VARONIS

How One of the Largest U.S. Credit Unions Uses Varonis for DLP

> We finally have eyes on our data. Knowing that we can provide answers on data access during investigations is a big sense of relief.

About this case study:

Our customer is one of the largest credit unions in the U.S. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

+ Identifying where sensitive data exists
+ Controlling excessive access to data
+ Detecting suspicious data access and other potential threats

Solution

The Varonis Data Security Platform:

+ Provides visibility and control over critical data and IT infrastructure
+ Finds and classifies sensitive data automatically
+ Pre-built classification patterns
+ Automatically eliminates excessive permissions
+ Streamlines data access governance
+ Enforces rules for data movement and migration
+ Monitors and alerts on abnormal behavior in critical systems
+ Detects and helps prevent data exfiltration
+ Helps fulfill DSARs quickly and easily

Results

+ Reduced open access by 93%
+ Identified 5X more stale data than they knew existed
+ Investigated and resolved three potential attack

CHALLENGES

Getting a handle on sensitive data

One of the largest credit unions in the U.S. (anonymous by request) approached Varonis with a long list of challenges they needed to solve, including:

+ Classifying sensitive data, especially PII and PCI, across the entire network
+ Protecting sensitive data from being encrypted by ransomware
+ Limiting access to sensitive data
+ Reducing the burden on IT to manage data access
+ Finding and safely removing stale data
+ Achieving and maintaining CCPA compliance

The concern underpinning all of these use cases was data loss. A data breach would have disastrous consequences for the credit union — both reputational and financial.

The company's CISO confirms:

> **"My number one concern is data loss, whether that's through ransomware or unauthorized access."**

Before Varonis, it was impossible for the company to get a handle on data. They lacked visibility into where data lived, who had access, and whether or not it was sensitive.

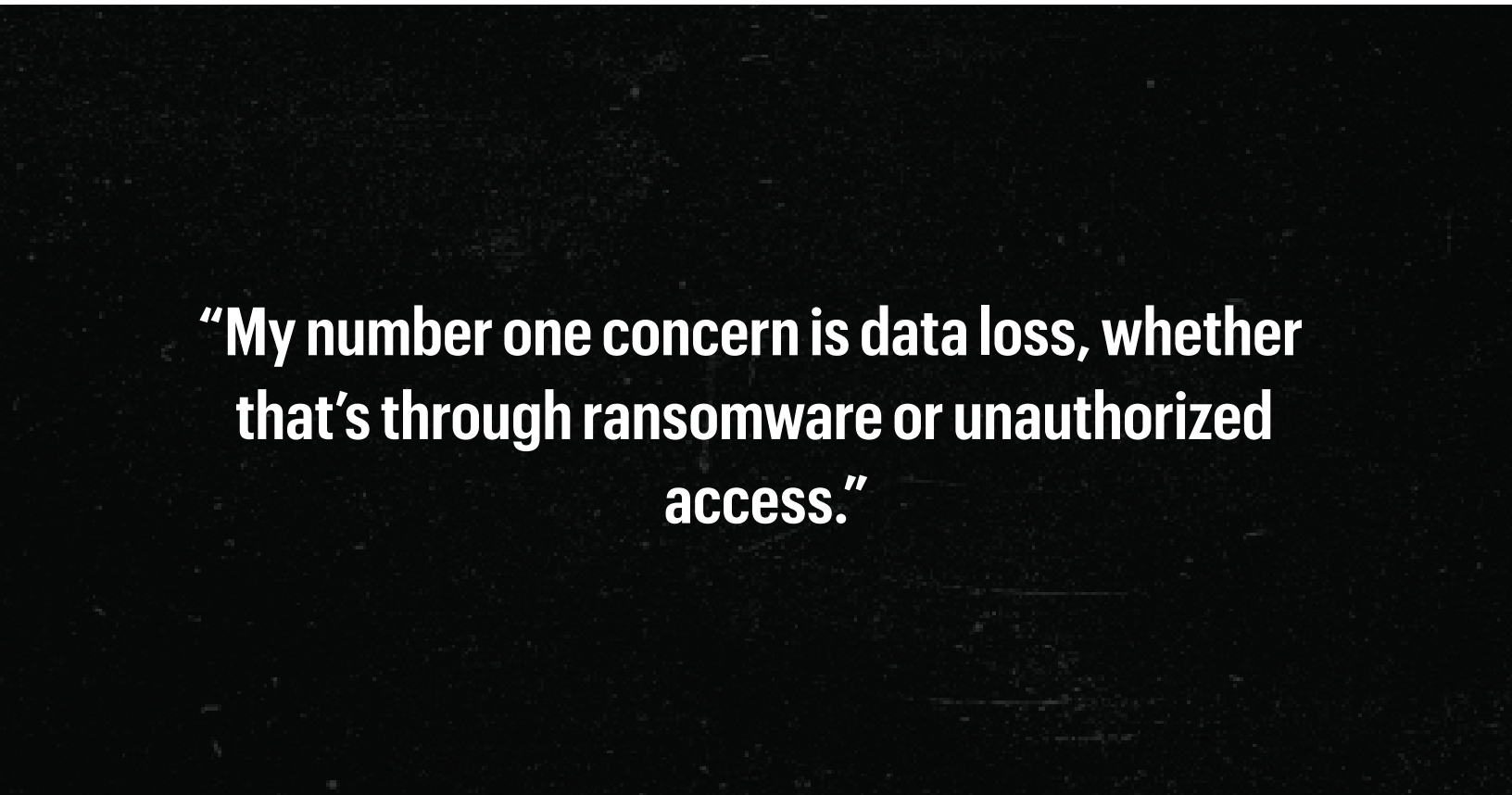
Just trying to identify data owners was a long and labor-intensive process.

