KATALYST

CASE STUDY

Food Manufacturer Improves Cybersecurity with Audit and Action Plan from Katalyst

150+

Actionable Results

"We now have a plan and the right team to help us do it."

Executive Summary

Cyberattacks are becoming increasingly common, and the food industry is no exception. Whether it's ransomware attackers looking for money, or malicious actors seeking to poison the food supply, food manufacturers are as much a target as anyone. Consumers trust food manufacturers to provide safe products, and any kind of attack can instantly ruin the deep trust that these companies have spent decades building. In the worst-case scenarios, this could lead to a massive public health disaster.

One North Carolina-based food manufacturer has served their customers with an immensely popular product line, becoming a household name. To maintain the trust they've earned, they understand that they need strong security measures in place to prevent any unwelcome access to their systems.

Project Goal

Proactively protect reputation as a trusted provider of high-quality food products.

The Client

The food manufacturer, based in North Carolina, has provided a line of beloved, best-selling food products across the United States for many years. During this time, they've built a trusted brand among consumers, and have grown substantially, gaining national recognition. They now supply their products to a wide range of distributors, with placement everywhere from small stores to big box retailers.

Katalyst's Role

Katalyst addresses talent shortages for IT and cybersecurity, assessing their customers' technological capacity and helping them improve. For this client, Katalyst provided a comprehensive audit of their current cybersecurity measures along with actionable recommendations for addressing risks.

The Problem: Blind Spots in Current Security Systems

The IT Director at this food manufacturing company had proactively taken steps over the years to improve their security. He spent about three years doing this: using a wide variety of cybersecurity tools, running scans, and working to implement best practices. He covered a good bit of ground on his own, but as someone who understands the importance of cybersecurity, he wanted some help identifying any blind spots that may have remained.

With this in mind, he needed a comprehensive cybersecurity audit that he could trust with the security of his company. He spent nearly a year evaluating different options, but didn't feel confident in what he was finding. All the potential partners presented him with audit plans that seemed inadequate. He wouldn't be able to rest easy with the welfare of his company in their hands. "They didn't give much confidence that they'd cover everything we needed, front to back." He knew they needed someone more capable.

Finding a Better Solution

Thankfully, in early 2022, a sales rep from Katalyst reached out. The IT Director knew him from a previous company and decided to hear him out. The sales rep connected the IT Director with Katalyst Security Consulting Engineer, Uriah Berry, for a conversation about Katalyst's approach to cybersecurity. In that conversation, the IT Director quickly realized the team at Katalyst had the expertise he had been looking for.

"They had a large list. They presented it well, and it was very comprehensive. The other companies we'd looked at weren't nearly that comprehensive. I felt confident that Katalyst could do this, and they were action-oriented... Uriah was very knowledgeable about what he'd be looking for. He could not just give results, but interpret and prioritize those results, and give a roadmap for what to work on, when." – IT Director

The Process of Partnering with Katalyst

To do the work necessary, Katalyst had to crawl through their systems, and the food manufacturer was initially concerned about giving such in-depth access.

"We had to give full access, and Uriah was very sensitive to how much access he was getting. He took all our network concerns very seriously."

They agreed to start small, with lower-stakes systems. From there, they gradually scaled up the project, scanning deeper as they worked. "It was a multi-step process, testing larger and more serious systems over time," explained the IT Director

Katalyst was sent a laptop with remote access tools to get access to the network. The IT Director was initially hesitant to enable remote registry across systems, but "nothing that was unreasonable or truly unexpected." They broke the work into phases, with Uriah working through the list, determining the access needed for each new system, and documenting everything he found as he worked through.

"Patience was required for this. It's a lot of information collected, lots of time to put it all together into a good report...but it was worth the wait."

