VARONIS

How Varonis Helps a U.S. City Protect Its Network From Ransomware and Insider Threats

> Varonis saves us time, energy, and money. It helps us prevent potentially catastrophic events and it saves us at least a year's worth of work from a full-time employee. No matter how big or small your security team, Varonis is definitely worth it.

About this case study:

Our customer is a U.S. city with over 1,000 employees. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

+ Stopping an insider threat before a data breach occurred
+ Protecting the city from ransomware and data loss
+ Preventing future attacks that put government data at risk

Solution

The Varonis Data Security Platform:

+ Provides visibility and control across all enterprise data
+ Discovers and protects sensitive data in the cloud and on-prem
+ Proactively reduces sensitive data exposure
+ Offers real-time behavior-based alerts on potential threats

Results

+ Classified and locked down sensitive data
+ Gained visibility into who has access to data and where it's exposed
+ Reduced time to detect, investigate, and respond to security incidents

CHALLENGES

Preventing a data breach from an insider threat

A CSO at a large U.S. city had a new email — an automated Varonis alert — because something suspicious was afoot.

An unauthorized user was accessing security tools:

> **"It was actually an insider threat. They were using security tools they shouldn't have been able to access, and running them from a server that they shouldn't have been running them from."**

It was a nightmare scenario for the CSO — and a big motivator behind their decision to purchase Varonis in the first place.

> **"You hear all these stories about city governments and businesses being compromised or getting hit by ransomware with impacts of millions of dollars.**
>
> **We knew we needed an automated response to mitigate risk. That's why we chose Varonis."**

The alert showed the CSO that the user had started making a number of suspicious changes to the environment, including giving an unauthorized user group the power to edit information in Active Directory.

> **Left unchecked, they would have unlimited power to create new users, delete existing users, and change permissions.**

With Varonis, the CSO saw the threat unfolding in real-time and he was able to stop the threat before it turned into a data breach.

SOLUTION

Data protection + threat detection and response

Varonis played a key role in alerting the CSO by helping them investigate the threat, and enabling them to take steps to mitigate risk to the government's environment. Varonis automatically:

+ Monitors files and email activity on the government's core data sources and authentication events in Active Directory. It provides at-a-glance insight into who does what and who should have access to critical data.
+ Identifies sensitive data, like PII, PCI, personnel records and other sensitive information. The CSO can prioritize risk remediation by limiting access to sensitive data, moving it to more secure locations, and enforcing stricter compliance policies.
+ Understands what normal user activity looks like in the government's environment, and then alerts the CSO when it detects anomalous behavior. Dashboard makes it easy to drill into potential threats, trace them to their source, and take quick action.
+ Analyzes perimeter activity from VPN, DNS, and web proxies to catch data exfiltration attempts.

> **"What we find the most value in is ransomware protection. Varonis helps us a lot with things like locking down open access and giving us all the information we need in a single pane of glass.**
>
> **I sleep better knowing that even if an attack does happen, we have the ability to stop it almost immediately."**

