How Varonis is Safeguarding One Real Estate Developer From a Difficult-to-Detect Cyberthreat

CASE STUDY

"Varonis Edge was the **only solution** that was able to detect DNS tunneling threats. **No other product was able to detect it.**"

Tony Hamil,
Cyber Security Engineer

ABOUT THIS CASE STUDY:

Our client is a respected real estate development company. We have happily accommodated their request to anonymize the company name and omit all sensitive details.

HIGHLIGHTS

CHALLENGES

- Monitoring file integrity during migration to a new cloud-based file sharing program
- Protecting sensitive information on-premises & in the cloud
- Detecting potentially destructive cyberattacks & data breaches using DNS tunneling & other methods.

SOLUTION

The most robust data security platform:

- **DatAdvantage** integrated with Windows & Exchange Online
- **Data Classification Engine** for Windows & SharePoint
- **DataPrivilege** to help ensure compliance & make data access governance easy
- **DatAlert** to detect potential malware or internal data leaks
- **Edge** to spot subtle signs of attack from the network perimeter

RESULTS

More confidence & peace of mind due to:

- Having a solution that can reliably detect DNS tunneling attacks
- A simple & intuitive UI that streamlines threat detection & prevention
- Customer support that's second-to-none
- Ongoing updates & add-ons to ensure the customer, and their data, is protected

Challenges

Protecting on-premises & cloud-based files

Tony Hamil is the Senior Cyber Security Engineer for a top real estate developer in North America. His responsibilities include protecting the company against hackers, continuously improving its ability to detect and respond to threats, and managing security applications like Varonis.

His company adopted Varonis back in 2015. They had just implemented Box, a cloud-based file sharing program, and needed to lock down permissions and gain more visibility into their on-premises and cloud-based data storage.

> "We originally got Varonis because DatAdvantage helped us map access to data, Data Classification Engine showed us where sensitive data was at-risk, and DataPrivilege helped us assign ownership to some of our bigger shares," Tony says.
>
> "When it came to file integrity monitoring, we had to go with Varonis. The other players were either outdated, didn't do the job as well, or resulted in too much of a performance hit," he adds.

As cyberthreats grew more sophisticated, the company continued to add Varonis solutions, such as DatAlert, to keep up with evolving threats and shore up their cybersecurity defenses.

> “DatAlert notifies me when something needs my attention. Alerts could include the presence of intrusion-based hacking tools, encrypted files from a CryptoLocker virus, or even someone uploading an unusual amount of data,” he says.

> “When it came to file integrity monitoring, we had to go with Varonis. The other players were either outdated, didn’t do the job as well, or resulted in too much of a performance hit.”

Challenge

Safeguarding against cyberthreats that sneak past traditional defenses

But what about threats that are notoriously difficult to detect? DNS tunneling is a method hackers use to escape notice by disguising data exfiltration as normal web traffic.

Because it’s hard to detect, this type of threat is often overlooked. But ignoring it has already cost companies around the world millions of dollars.

For example, a DNS attack in 2016 compromised the entire DNS infrastructure of a major Brazilian bank, including corporate email and all 36 of its domains.

The hackers were able to intercept everything from online banking to all mobile, point-of-sale, ATM, and investment transactions. Thousands, if not millions, of the bank's customers were victimized by the attack.

And the bank was just one of ten different institutions hit by the same cybercriminals using DNS tunneling.

Tony saw how significant the risk was to his company.

> "Every company that has a domain has DNS servers, and those servers have DNS open to the world. You normally can't use port 53 from your system to the outside world, but if you tunnel it through the DNS servers then it looks like legitimate activity," he explains.

He was only willing to continue trusting Varonis to protect his company's vulnerable data if it was able to counteract this threat—and prove that it could help him detect and safeguard against even the subtlest attacks.

Solution

The most robust data-centric audit & protection against practically invisible threats

Edge is one of Varonis's newest products. By analyzing metadata from perimeter technologies (DNS, VPN, and web proxies) along with data access activity, it helps you detect and stop even the most stealthy malware, APT intrusions, and data exfiltration attempts.

Tony put the demo version of Edge through the wringer. He did a red-team exercise with DNS exfiltration, by simulating a DNS tunneling attack and then pitting all of their solutions against it.

> “I used a tool called DNScat2 to simulate a DNS tunneling attack through both our public DNS servers and our internal DNS servers to show how dangerous it really is,” he explains.
>
> **“Varonis Edge was the only solution that was able to detect DNS tunneling threats. No other product was able to detect it.** Some of them could collect DNS events, but even they couldn’t tell me at a glance what was going on like Varonis could,” he adds.

Even though the company has millions in cybersecurity investments, Varonis Edge was the only product that picked up the DNS tunneling attack. The successful test made it easy to convince stakeholders of its necessity.

Tony was happy for the chance to demo Edge before purchasing—and it’s that level of support that he says is one of his favorite things about working with Varonis.

> He says, “Whenever I need an issue solved or want to take a new product for a test run, their customer service is always top notch.”
>
> He elaborates, “We faced an issue three years ago and their response was immediate. They had somebody working on it 10 hours a day until it was solved. I don’t know any other company that offers the same level of support and customer service.”

And while Varonis isn’t the only company to offer data classification or file integrity monitoring, Tony can’t think of another solution that offers the same level of detailed reporting or such comprehensive protection for his organization and its users.

He says, “Varonis goes beyond file integrity monitoring. Most platforms can tell you where an event happened. But only Varonis gives you full data correlation and a unified audit trail of events that shows exactly what’s happening and every file that’s been touched, including in the cloud.”

“Varonis Edge was the only solution that was able to detect DNS tunneling threats. No other product was able to detect it.”

Results

Saved time, peace of mind & confidence that they have the most robust data security platform

Tony has been in the cybersecurity business for a long time, and he’s worked with Varonis for years. In that time, he’s seen how much Varonis has evolved.

“Back in 2015, Varonis did the job we needed but the learning curve was steep. It’s insanely different now. It’s easy to use, much more streamlined, and it presents data in real time.”

> “In less than a minute, I can click on an alert and look at the analytics. I can see every file the person accessed both on the server-level and in the cloud. I can see if it happened during the off-time, if they were supposed to have access to that file, if they uploaded anything suspicious, or if there were any other anomalies.”
>
> “If I was trying to do all of this with multiple tools, it would take way more time to find all the logs, put them together, correlate all of the data, and make sure everything lines up. Varonis lets me do all of that quickly in one place. It’s easily saved us an entire FTE (full-time equivalent).”

The technical improvements and add-on features Varonis has introduced over the years have increased both its ease-of-use and its ability to protect sensitive data. Not even the most difficult-to-detect threats, like DNS attacks, can sneak by Varonis and Edge.

That is why Varonis was Tony’s go-to cybersecurity solution in 2015, and why it remains his top pick to this day.

> “When it comes to ease of use, data classification, monitoring files and permissions, or pulling all of that data together—no other solution can hold a candle to Varonis,” he says.
>
> “I know all the major players, and no one else gives you the same level of detail, performance capabilities, or the breadth of extra knowledge,” he concludes.

Don’t let a single security threat slip by unnoticed.

Varonis helps you keep your data safe, remain compliant, and detect potential threats before they turn into major problems.

REQUEST A DEMO