VARONIS CASE STUDY:
City of San Diego

The City of SAN DIEGO

"In the last year, we've gone from averaging five ransomware attacks a month to now around 10-15 times a day – all because someone clicks on something they shouldn't have...Varonis DatAlert helps us to identify and stop these breaches."

-- Gary Hayslip, Deputy Director, Chief Information Security Officer at City of San Diego

THE CUSTOMER

Location: San Diego, California

Products: Data Classification Framework, DatAdvantage for Windows and Directory Services and DatAlert

Industry: Government

With its great weather, miles of sandy beaches, and major attractions, San Diego is known worldwide as one of the best tourist destinations. San Diego is also a location for cutting-edge businesses for telecommunications, biotechnology, software, electronics, and other major industries.

THE CHALLENGE

The City of San Diego needed to find a way to address hundreds of thousands of daily cybersecurity threats.

Gary Hayslip, hired by the City of San Diego as its first CISO in 2013, has been involved with cybersecurity for nearly 30 years and co-authored the book, *"The CISO Desk Reference Guide."* In his current role, he is responsible for the development and implementation of the city's information security strategies, policies, procedures and internal controls. For a city of more than 1.3 million people, Hayslip advises the city's executive leadership and protects a network that blocks about half a million cyber-attacks a day.

After a careful evaluation, the City of San Diego chose to implement the data security platform from Varonis, which includes Data Classification Framework, DatAdvantage for Windows and Directory Services and DatAlert solutions.

Hayslip said, *"The more I began to examine the cybersecurity landscape, the more I realized that the traditional perimeter security strategy was inadequate for the threats we currently face today. In my present enterprise environment, we don't have one network. We have 24 networks, with about 40,000 endpoints spread across the county, and we have employees on mobile devices like smart phones and laptops in the field. It's this disparate view that brought me to the conclusion I needed to move security from the edge down to the data level, where my data flows are at, and actually start tracking who's accessing it and what's being done with it."*

RANSOMWARE

Hayslip continued, *"We have 14,000 desktops, in everything from police cars to trash trucks, sitting in city buildings or laptops out in the field, and they get phishing emails. In the last year, we've gone from averaging five ransomware attacks a month to now around 10-15 times a day – all because someone clicks on something they shouldn't have. The growth in malicious activity is largely due to the fact that ransomware makes cyber criminals money. Varonis DatAlert helps us to identify and stop these breaches. It helps us better understand if the ransomware was successful and whether it reached any of our share drives. We need this context so we can respond quickly and stop it from expanding and destroying folders."*

DATA SECURITY AND LIFECYCLE GOVERNANCE

"We process everything from credit card payments to trading municipal bonds. There are several different regulatory verticals that our data, accounts and business practices fall into and I wanted to build a data security platform to look at all the various types of data the city has, who is accessing it and the practices we have for processing it. Varonis is that platform for us."

Hayslip added, *"As we started using Varonis, particularly the Data Classification Framework and DatAdvantage for auditing and protection, we were able to see data that was stale and hadn't been touched in years. The interesting thing about cities is that if a technology works they will keep that technology and its data forever. Unfortunately, that can mean cities won't innovate and try a new technology unless the old one breaks or they are forced to change. Currently, we estimate we have more than five petabytes of data – copies of copies of copies of copies. We estimate that we can probably reduce that amount by about 30% through understanding how our data is used and identifying what we truly need for operations. One of the most valuable things that Varonis has been able to do for us is to identify stale data that isn't needed for business operations. We're able to store it in less expensive facilities and remove unnecessary duplicates, freeing up a lot of critical space and saving money."*

Varonis Risk Assessments quickly show you where your most vulnerable data is stored, who is accessing it, and what needs to be done to secure it. Find out more here.

About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis empowers enterprises to stop ransomware in its tracks, discover where sensitive data is overexposed, prioritize vulnerable and stale data, and lock it down without interrupting business. Varonis builds context around the content of data and activity; automates threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning; and monitors critical assets for suspicious activity, including unusual access to sensitive data, abnormal user behavior and file activity to protect against potential exploitation.

All Varonis products are free to try for 30 days.

Our systems engineering team will get you up and running in no time.

Fast and hassle free

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis - with concrete steps to improve your data security.

Fix real security issues

We'll help you fix real production security issues and build a risk report based on your data.

Non-intrusive

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

START YOUR FREE TRIAL