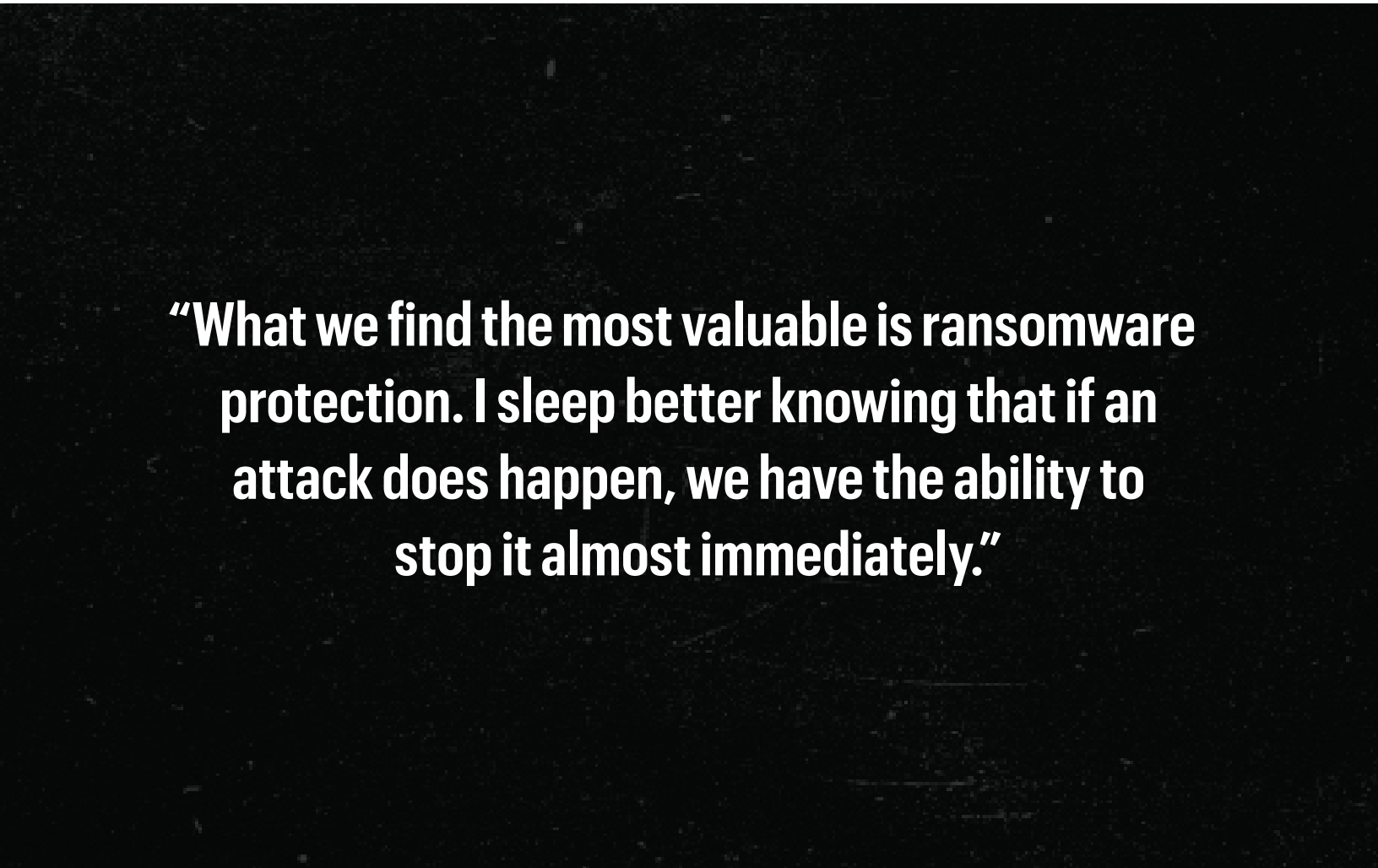
Varonis identified admin accounts with SPN (Service Principal Name) that should not be used as a service account. It also caught the permissions being added to the root of the domain. Follow-up investigations revealed that the threat was benign. The user had made a serious, but not malicious, misconfiguration.

> **"The Varonis alert contained all of the information: Threat details, possible causes, what to do about it, and who to contact."**

In a different scenario, Varonis would have helped safely restore deleted data, re-enable circumvented security measures, and help detect newly-introduced malware should any of those things be needed. Fortunately, in this case, it wasn't necessary.

The larger priority was correcting the vulnerability that the threat had revealed. Varonis made remediation easy.

> **"Auditing our AD schema to see what permissions people had was on the to-do list, but it wasn't a priority before the alert. Varonis helped us limit the permissions to files and limit who could access what and how often. It helped us be more proactive."**



“It was actually an insider threat. They were using security tools they shouldn’t have been able to access, and running them from a server that they shouldn’t have been running them from.”

RESULTS

Protection against data loss

The public sector — especially government offices — have a lot of critical data in their environments and must ensure systems stay online to serve constituents.

With Varonis, the city can take precautions to protect its network from ransomware, insider threats, and data loss. Varonis enables them to proactively and continuously assess risk to data in the cloud and on-premises — and take action to reduce that risk.

Thanks to Varonis, they clearly see who has access to sensitive data and where it's exposed to the wrong people.

> **"Social security numbers, credit cards, personal information... you really don't want that out there. Varonis helps us lock it down."**

They've gained critical alerting on potentially malicious behavior in real-time and minimized the time to detect, investigate, and respond to the most important security incidents

> **"The alert dashboard saves me tons of time. We probably get 600,000 events, but Varonis helped me tune it so that I only need to look at around a dozen events each week."**

According to the CSO, Varonis' value is immeasurable. It's already saved the government time and money, and it has helped prevent more than one potential data breach.

> **"Varonis saves us time, energy, and money. It helps us prevent potentially catastrophic events and it saves us at least a year's worth of work from a full-time person.**
>
> **No matter how big or small your security team is, Varonis is definitely worth it."**

Your Data. Our Mission.

Varonis protects your data wherever it lives, across multi-cloud, SaaS, IaaS, and on-prem.

Request a demo