

Dunn Lumber Reduces Time to Resolve Security Incidents and Improves PCI-DSS Compliance with Rubrik Sonar



INDUSTRY:

Retail

RESULTS

- Significantly faster time to resolution during a security incident
- Avoided potential PCI-DSS fine violations by identifying credit card information in unauthorized locations
- Lower cyber insurance premiums
- Streamlining audits by proving how sensitive information is managed to auditors

THE CHALLENGE

- Blind spots on high risks within sensitive data on internal servers
- Manual data discovery processes are time-consuming and complex
- Legacy solutions are costly and tax production infrastructure

Dunn Lumber services the Greater Seattle area with building materials and hardware for consumers, contractors, and home builders. Family owned and operated for over a hundred years, Dunn Lumber offers a personalized customer experience with a focus on exceptional quality and service. It has over 400 employees across its nine locations.

As a retail organization, data governance is a top business priority to ensure customers' financial data is protected and Payment Card Industry Data Security Standard (PCI-DSS) compliance is met. Tyler Banken, Director of Information Technology at Dunn Lumber, is responsible for all aspects of technology services, including data security and compliance. "Given the rise of security threats, there is an increased focus on how we secure and manage financial and personally identifiable information (PII). Our greatest risk is our own employees unknowingly providing user credentials to a bad actor. By identifying and removing sensitive data no longer needed for business operations, we decrease our risk of a potential breach," said Banken.

INVESTIGATING AND RESOLVING A POTENTIAL DATA BREACH DURING COVID-19

"At the start of COVID-19, several of our employees began receiving notices about unemployment claims from the State of Washington. The emails contained very sensitive personal information, such as compensation details and social security numbers. However, these employees were not terminated, and thus, were fraudulent. We initially thought a third party obtained unauthorized access to our information and immediately began investigating the incident with Sonar," said Banken.

"We used Sonar to run a custom search in order to identify which documents had contents that matched the sensitive information in those emails. As a result, we were able to narrow down the results to a single document. Next steps included conducting an audit trail of who had access and tracing file movement. Ultimately, we found there was no data breach on our end, and no one had gained unauthorized access to our systems. In fact, the State of Washington already had that sensitive information due to unemployment reporting, and the state was experiencing nearly \$650 million in unemployment fraud from bad actors at the time," stated Banken.

While Dunn Lumber did not have a data breach, this incident demonstrated how their team leveraged Sonar to automate data discovery processes at speed and scale. Banken stated, "The custom scan across our environment only took about an hour to complete. The entire investigation for this incident was a week and a half. Without Sonar, it would have been nearly impossible to locate the single file at the root cause and could have taken days to weeks more to resolve. This is an example of how Sonar

helps automate manual processes and significantly reduces the time to resolution for potential security incidents.”

MANAGING FINANCIAL DATA TO MEET PCI-DSS COMPLIANCE

A major compliance requirement for retail organizations, such as Dunn Lumber, is PCI-DSS to ensure companies process and manage credit card information securely. Non-compliance can result in penalties ranging from \$5,000 to \$100,000 per month.

“For PCI-DSS compliance, we must ensure no credit card data is stored on-premises, and anything we store is tokenized. Previously, we were very focused on data loss prevention at the perimeter. However, we had a blind spot on potential risks within human-generated data stored internally on our servers,” explained Banken. “Prior to Rubrik, we had no way of identifying those risks. Now, if there is a business reason to keep that data, we can find a secure solution, such as moving it to an encrypted folder.”

When Banken and team first ran Sonar across their unstructured data, they were able to immediately identify files containing sensitive information in unauthorized locations. “From an initial scan, we saw thousands of documents that could be deleted. For others, we were able to contact the business owner and remove sensitive information that could pose a risk. We did identify credit card numbers in folders where they should not be. That could put us at risk for PCI-DSS fine

violations. However, we could now quickly delete unnecessary financial data and educate individuals on proper policies without putting us at risk for potential fines,” said Banken.

Additional benefits include:

- **Lower cyber insurance premiums:** “Our cyber insurance provider asks what sensitive data we store on-premises. Due to Sonar, we can show how we are managing sensitive data and what mitigating factors are in place. This can help us lower our cyber security insurance costs since that sensitive information is not readily available to bad actors.”
- **Streamlined audit process:** “Those processes are typically very challenging, requiring us to answer hundreds of questions. Sonar will help us prove to auditors what sensitive information resides on our servers, how we are tracking it, and what mitigating steps we have taken to limit unauthorized access,” stated Banken.
- **No production impact or additional infrastructure:** “Other solutions tax our production infrastructure or are expensive. Sonar is built to run on our existing backup infrastructure with zero production impact.”
- **Up and running in less than 30 minutes:** “The setup is incredibly simple. We simply selected from the pre-built policies and started scanning. When needed, it is very easy to build custom policies and searches as well.”



Global HQ

1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter. © 2020 Rubrik. Rubrik is a registered trademark of Rubrik, Inc. Other marks may be trademarks of their respective owners.