client information, including data that could potentially be used for insider trading. It's imperative that only need-to-know permissions are implemented and maintained.

But with several hundred lawyers, paralegals, and other users who might need access, enforcing least privilege before Varonis was a challenge. It became such an issue that they even hired interns specifically to help lock down sensitive data.

> “I don’t have time to figure out for each individual attorney what case or client they’re assigned to, or if it’s normal for them to be working on this case at these hours,” says the security engineer.

Even with a team of interns, it was a big job. The firm had nearly 12 million folders, approximately half of which were open to everyone in the company.

Worse, the nature of the work made it difficult to monitor folder access for suspicious activity. Information access peaks while attorneys review material for cases, but otherwise files may sit untouched for a long time. Without Varonis, maintaining least privilege was impossible.

> “We deal with long timelines in the legal community. Varonis is really good about telling us whether someone accessed something for the first time or whether they accessed something way outside of the norm for that user or for those set of files.”

> “I don’t have time to figure out for each individual attorney what case or client they’re assigned to, or if it is normal for them to be working on this case at these hours.”

Solution

Monitoring and alerting on critical systems

In 2012, the law firm purchased **DatAdvantage** to auto-identify privileged accounts and other metadata, which Varonis uses to build a baseline of normal user activity.

Dozens of built-in reports make it easy to gain on-demand visibility into permissions, stale data, and altered files. Security engineers can also schedule regular reports for automatic delivery.

> “Varonis assists in the technology aspect of auditing and it enables us to provide security updates to the C-suite in layman’s terms.”

The firm also purchased **Data Classification Engine**, which locates and identifies sensitive data stored on premises.

With visibility into who had access to what data, combined with knowledge of overexposed sensitive data, security engineers could prioritize risk remediation efforts on the highest impact areas.

In 2016, the law firm added **DatAlert** to their Varonis lineup. When anomalous activity occurs, Varonis alerts the firm’s chief information security officer (CISO). DatAlert uncovers threats across the kill chain, from suspicious lateral movement to unusual download or upload activity.

> “Once we had reporting and alerts in place, our folder hygiene improved. Varonis enabled us to create and execute a plan that matured how we grant ownership and enforce least privilege.”

In 2019–2020, the firm added DatAdvantage for Directory Services and Exchange. This enables the firm to monitor and protect Active Directory and email servers, and detect anomalous activity such as unusual access and permission changes.

The law firm also added Automation Engine to safely repair and maintain file systems. By automatically fixing hidden security vulnerabilities and revoking unnecessary user access, Automation Engine reduces company-wide risk.

> “Picture a coffee machine. You walk into your kitchen in the morning, flip a switch, and it starts brewing. You can expect to have coffee ready in three minutes flat—that’s what Automation Engine does for us.”
>
> “We don’t have to spend time building out remediation processes. We can run it at a moment’s notice, and it automatically enforces the rules we’ve set—way faster than it would take interns to do the same thing.”

With Varonis, security engineers had heightened visibility and the control needed to undertake a massive remediation project. The goal: address the large quantity of overexposed data in their on-prem environment.

“Once we had reporting and alerts in place, our folder hygiene improved. Varonis enabled us to create and execute a plan that matured how we grant ownership and enforce least privilege.”

Results

A 10-year remediation project completed in 6 months

In six months, Varonis helped the law firm **reduce the folders with open access by a staggering 5,144,800 folders**. At the same time, they were able to find and fix other issues like broken permissions on tens of thousands of folders.

According to a security engineer, it took a full team—including interns—two-and-a-half years to lock down just 1,500 files back when they were performing cleanup manually.

The time savings, he says, are astronomical.

> “It would have taken an estimated 10 years to lock down those permissions manually. Varonis did it in six months.”

But Varonis delivers more than just time savings—it also gives the security engineer and his team tremendous confidence that they're capable of detecting and responding to potential incidents.

Before, they would have had no way of knowing if a user accessing certain files was suspicious. Now, Varonis flags anomalous behavior and gives the security team context to eliminate doubt.

> "When it comes to potential insider threats, Varonis provides a lot of peace of mind. Every morning, I review a list of all the file accesses that took place over the last 24 hours. Varonis tells me if users accessed anything abnormal."

The firm has never had to contend with a data breach, but if the worst should occur, they're glad to know that they have Varonis.

> "The support is fantastic. You can expect a same-day response or better. Varonis' team is very solution-oriented and easy to work with. They take feedback and enhancement requests seriously, and they're good at locking down environments when you are worried about ransomware or insider threats."

> "It would have taken an estimated 10 years to lock down those permissions manually. Varonis did it in six months."

VARONIS

Mitigate the risk posed by insider threats and ransomware.

Varonis helps you find and fix security vulnerabilities in a fraction of the time.

REQUEST A DEMO