CISCO
SECURE

Case Study
Cisco Public

How a wine and spirits distributor protects its data and reputation with threat hunting

"With Cisco, we have the best threat hunters in the world able to see directly into our network, use best practices in threat hunting, and correlate data based on up-to-the-minute information in the industry."

Eric J. Mandela, Assistant Director of Technology Infrastructure, Allied Beverage Group

Organization
Allied Beverage Group

Headquarters
Elizabeth, New Jersey

Users
1,000 employees
at two locations

Industry
Wine and spirits distribution

cisco SECURE

Case Study
Cisco Public

Objective

Allied Beverage Group wanted to protect endpoints against advanced and emerging threats with a solution that's easy to manage and integrates seamlessly with other security tools.

Solution

Cisco Secure Endpoint Premier

Cisco Umbrella

Cisco Secure Email

Cisco SecureX

Impact

- Prevented a ransomware attack and has avoided any breach-related downtime to date.
- Quickly and seamlessly transitioned most of its workforce to a remote environment in response to the COVID-19 pandemic.
- Overcame limited in-house resources and expertise to implement a best-in-class program for threat hunting.

Challenge

An integrated security strategy to protect against new and emerging threats

Allied Beverage Group is the largest wholesale wine and spirits distributor in New Jersey and one of the 10 largest in the United States. To transform its business for the future, Allied built a state-of-the-art facility at its headquarters in Elizabeth, New Jersey. Following the implementation of all-new IT infrastructure, the security team had to develop a new strategy from the ground up.

"We need to know that we're doing everything in our power to keep things secure. We know how advanced the attackers are, and they get more advanced and have new techniques every day," says Eric J. Mandela, Allied Beverage Group's assistant director for technology infrastructure. "We want to keep our devices, users, and company safe, so we want to lower the attack surface for any possible security breaches."

To effectively protect users, endpoints, and data against advanced threats, the team looked for a solution that integrated well with other security products. "We needed something that's easy to manage, has best-in-class security, and provides that security across the entire spectrum—from malware and ransomware to viruses, exploits, and everything else," Mandela explains. "In addition, it had to be cost-effective and within budget, while protecting against all the new and emerging threats."

> "We want to keep our devices, users, and company safe, so we want to lower the attack surface for any possible security breaches."
>
> Eric J. Mandela
> Assistant Director of Technology Infrastructure at Allied Beverage Group

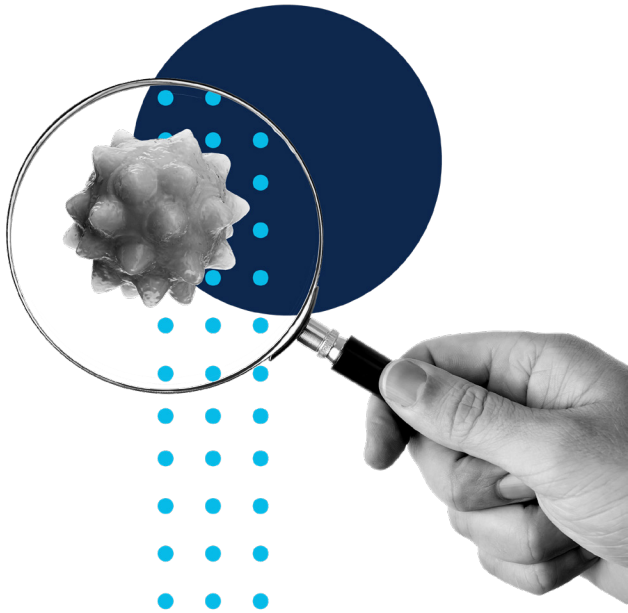
Solution

Tapping into the expertise of the world's best threat hunters

After evaluating a variety of options, the Allied team felt Cisco's suite of security products "really fit the bill," according to Joseph Rodriguez, Allied Beverage's manager of infrastructure operations. The company chose Cisco Secure Endpoint for its capabilities to detect and respond to threats faster and more effectively thanks to integration with other security solutions such as Cisco Umbrella, Cisco Secure Email, and AnyConnect.

"We want really deep integration between all these products so that we can have a single pane of glass, and we use the SecureX portal to understand what's important to look at on any given day," Mandela says. "Cisco offers all these different elements of the overall security solution and the overall network solution, which makes integration so much easier—with the click of one button."

