snowflake®

CUSTOMER CASE STUDY

CSAA'S DATA-DRIVEN SECURITY TRANSFORMATION WITH SNOWFLAKE

INSURANCE

CSAA Insurance Group, a AAA Insurer

COMPANY CSAA Insurance Group
LOCATION Glendale, AZ

CSAA Insurance Group, a AAA insurer, offers automobile, homeowners, and other personal lines of insurance to AAA members through AAA clubs in 23 states and the District of Columbia. Founded in 1914, CSAA is one of the top personal lines property casualty insurance groups in the United States, according to the National Association of Insurance Commissioners.

CHALLENGE:

Lack of visibility into security metrics and controls

The security organization at CSAA Insurance Group set strengthening controls and reducing risk as top priorities. For Chief Information Security Officer Marlys Rodgers, that meant quantifying the organization's security posture and its improvement over time.

Rodgers wanted to focus on projects that would best reduce the frequency and impact of security incidents and ensure that CSAA identified and expanded successful initiatives that prevented breaches.

According to a recent study, most companies' cybersecurity efforts lag behind their embrace of data analytics. Only one in five respondents reported that their company used security analytics. This finding supports anecdotal evidence that companies rely on slide decks and spreadsheets to track security metrics monthly or quarterly.

But embracing a data-driven approach has been challenging for many organizations. Security data is often split across many solutions and data stores. Identity and access management, endpoint detection and response, and cloud security posture management data sets are large and complex. As a result, key risk indicators (KRIs) have not been broadly established or tracked, and there are few common best practices around data-driven security.

As a dynamic and increasingly cloud-centric company, CSAA wanted to do better.

SOLUTION:

Using Snowflake for security analytics

CSAA was already using Snowflake as its foundation for data analytics, and Rodgers realized that Snowflake could help CSAA address its security challenges. Through its scalability, flexibility, and cost-effectiveness, Snowflake has helped CSAA's security program achieve a unified source of truth for security analytics.

Brian Kindred, Director of CSAA's Cybersecurity Strategy and Threat Management group, uses standard BI tools to bridge the gap between the cybersecurity team and other CSAA teams, report on KRIs, and foster collaboration with CSAA's Enterprise Data Hub (EDH) team (see Figure 1). Rodgers said, "Before, the challenge was getting to the security data. But with Snowflake, all of our data is centralized, and we can establish KRI metrics that matter to leadership."

The time-intensive tasks of gathering evidence for audits and reviews have been replaced by streaming data pipelines that constantly record activity and configuration events. Reports and metrics provide an up-to-date picture of the environment, and asset details and user records are centralized for a complete 360-degree view.

As CSAA continues to increase its data savviness, cybersecurity analysts are increasingly collaborating with data analysts and engineers. According to Kindred, "We are able to glean expertise from each other. It's a very fruitful collaboration. The data team is given access to security data. They go through and analyze the fields, teach us how to measure and calculate, and put it into Snowflake. They're a great fit. You're not going to typically find data analysts that know the security world. This is changing the cybersecurity industry, and we can see many companies having a data science team dedicated to security one day. The partnership between the cybersecurity team and the EDH team has been the key to success, leveraging their expertise, skills, and data analytics processes, enabling a faster transition to the needed security data insights."

> **"Snowflake has transformed the way we view and address security risks. Our near real-time risk reporting drives prioritization and focus. You can't argue with facts that are backed by data."**
>
> **—MARLYS RODGERS,** CISO, CSAA Insurance Group

DOMAIN	KEY RISK INDICATOR	DESCRIPTION
Identify	% of High Risk Findings that have Remediation Plans within SLA (30 Days)	Measures risk reduction remediation efforts and provides insight on risks with no identified plan for closure.
	# of New High Risk Information Security Findings	Measures high risks introduced and identified within the environment and provides insight into new potential high risks for security that may become incidents in the future.
	# of overdue high risk findings	Measures the # of findings that have gone past the remediation anticipated date and provides insights into delayed high risk remediation that may result in future incidents.
	# of approved high risk exceptions with expired target dates	Measures the # of security risks with expired exceptions and outlines expired exceptions that may indicate potential failures in the future/risk impacts.
	# of unknown assets with discovered vulnerabilities	Measures the # of missing CM DB Configuration Item (CI) records for assets with known vulnerabilities. Assets without owners may be unmanaged and increase risk for security vulnerabilities.
Protect	% of New Hire security awareness training completed on-time	Measures new hire training and completion of the training for both employees and contractors in rolling fashion, month over month.
	% of users responded (Clicked) to Phishing Assessments	Measures the associated risk of users clicking on phishing attempts. Increase in phishing campaign failures may indicate risk for real phishing clicks.
	% Certification Completion On-Time by Month	Measures the certification of access across the organization. Access certification delayed can mean people have access to systems they no longer need to have access to creating increased risk.
	% Privileged Certification Completion On-Time by Month	Measures the certification of access across the organization for privileged certification. Privileged access certification delays can lead to unnecessary risk.
	% of High Application Security Pre-Production Defects Discovered Per Month	Measures the % of security defects overall that are detected each month in the development pipeline. An increase in discovered issues may be indicative of the lack of security knowledge, prioritization or other risks in development efforts.
	% of High & Critical Application Production Security Defects	Measures the # of application security defects in production. Increase means increased risk for future security incidents.
	# of Applications Released Not Test	Measures the # of application updates released into production without security testing performed. Any non-tested applications means an future increase of risk for untested apps.
Detect	# of High/critical active vulnerability (CVSS7+) non-compliant per month	Measures the # of critical and high vulnerabilities per month. Any critical/high vulnerability in the environment can result in an incident - an increase is a risk.
	% of systems with endpoint protection coverage	Measures the % of endpoint protection (malware) installation across workstations and servers. Missing installations create increased risk with missing coverage for the endpoint security.
Respond	Meant time to detect cybersecurity incidents	Measures the time it takes to discover a potential security incident.
Recover	Meant time to resolve from cybersecurity incidents	Measures the time it takes to resolve a potential security incident.