> **"I didn't really have an automated way to identify data. I would go in manually, right-click each folder, and look at who had access to it to try and identify data owners."**

After researching a myriad of cybersecurity solutions and discussing their needs with multiple vendors, the credit union decided that Varonis was the best fit for their environment.

According to the CISO:

> **"I knew we had data all over the place and a lot of people in and out of our data. There was a lot of cleanup to do. Varonis fulfilled our needs better than anyone and the proof of concept confirmed that they'd be able to help with our data governance initiatives."**



SOLUTION

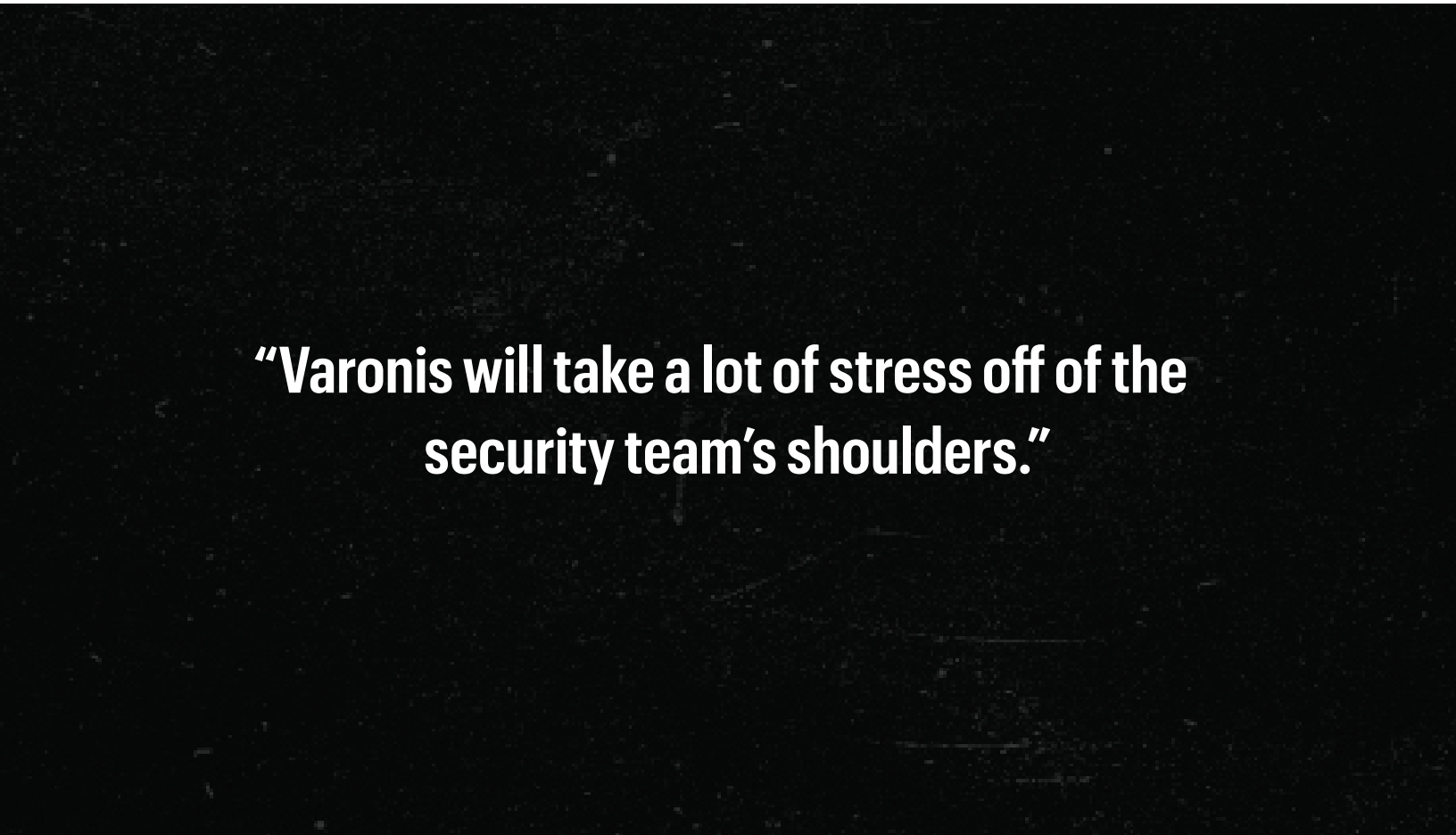
Reducing an attack's blast radius with a data-centric approach

