VARONIS

How Varonis Helps One Real Estate Company Secure Sensitive Data in Box

> Depending on how mature your environment is and how heavily you utilize Box, you really need to try Varonis. If you want to get that visibility or improve data governance, it will definitely help you out.

About this case study:

Our customer is a top real estate organization in the U.S. We have anonymized the company name at their request.

HIGHLIGHTS

Challenges

+ Protecting HIPAA, GDPR, and CCPA data in Box
+ Gaining visibility into data sharing and permissions
+ Improving cloud threat detection and response

Solution

Varonis Data Security Platform:

+ Visibility into cloud apps and services including M365 and Boxy
+ Finds and classifies sensitive data across cloud apps
+ Streamlines data access governance
+ Monitors and alerts on abnormal behavior on critical systems
+ Detects and helps prevent DNS exfiltration attempts

Results

+ Monitoring and alerting in Box
+ Eliminated excessive permissions in Box
+ Discovered and classified sensitive data across cloud platforms

CHALLENGES

Protecting sensitive and regulated data in Box

One of North America's top real estate organizations (anonymous by request) has been using Varonis to protect its sensitive data from threats like ransomware since 2015.

Between 2015 and 2020, the company relied on Varonis to secure Microsoft 365 and Windows hybrid environment, map user permissions, and be alerted to suspicious activies.

But as employees began to work more from home, a new issue emerged. Collaborative apps like Box were quickly becoming commonplace — and this left sensitive client information and regulatory data exposed to new risks.

As Senior Cybersecurity Engineer Tony Hamil explains:

> **"We're a heavy Box adopter. But with Box, you can make a link public with no password and nobody will know."**

Box does have data governance built into the platform, but Tony's small team didn't have the capability to set it up or build out the rigorous alerting his organization needed.

At the same time, he knew that a substantial amount of public and external sharing was already occurring on Box. He was worried that cloud sharing might make it all too easy to overshare sensitive information.

> **"While using Box, we still need to protect data across the board. We store a lot of PII and PCI and other sensitive data that falls under HIPAA, GDPR, and CCPA."**

To mitigate risk, the company needed an easy way to:

+ Classify critical and sensitive data and then protect that data from overexposure.
+ Understand where data is being shared and enforce least privilege by locking down unnecessary access.
+ Visualize and clean up permissions to sensitive data to reduce the blast radius of a potential incident.
+ Automate threat detection and response to proactively identify and stop malicious activity.

Varonis was already helping the real estate organization answer critical questions about their Microsoft 365 and on-prem data. Tony wanted that same level of visibility in Box.

"We needed to protect our data and make sure that we have the right permissions around it. If it's public and sensitive, I want to know about it. And if someone is doing something that's considered malicious, I want to stop it."

SOLUTION

Varonis helps support rapid digital transformation

To support the real estate organization in their move to the cloud, Varonis performed a free Cloud Data Risk Assessment. The assessment covered all of the company's critical cloud services, including apps like Box and Salesforce.

The audit confirmed many of Tony's suspicions, including that a large amount of external sharing was already occurring in Box. But it also revealed some surprising security gaps.

> **"If you're actually serious about making sure your data is secure, you need to do a Proof of Concept. Trust me, I thought our environment was tight, but the POC might prove that you don't have the control you think you do."**

Varonis engineers showed Tony that the number of Box users within his organization was 180% the number he'd expected. They shined a light on excessive external sharing, personal account activity, and risky misconfigurations taking place.

> **"Without Varonis, we'd be blind to all of those issues. I had no idea that use had exploded as much as it had—and I had no visibility into the traffic, events, and possible interactions that you want alerting on."**

Setting up Varonis within the company's environment was fast and seamless. Tony was thrilled to be able to use Varonis to do the same things in Box that he had been able to do on prem for years.

> **"The value of Varonis' out-of-the-box rules for Box and Salesforce, and of course the ones that they have for Windows, can't be overstated. It means that we don't have to hire roles specifically to monitor these products and keep them updated. And Varonis is releasing updates all the time."**

With Varonis Tony can quickly find and fix the biggest data risks. He has the visibility he needs to weed

out excessive permissions and eliminate shared links that might compromise cybersecurity and lead to a breach.

> **"Varonis helps us monitor Box for anomalous logins, over sharing, and odd data activity—like somebody uploading, deleting, or touching a lot of data. Box is very secure when used properly, which we can now confidently say we're doing."**

Real-time and interactive views of data access, roles, and permissions give Tony more confidence in his ability to manage data risk and securely offboard employees.

> **"One of the nice things about Varonis is that you can trace back what's going on by using what they call CRUDS—Create, Read, Update, Delete, Share. So I can search for the share function and actually see if one of our users shares something out and gives permission to an external vendor or user that's not considered trusted."**

The real estate organization also uses Varonis to classify data in Box, which automatically matches file contents to hundreds of classification patterns, accurately identifying PII, PCI, PHI, and more.

"Varonis helps us monitor Box for anomalous logins, over sharing, and odd data activity — like somebody uploading, deleting, or touching a lot of data. Box is very secure when used properly, which we can now confidently say we're doing."

RESULTS

Critical data protected from misuse and overexposure

With Varonis monitoring and alerting on Box content shares, Tony can rest easy knowing that user error isn't undermining his organization's IaaS and SaaS cybersecurity.

> **"Varonis is extremely good at catching a lot of these anomalous events that most other cybersecurity providers will not catch. Now that we have more people utilizing Box, that visibility is key."**

Tony especially loves that Varonis removed the onus from his team to set up data governance and alerting in-house, which enabled data engineers to focus on other parts of the job.

> **"It's great if you have a team that can set up Box's built-in data governance. But if you have a smaller team that lacks the ability to manipulate all of these alerts and built-in functions, Varonis will come in and do all that backend work for you."**
>
> **"With Varonis, we have a healthy coexistence. That partnership is the difference between spending a couple of hours versus working an entire weekend to solve an issue."**

Now, cybersecurity engineers at this organization utilize the Varonis Data Security Platform to:

+ Gain critical visibility into on-prem and cloud activity.
+ Classify sensitive data and maintain compliance.
+ Alert on suspicious behavior and investigate alerts in real-time.
+ Stop intrusion and data exfiltration attempts.

As this organization's cybersecurity needs continue to evolve, Varonis is excited to support them in their journey.

According to Tony:

> **"Depending on how mature your environment is and how heavily you utilize Box, you really need to try Varonis. If you want to get that visibility or improve data governance, it will definitely help you out," he says.**
>
> **"We truly were trying to get full visibility into our Box environment since 2014 using CASBs or other products, but without the ability to integrate it properly with a tool like Varonis, we did not receive the benefits that we incur now with UEBA and cross-platform visibility."**

"Varonis is extremely good at catching a lot of these anomalous events that most other cybersecurity providers will not catch. Now that we have more people utilizing Box, that visibility is key."

Get advanced data security for Box.

Secure your sensitive data in Box and other cloud services.

Request a demo