Figure 1: Examples of KRIs implemented on Snowflake

RESULTS:

Real data driving strategic prioritization and focus

Data analytics provide better visibility into security risks and lay the foundation for action. Rodgers established committees that became responsible for keeping the reported risk levels in line with business requirements, giving them a greater investment in the company's security.

CSAA uses Power BI visualizations to report on data from Snowflake in the form of dashboards, where regular reviews against its thresholds spawn actions that are tracked through findings (see Figure 2A–Figure 2F). "We can go and immediately start mitigating these overdue high-risk findings. Our near real-time risk reporting is not just telling us where risks are; it's empowering us to make better decisions for the company," said Rodgers.

Reduced manual research for audits has further accelerated the security organization's digital transformation. With a unified source of truth in Snowflake's Data Cloud, CSAA can easily show auditors the proof they need. As Rodgers described it, "The time and energy it takes to track down information can be exhausting. We've had huge improvements in year-over-year auditing reports. That's a huge selling point by itself."

> **"It's not just managing security risks. It's also the time you're spending to manage the risk, because spending too much time is a form of risk itself. Snowflake is a key piece to helping us be more judicious with our time."**
>
> **—MARLYS RODGERS,** CISO, CSAA Insurance Group

Having access to interactive dashboards and scorecards creates an accountability model that empowers stakeholders. According to Kindred, "Put these security risk dashboards in front of people, and they know what they need to do." For example, Kindred's team now works with teams to build in security rather than adding it at the end. "One of my colleagues says that the visibility into risks has created a culture of accountability and responsibility to do better from the beginning," said Kindred.

Power BI dashboards
[Demonstrations purposes only. Graphs include mock data.]

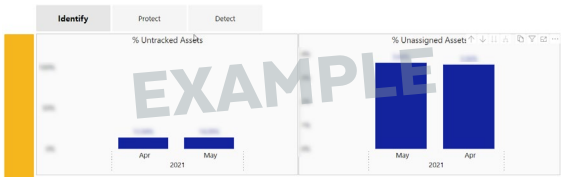

Figure 2A: Asset Inventory Metrics

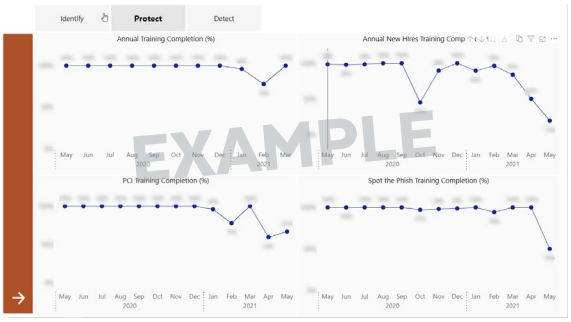

Figure 2B: Security Awareness Training Metrics

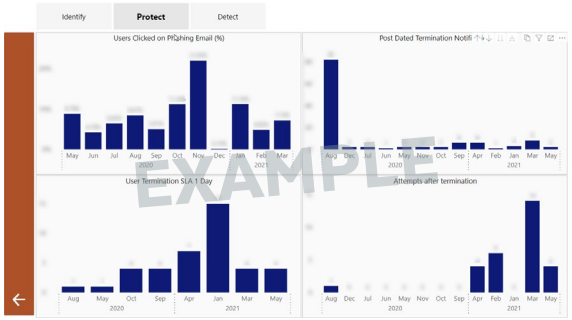

Figure 2C: Deprovisioning Terminated Employee Metrics

Figure 2D: Endpoint Security Metrics

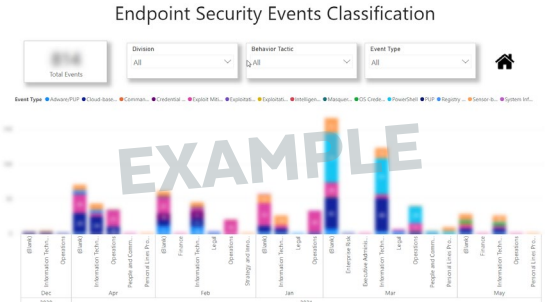

Figure 2E: Threat and Target Statistics

Figure 2F: Vulnerability Management Metrics

FUTURE:

Further reducing risks by combining data in new ways

Rodgers and her team will continue to expand their source of truth in Snowflake to cover additional data sets and new metrics. The goal is to help CSAA make better informed risk decisions as a business. The opportunity, as Rodgers described it, "is where looking at different combinations of data and indicators will help reveal new insights of how we look at security risks. New business processes constantly arise, and having a solution like Snowflake allows us to continually evolve our process to contextualize and decrease risk through data."