To support their many use cases, the credit union adopted the Varonis Data Security Platform. They started by using Varonis to secure their on-prem environment.

Varonis maps file and folder structures and catalogs permissions to provide a clear picture of where data is overexposed and at risk. The platform provides real-time insight into who accesses data, when, and from where. This solution makes it easy for the credit union to limit who can access data in their environment. It also allows them to collect, enrich, and report on the data in their network.

Varonis also accelerated their permissions cleanup project by eliminating excessive access to data at scale. By removing global access group permissions and enforcing least-privilege access, the credit union is moving toward Zero Trust data security and minimizing the blast radius of a potential attack

> **"I was extremely happy with how Varonis was able to go in and automatically fix broken permissions and open access issues in our files and folders. Then it automatically created new groups with only the applicable users and identified data owners. That was great."**



Varonis maintains least privilege by giving data owners control over access to their data, rather than having IT manage all data access requests. This not only speeds up access request approvals for people who need it, but also prevents people who don't from accidentally receiving access. Data owners can even set up automated expiration dates to remove access when it is no longer needed.

> **"We're now working to remove IT's ownership of having to assign permissions by putting that process in the hands of data owners where it belongs. Varonis will take a lot of stress off of the security team's shoulders."**

Detecting and stopping threats

Varonis adds automatic monitoring and threat-detection to sensitive files. When Varonis detects anomalous behavior, the platform can lock those compromised accounts out of the network so the CISO's team can investigate the incident. Varonis analyzes metadata from perimeter devices like DNS, VPN, and web proxies to look for the telltale signs of malware, APT intrusion, and data exfiltration.

According to the CISO:

> **"I was pleasantly surprised by Varonis. When it sees unusual file system access that may indicate a ransomware attack, it sends an automated text alert to the security team.**