Comprehensive, Action-Oriented Security Assistance

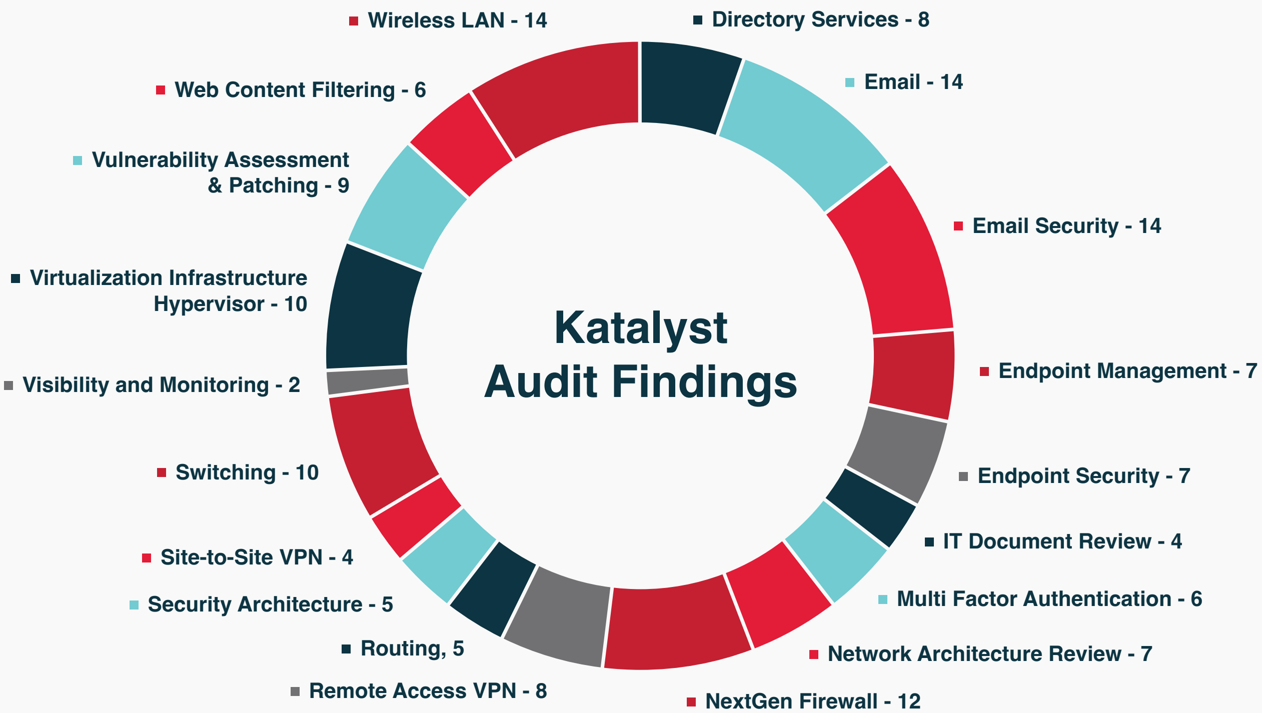
In total, the project was a three-month process. But just a month or so into it, the food manufacturer was already finding value.

The IT Director brought up concerns about email filtering and web filtering around the one-month mark, so the Katalyst team took a look. They soon discovered one of those blind spots the IT Director was concerned about: important security features that the company had access to for years hadn't been enabled. "It's a hosted system, and the host who set it up hadn't enabled those features."

Uriah suggested they consider turning these on, explaining what would happen, and why the company should do it. He "paused his current processes to walk us through improving our security right then and there." That's when the IT Director realized he'd made the right decision to work with Katalyst.

From there, Katalyst continued their work to create a comprehensive report of findings and over 150 actionable recommendations. Katalyst also provided an add-on service called a "Threat Analysis," where they used a tool to gather data for a month and then use that data to make data-driven decisions and recommendations for the company to improve its security landscape.

> "The vulnerability report was very actionable...It was a 200+ page document structured really well—easy to look at and knock things off the list. We have guidance on what we need to be doing from a security perspective. It had been harder to know what to tackle next, and what after that, and how we were going to eventually get to everything.
>
> Cybersecurity is a race, a marathon you have to keep running. [Working with Katalyst] is like having a team that's going to help you win this marathon. Instead of 'I'm going to do my best,' we now have a plan and the right team to help us do it."



The food manufacturing company plans to continue working with Katalyst in the future, with other projects in mind on their roadmap.

For others looking to get started with Katalyst, the IT Director says: “they did a great job on the security assessment, and they have very knowledgeable people. Be ready to discuss what you have, and talk through everything in depth, because they’re going to cover it all. They were very thorough, very knowledgeable, and worth the money.”

Ready to identify your organization’s cybersecurity blind spots?

Schedule a call with the Katalyst team to learn more.