How an Online U.S. Bank Secures its Remote Workforce During the COVID-19 Crisis

CASE STUDY

> “I can pull logs from our VPNs directly into Varonis. Now we get suspicious login reports delivered straight to our email inboxes at 10 o’clock every morning—and that has been truly valuable with over 75% of the company working remotely due to the current world situation.”

ABOUT THIS CASE STUDY:

Our client is an online U.S. bank. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Pivoting to a remote workforce with minimal disruptions
- Mitigating the risk to critical systems posed by remote login attempts
- Ensuring expedient issue resolution for people working from home

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Windows, Exchange, and Directory Services maps remote user activity and permissions
- **Data Classification Engine** for Windows and SharePoint pinpoints sensitive data
- **DatAlert Suite** monitors and alerts on all data and systems
- **Edge** to analyze metadata from VPNs, DNS, and other perimeter technologies to spot signs of perimeter attacks

Full integration with key systems

- **Pulse Secure (VPN)**
- **Palo Alto GlobalProtect (VPN)**
- **LogRhythm (SIEM)**

RESULTS

- Comprehensive login reports are automatically pulled from VPNs
- Time savings for security teams and key system admins
- Enhanced data security and more peace of mind as the bank mobilizes its remote workforce

Challenges

SECURING A LARGE REMOTE WORKFORCE

When an online U.S. bank (anonymous by request) rolled out Varonis in 2017, they had no idea how pivotal it would become to maintaining a flexible and secure workforce in the following years.

COVID-19 changed everything. It wasn't long before over 75% of the company was working remotely. This placed immense pressure on the Senior Applications Administrator to ensure that employees could work seamlessly from home.

> “Prior to Varonis, we didn't have any real data in front of us that compiled login and logout failures, account lockouts, and other issues that need to be in front of your face to alleviate.”

The company relied on two VPNs—Pulse Secure and Palo Alto GlobalProtect—to protect user and company information. But diving into each of those systems to diagnose issues took time and it wasn't immediately obvious when users encountered a problem.

> “If we were looking for something, we'd have to go into each individual system to see who is walking in, what the capacity is, who is trying to log in and failing—it was time-consuming, for sure.”

Worse, supporting a large remote workforce increased the threat of cyberattacks. The Senior App Admin needed to be able to diagnose at a glance whether a failed login attempt was simply a user mistyping a password—or something more insidious.

> “The bank’s security is riding on my shoulders. I need to know who is trying to access and who is accessing our data. I need that information in front of me at all times.”

As more of the bank’s workforce began working remotely, senior leaders were concerned: “How are we going to monitor all of these people working from home?”

> “Fortunately, we already had Varonis in place,” the Senior App Admin says. “It was a simple matter to set up login reports and get those reports delivered automatically via email to the head of IT.”

“The bank’s security is riding on my shoulders. I need to know who is trying to access and who is accessing our data. I need that information in front of me at all times.”

Solution

MONITORING AND ALERTING TO MITIGATE THE RISK OF WORKING REMOTELY

When COVID-19 became a global pandemic, the online bank had already rolled out four Varonis products in a push to fill security gaps and shore up its defenses: DatAdvantage, Data Classification Engine, DatAlert Suite, and Edge.

This was important for three reasons:

1 Varonis was already providing critical visibility into data access behavior

DatAdvantage and Data Classification Engine, the first two products the bank adopted, give more visibility into what data users are accessing and where they have too much access.

At first, the bank's goal was just to use this information to enforce data protection and compliance. But when most of their workforce needed to work from home, **DatAdvantage for Exchange and Directory Services** became especially pivotal for ensuring security.

While users collaborate via Exchange and log into the bank's servers remotely, Varonis monitors these systems and gives the security team a comprehensive, prioritized picture of where data is exposed.

> "Varonis gives me the ability to know what's going on in our file systems at any given time. It's not something I have to concentrate on because the software is doing it for me," says the Senior App Admin.

2 Threat detection and response capabilities to protect critical systems and remote users

If Varonis detects any irregular activity (e.g., a user account accessing data it doesn't normally access, attempting to view information it doesn't have permission to view, or suddenly deleting files), **DatAlert**'s real-time alerting and monitoring enables the bank's security team to get a handle on the situation immediately.

Best of all, Varonis integrates seamlessly with the bank's SIEM solution, LogRhythm. Varonis feeds rich context and unstructured threat intelligence into LogRhythm, which applies its pattern recognition and log management capabilities to the data.

The result is detail-rich threat detection capabilities that alert the bank's security team to even the earliest warning signs of suspicious user activity before it could potentially turn into a full-fledged data breach.

> "The alerting capabilities let us know if a user mass deletes data or starts cleaning out a directory that someone else may need. We haven't seen any sign of attacks yet, but it's comforting to be able to review daily logs and recognize legitimate users making honest mistakes, like mistyping a password."

3 Edge adds extra security to remote logins through VPNs

When remote employees use Pulse or Palo to connect to the bank's corporate network, Edge analyzes and enriches metadata from the VPNs to spot login issues and the telltale signs of attacks on the perimeter.

This insight is possible because Edge combines perimeter activity with other data streams (like file, email, and Active Directory). By baselining a user's typical access activity, geolocation, and security group memberships, it's easy to spot the difference between a user who forgot their password and a potential data breach in progress.

Varonis automatically compiles information from both VPNs into comprehensive logs, enabling the Senior App Admin to get ahead of login issues that remote users may be having.

> “I can pull logs from our VPNs directly into Varonis. Now we get suspicious login reports delivered straight to our email inboxes at 10 o’clock every morning—and that has been truly valuable with over 75% of the company working remotely due to the current world situation.”

> “Varonis gives me the ability to know what’s going on in our file systems at any given time. It’s not something I have to concentrate on because the software is doing it for me.”

Results

A SECURE REMOTE WORKFORCE

With Varonis, the Senior App Admin is able to start every day by reviewing a comprehensive report that breaks down the previous day's activities. They say it's had a tremendous impact on ensuring workflow efficiency as they mobilize their remote workforce.

> "If I notice one of our VPNs slow down, I can go to Varonis and pull the report on user activity. With that log, I can see where the bottleneck is and quickly come up with a solution."

Diagnosing and resolving similar issues pre-Varonis wasted tremendous amounts of time and resources. Now it's a non-issue.

> "Prior to Varonis, we used to have our internal security team digging through event logs on all the different servers that they have. With Varonis, it's like having an extra employee instantly handling a task that used to take a team of five people a full day."

Despite the fact that most of the bank's employees are now working remotely, the Senior App Admin and leaders at the bank are able to rest easy knowing that Varonis is monitoring their sensitive data and enforcing least privilege, even when they are out of office.

> “Every company needs Varonis. It’s eye-opening to see the amount of private data that is on the network and how many copies of that same data exist. If you’re blind to that information, you’re setting yourself up for disaster.”

For extra peace of mind, Varonis support teams are always on hand to help this bank—and all of its customers—secure their remote workforce and cope with new security challenges.

Varonis is also offering free incident response services and threat monitoring for O365 Teams, VPN, Active Directory, and more.

> “Every company needs Varonis. Gaining visibility into how much data exists on your network is eye-opening. If you’re blind to that information, you’re setting yourself up for disaster.”

VARONIS

Secure your remote workforce.

Don’t let insecure networks and devices stop you from getting back to “business as usual.”

REQUEST A DEMO