Query.ai

Case Study

Absolute Visibility And Swift Investigations Across 60 Tools—From One Console

AUTHENTICID

Overview

Run by a "who's who" in the global fight against fraud, AuthenticID provides a disruptive and cutting-edge, AI-driven solution that accurately and securely reproduces real-world identity verification. Their technology enables companies to be assured of who they are conducting business with, strengthens underwriting, reduces losses associated with fraud, and streamlines onerous customer onboarding procedures. For AuthenticID, providing a leading solution also means applying rigorous security practices to every part of the business—from product development to managing security operations.

Situation

As a cybersecurity company, AuthenticID holds itself to the highest standards. Even at the early stages of making its fraud prevention and identity verification platform publicly available, AuthenticID significantly invested in compliance by securing its ISO 27001 and SOC 2 Type 2 compliance attestations.

When AuthenticID's COO & CISO, Chris Borkenhagen, joined the organization in 2020, his first priority was to conduct a security gap analysis. He needed to assess whether the company had sufficient controls in place and identify opportunities for improvement. Because AuthenticID had already received its compliance attestations, the path was a lot easier for Borkenhagen to narrow in on his most important initiatives: to get holistic visibility into the company's security posture and build efficiency into its investigation process.

At a glance

Industry
Cybersecurity company

Environment
On-premises corporate infrastructure; cloud service provider hosting the company's SaaS product offering

Challenges

- Incomplete visibility of the company's environment made it difficult to assess the company's security posture
- Time consuming, manual investigation process across 60 tools, impeding fast, proactive response to alerts

Solution
Query.AI security investigations platform

Results

- Gained holistic visibility across cloud and corporate environments from one console, without needing to duplicate or centralize data
- Increased speed and efficiency in managing investigations across 60+ tools from a single solution
- Empowered team with unified search across all security tools, without having to become an expert in each one
- Simplified ISO 27001 audit process, saving staff time and enabling re-certification in three weeks

"My top objective was to gain end-to-end observability and insights from our disparate and siloed security tools in an easier and more proactive way. Our team was, essentially, in a reactive mode looking individually at 60 technologies to surface answers for security investigations," said Borkenhagen. "Purely measuring cyber resiliency based on the labor needed to look at 60 tools and do the deep security analysis, we weren't set up for success."

Solution

To gain real-time, centralized access to decentralized data and the ability to more quickly, accurately, and cost-effectively address security threats across the company's cloud and on-premises corporate environments, Borkenhagen turned to Query.AI.

The Query.AI platform enabled AuthenticID to adopt a single, browser-based technology that accomplishes the security operations goal of timely and holistic visibility, and the powerful search capabilities to handle daily investigations.

The team can now ask a single investigation question and receive the relevant details back from across its security ecosystem. With the platform's flexible search capabilities, each team member can ask investigation questions using their preferred method: text, natural language, unified query language, or any tool's specific syntax.

"Running security investigations and the ability to respond quickly can take a lot of time and labor, which is costly," said Borkenhagen. "Query.AI provides us with cross-platform environment visibility and the ability to do event management to search and act on security logs across that entire spectrum. Query.AI gives us that winning combination."

Outcomes

Gained holistic visibility of the decentralized environment, without centralizing data

One of the biggest values AuthenticID has gained since adopting Query.AI is total environment visibility and transparency through a single console, without requiring the uplift of duplicating or centralizing the data.

The platform accesses AuthenticID's data in its native location to provide centralized insights. Now, when there's an alert or potentially suspicious activity, a security team member can view all of the relevant information about the environment from one place, and more quickly take action.

"Query.AI gives us a 365-pane-of-glass. It's immensely valuable to see everything in our multi-complex environment through a central console. I can't even put numbers on it," said Borkenhagen.

Significantly increased investigations speed and efficiency

The security team's investigations and incident response playbooks are now optimized for speed and efficiency. An investigation that used to require multiple steps to manually log in and search in many of the company's 60+ tools can now be done in minutes with a single, real-time search across all tools.

"Query.AI is our solution-of-choice for centralized observability and incident management. The broad-based ability to access, investigate, and respond to what's happening in every one of our core environments through a single console gives us speed and efficiency. Our ability to identify, react, and quarantine is significantly faster, and as a result, more cost effective," said Borkenhagen.

Empowered team with simplified search from a "single-source-of-truth"

AuthenticID now has a single access point to dive into the information they need. "Query.AI makes it easy to nurture our analysts and engineers into a single environment, knowing that they're all feeding and extracting data from the same 'source of truth'," said Borkenhagen.

Borkenhagen now has a strategic, analyst-enabling solution that helps make his team more efficient, more quickly. "The platform's unified query language is the winning ticket. It's easy to learn how to use Query.AI, just one solution, that lets us access and investigate on every platform technology we have," said Borkenhagen. "Query.AI lets us put the power of our security tools in our team's hands, without having to train and get them comfortable on each and every one of those systems."

Accelerated ISO 27001 annual audit

The ISO 27001 and SOC 2, type 2 certifications are important to AuthenticID and enable the company to convey that it is a brand of the highest caliber, one that keeps security top of mind in all of its business practices and decisions.

> "Query.AI is our solution-of-choice for centralized observability and incident management. The broad-based ability to access, investigate, and respond to what's happening in every one of our core environments through a single console gives us speed and efficiency. Our ability to identify, react, and quarantine is significantly faster."
>
> **Chris Borkenhagen**
> COO & CISO
> AuthenticID

The original ISO 27001 certification took a long time, requiring the team to extract log files from every technology. This meant taking lots of screenshots, putting them into a document, and then providing detailed explanations on them.

"We navigated our ISO 27001 audit and received the re-certification in three weeks. Query.AI helped enable that tremendously. It was invaluable in streamlining and simplifying the effort," said Borkenhagen.

Getting started with Query.AI is fast and easy

1 Set Up a Meeting
Meet with us so we can get to know you and understand where you want to go.

2 Configure in Minutes
Connect our unified browser interface to your security systems via APIs.

3 See Results
Accelerate cybersecurity investigations and efficiently respond to threats.

GET STARTED

https://info.query.ai/contact-us