Streamlining compliance

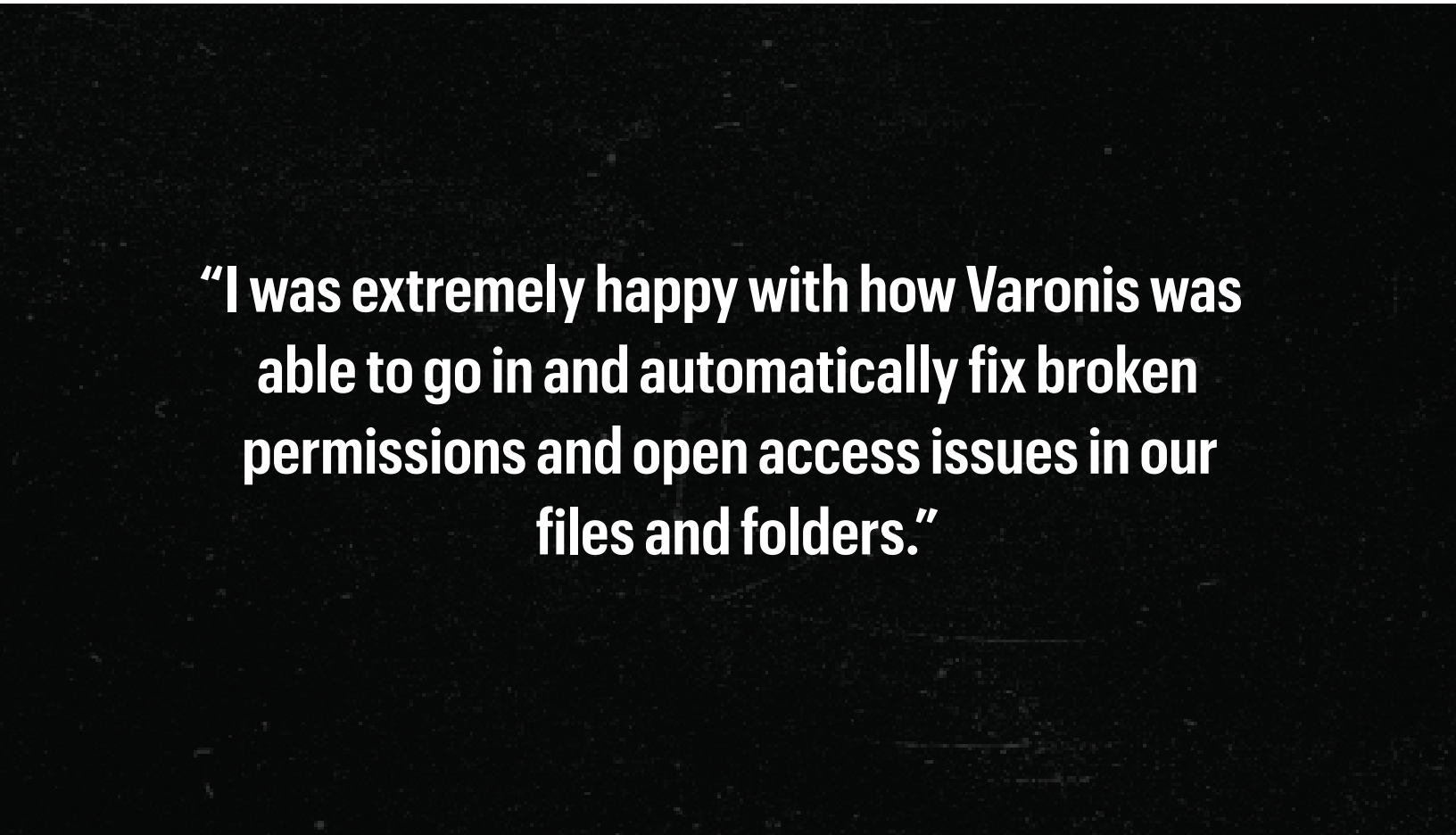
Varonis automatically scans, classifies, and indexes file contents and properties. The solution provides insight into where sensitive data lives, enabling the CISO to prioritize access remediation to those files first or move the sensitive data if it doesn't belong there. The solution pinpoints CCPA-regulated data.

> **We have certain locations on the network where PII shouldn't be stored. Varonis scanned that location and found a bunch of sensitive data that shouldn't have been there and we were then able to move that data.**

Varonis makes the process of moving data safe and easy. It can automatically move, quarantine, or delete data according to existing data governance policies..

When a customer wants to know what personal information the credit union has about them, Varonis acts like a search engine that quickly and easily pulls up all relevant data.

> **"Now we can easily pull a report for CCPA compliance. I'm also able to pull reports on specific areas, like where our development code is stored, and ensure that the right people have access. I now generate a weekly report for the business to review in case there are any changes to that."**



RESULTS

Eliminating data exposure

Before Varonis, the credit union didn't have a holistic view of their data, an easy way to remediate permissions, or a way to identify threats — at least, not until it was too late. With Varonis, they now have 360-degree visibility into their data, advanced threat detection and response capabilities, and the controls needed to maintain CCPA compliance.

> **"We finally have eyes on our data. Knowing that we can provide answers on data access during investigations is a big sense of relief."**

Within one year, the CISO successfully reduced open access on sensitive files by 93 percent. They also identified more than 5X the sensitive stale data they'd previously known about, and they're using Varonis to safely move, quarantine, and delete it.

> **"Access remediation is always a work-in-progress, but having a better handle on your data and knowing that nobody has accessed your sensitive information removes a lot of stress."**

To help guard against ransomware, the credit union reached out to the Varonis Incident Response team to help investigate alerts three times. Thankfully, every incident was benign. The CISO is glad to know that when the credit union needs help, Varonis steps up to the plate.

> **Varonis has fired off three times so far when it detected unusual data access activity. We engaged the IR team to investigate and they were tremendous to work with — very responsive, very knowledgeable."**

Your data. Our mission.

Varonis takes the time and complexity out of securing sensitive data and meeting auditing requirements.

Request a demo