Early on, Allied understood the importance of uncovering hidden threats across multiple control points. However, the small security team had limited resources and staff hours. When Cisco introduced the Secure Endpoint Premier tier—which includes SecureX Threat Hunting—Allied saw an opportunity to access some of the world's most-elite threat hunters and best threat intelligence.



> "Cisco offers all these different elements of the overall security solution and the overall network solution, which makes integration so much easier—with the click of one button."
>
> Eric J. Mandela
> Assistant Director of Technology Infrastructure at Allied Beverage Group

"Since we don't have a person looking at threats 24 hours a day on our own staff, having a partner like Cisco is very valuable. Additionally, even if you had somebody on staff who's a great threat hunter, there's a possibility that they might miss something," Mandela says. "With Cisco, we have the best threat hunters in the world able to see directly into our network, use best practices in threat hunting, and correlate data based on up-to-the-minute information in the industry."

One of the key benefits of the threat hunting console is the unified visibility that Allied can use to uncover threats faster across the attack surface. The console provides a wider overview of the scope or impact of an incident—a capability Allied didn't have in the past.

"The console allows us to see where else in the network a threat may have touched and then to investigate those other endpoints or areas," Rodriguez says. "It gives us detailed information about files that may have been compromised, sites that these individuals have visited, sites that may be communicating back and forth with the endpoints, and what endpoints are affected."

Mandela notes that Allied has the duty to ensure that its data, networks, and systems are as secure as possible. "And any kind of additional set of eyes that we can put on our network, especially someone as renowned as Cisco Talos, is really valuable. To have those experts be able to query all our devices and catch the things that we might miss—this kind of capability gives us extra peace of mind."

Results

A partner who's always there to protect company data and reputation

Partnering with Cisco for managed threat hunting gives the security team confidence that they have "an extra set of eyes" to detect threats. Allied saw immediate results—even though SecureX Threat Hunting was still in beta testing—when the Cisco team discovered the beginning of a ransomware attack and facilitated a quick response.

When Cisco detects a threat, customers receive a notification that includes context, impacted targets, and remediation guidance. During this particular incident, Allied had initially remediated a threat after seeing a high-priority alert in the Secure Endpoint console. But the next day, a Cisco threat hunter called to notify Allied that this was part of an infiltration attempt. A threat actor was trying to establish privilege access in preparation for launching a bigger attack.

"This is something that could've become a major disaster, but Cisco advised us to immediately wipe that computer completely," Mandela says. "If we didn't get the threat hunting alert, we might have thought that it was not that serious or that the threat was completely eliminated—and the attacker could've still been able to leverage that machine."

Mandela especially likes that Secure Endpoint uses different engines and methods to protect endpoints. He notes that calculating return on investment (ROI) of a security solution can be difficult because "you never know what you prevented," but the value of Secure Endpoint became obvious during the pandemic.

"This is something that could've become a major disaster, but Cisco advised us to immediately wipe that computer completely,"

Eric J. Mandela
Assistant Director of Technology Infrastructure at Allied Beverage Group

> "All vendors say that they want to be a partner with you, but I think Cisco has absolutely lived up to that. And whenever we've needed help, they've always been there."
>
> Eric J. Mandela
> Assistant Director of Technology
> Infrastructure at Allied Beverage Group

"Any ROI we needed was realized with our response to COVID-19," Mandela explains. "We had security in place on all the laptops. At a moment's notice, we were able to transition 80% of our workforce to be remote—and our company was never remote before. Because of our Cisco solutions, we were able to deploy everything and have people work well remotely with very minimal issues."

Thanks to Cisco Secure Endpoint and the integration with other Cisco security products, Allied Beverages Group hasn't had any downtime due to security breaches. Mandela says the team has peace of mind knowing Cisco helps protect not only Allied Beverage's data but also its reputation. "We don't want to be known as somebody who was hacked. We don't want to put any partners at risk if we were to have a breach," he says. "All vendors say that they want to be a partner with you, but I think Cisco has absolutely lived up to that. And whenever we've needed help, they've always been there."

For more information on the Cisco portfolio and platform approach to security, go to: cisco.com/go/secure