How Varonis Helped a U.S. Casino and Hotel Stop a Cyberattack within 30 Minutes

CASE STUDY

"Without Varonis, I probably wouldn't even have known that an account had been breached. With Varonis, I was on a call with their Incident Response Team for about 30 minutes and we had it resolved."

ABOUT THIS CASE STUDY:

About this case study: Our client is a U.S.-based casino and hotel. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Attackers targeted an open RDP and obtained account names
- They began brute-forcing their way in, attempting to hack into privileged accounts
- Sensitive data, including PII and PCI, was at risk

SOLUTION

The most robust data security platform:

- **DatAdvantage** monitors data access and activity on prem and in Active Directory
- **Data Classification Engine** identifies at-risk sensitive data, including PII and PCI
- **DatAlert Suite** provides continuous monitoring and alerting on critical systems

RESULTS

- Varonis detected the threat and the Incident Response team helped defeat it within 30 minutes
- Network admin saves 2–3 hours per day with automated alerting and reporting
- Having a team of experts one phone call away provides peace of mind

Challenges

Defeating a malicious attack before it could escalate

It all started with an exposed server.

A U.S.-based casino and hotel (anonymous by request) had an open RDP (remote desktop port) connection to the internet.

Attackers gained access to the server and even obtained account names. They began trying every password they could, attempting to brute-force their way into user accounts.

It was a gut-wrenching moment for the network admin in charge.

> “They had account names. They could have sat there and brute-forced those accounts until they got into a privileged account. After that, who knows? They could have accessed our file servers… or any of our systems.”

A breach would have been devastating. The PII and PCI of hundreds of employees and thousands of customers could have been stolen. And, because the incident occurred on a weekend, it’s possible nobody would have noticed the attack for 48 hours or more.

In fact, with their previous security solution, they may never have discovered the threat. A lack of support and training had left them unprepared to track down and deal with aggressive attacks like this.

> "Only one person had been trained to use our previous product. We could limp our way through it, but we couldn't fully utilize it. **So we switched to Varonis, in part because of the awesome training materials and excellent support**."

Varonis provides continuous monitoring and alerting on all of the casino and hotel's critical systems—so the network admin knew about the attack within seconds.

With the support of Varonis' Incident Response team, the potential security breach was quickly defeated.

> "They had account names. They could have sat there and brute-forced those accounts until they got into a privileged account."

Solution

A reliable way to detect and defeat threats proactively

Three Varonis products helped the network admin detect and defeat the attack on the casino and hotel's exposed server:

1. **DatAdvantage for Windows and Directory Services**, which supports on-prem servers and Active Directory by shining a light on who can and who is accessing data.
2. **Data Classification Engine for Windows and SharePoint**, which automatically identifies at-risk sensitive data including PII and PCI.
3. **DatAlert Suite**, which monitors critical assets for suspicious activity and unusual behavior.

> "Varonis provides alerts whenever somebody tries to access the server. It records who accesses what files. It also watches for people outside of our network trying to log into equipment so we can narrow it down and take care of those issues."

The first sign of the attack came when Varonis detected anomalies within Active Directory and sent the network admin two alerts:

- Account enumeration attack from a single source (using NT LAN Manager or 'NTLM')
- Lockout: multiple account lock-out events

The network admin immediately called their Varonis account manager, prompting the Varonis Incident Response team to jump into action.

> “It was amazing. I called my account manager at 8 o’clock on a Sunday morning. They immediately got someone on the phone with me. They helped us resolve it quickly and easily and we haven’t had any other issues since then.”

Using the Web UI, the Incident Response team investigated the failed authentication events and determined that usernames and device names had been spoofed. They then turned to the domain controller reporting the failed authentications and reviewed the NTLM logs.

Forensic analysis revealed that EXCHSRV and HVAC were the source devices for the failed authentications. A server had been left open so the HVAC maintenance company could access it—a vulnerability that could have compromised their entire network.

> “Varonis allows me to narrow down which servers and ports attackers are hitting. It makes it easy for me to lock down individual servers and prioritize our most at-risk areas.”

To identify the source IP and port used in the brute-force attack, the Incident Response team ran a NETSTAT (network statistics) command on affected workstations. This revealed that the failed authentications were coming from a Russian-based IP address over RDP.

The Incident Response team helped the network admin disable the HVAC server during their call and stop the brute-force attack. They also recommended that the casino and hotel disable external RDP access, and enable the Windows firewall on the Exchange server to safeguard against future attacks.

"I was on a call with the Varonis Incident Response team for about 30 minutes and we had it resolved."

Results

Peace of mind and time savings

With Varonis, the network admin gained visibility into on-prem servers and Active Directory. They never imagined how crucial the security solution would become.

"I was excited to have the ability to monitor and see everything happening in my servers. The automated alerts were a nice bonus. All of those things quickly paid off."

Having an Incident Response team in their court—and a partner that's willing to leap into action to help them trace threats and defeat them at their source—provides ongoing confidence.

The network admin explains how a potentially crippling cyberattack was resolved quickly, thanks to Varonis:

> "Without Varonis, I probably wouldn't even have known that an account had been breached. With Varonis, I was on a call with their Incident Response Team for about 30 minutes and we had it resolved."

Now, Varonis continues to provide monitoring and alerting on all of the casino and hotel's critical systems. The increased visibility enables the network admin to find and fix vulnerabilities with confidence, and saves hours every day.

> "Between the continuous alerting and the automatic reports, Varonis saves me 2–3 hours every day. It makes monitoring critical systems a lot easier. The reporting function alone justifies the cost."

"Between the continuous alerting and the automatic reports, Varonis saves me 2–3 hours every day."

Get the peace of mind that comes from having a team of experts in your court.

Varonis helps you investigate threats, resolve security incidents, and protect your critical systems.

REQUEST A DEMO