Global Restaurants Company Avoids Million-Dollar Losses

Around-the-clock defense successfully blocks ransomware attach

---

Thank you for downloading this Mandiant datasheet. Carahsoft serves as Mandiant's Master Government Aggregator® making the company's cyber solutions and services available to the Public Sector through Carahsoft's network of reseller partners, Solutions for Enterprise-Wide Procurement (SEWP) V, DoD Enterprise Software Initiative (DoD ESI), National Cooperative Purchasing Alliance (NCPA) and other contract vehicles.

To learn how to take the next step toward acquiring Mandiant's solutions, please check out the following resources and information:

For additional resources:
carah.io/MandiantResources

For upcoming events:
carah.io/MandiantEvents

For additional Mandiant solutions:
carah.io/MandiantSolutions

For additional Mandiant NetBackup solutions:
carah.io/MandiantNetBackup

To set up a meeting:
Mandiant@carahsoft.com
(703)-889-9710

To purchase, check out the contract vehicles available for procurement:
carah.io/MandiantContracts

CUSTOMER STORY

GLOBAL RESTAURANT COMPANY AVOIDS MILLION-DOLLAR LOSSES

Around-the-clock defense successfully blocks ransomware attack

Industry
Consumer/Leisure & Entertainment

Mandiant Managed Defense

Mandiant Expertise on Demand

Mandiant Incident Response Retainer

I can't say enough good things about Mandiant Managed Defense. We had the right people on our team when we needed them, and we have Mandiant to thank. It is TRUE Managed Defense

— **CISO**, global restaurant company

A major, global restaurant company, this U.S.-based corporation serves millions of consumers annually with a variety of fast-food and sit-down dining experiences. The organization has over 30,000 locations and a global presence in over 50 countries.

Outcomes

Avoided potential losses of millions of dollars in revenue

Detected and mitigated ransomware attack before servers could be encrypted

Acted on attack immediately—no delays while alerting internal management

Eliminated need to find and retain additional in-house security talent

When a ransomware attack emerges

The corporate information security officer (CISO) of a major global restaurant company paid close attention on the eve of the U.S. Independence Day weekend, one of the company's top weekends for revenue generation. Newly reported ransomware exploited a vulnerability in Kaseya VSA, a remote monitoring and management tool. There were no documented deployments of Kaseya on any of the restaurant company's servers. It seemed his company was safe.

Then the CISO received an alert from Mandiant.

> *The value of Mandiant Managed Defense is not just monitoring. It's containment. They don't just watch the logs; they take action if that's what's needed to protect my environment from attack. They will remove emails and quarantine servers if that is what is required.*
>
> — **CISO**, global restaurant company

Cyber risks of decentralized, heterogenous infrastructures

The restaurant company was growing rapidly via multiple acquisitions. Although it had embarked on a major initiative to consolidate and standardize its infrastructure, not all its servers were in compliance with the new standard. A handful of legacy systems used by some subsidiaries were running Kaseya.

By the time the CISO was alerted, the Mandiant team had already quarantined the at-risk servers.

Mandiant experts add powerful layer to security protections

Partnering with Mandiant is a critical element of the company's security strategy. The company uses Mandiant Managed Defense, Mandiant Expertise on Demand, and Mandiant Incident Response Retainer as part of a broader IT standardization project.

"Mandiant does more than monitor logs," the CISO said. "If needed, Mandiant takes action, whether that's deleting malware from mailboxes or shutting down servers. We never lose time because someone on my team didn't see an alert or answer a phone call."

Top-notch security talent always in place

The restaurant company's relationship with Mandiant lets the CISO focus on security strategy, instead of finding and retaining security talent. "The last thing I want to worry about during an incident is whether I have the right security resources in place," said the CISO. "With Mandiant, I don't have to. They hire the best out there, which means I have top-notch experts supporting my team."

Operations protected during high-sales weekend

Had the ransomware attack successfully encrypted the restaurant company's vulnerable servers, the impact would have been enormous. Restaurants—some of which were running targeted holiday promotions—would have had to shut down. The company would have lost millions of dollars in sales and potentially had a public relations incident to recover from.

"Our partnership with Mandiant paid off," the CISO said. "Thanks to Mandiant, I can sleep at night."

> *I can sleep at night, knowing that Mandiant is there around the clock, monitoring my infrastructure and taking action immediately if there's an issue.*
>
> — **CISO**, global restaurant company

Learn more at **www.mandiant.com**

MANDIANT