Deloitte.

A recipe for greater cyber confidence

Food service company orders up detect and respond solution as a service

MXDR by Deloitte

24/7 incident detection and response	Cloud | SaaS	Managed services | Operate	Security operations
Core need	Solution environment	Key capabilities	Function

Cyber Stories

The starting point

The call came in on a Saturday night. A large US food service company with hundreds of locations had been hit by ransomware, bringing critical back-office operations to a halt. Functions such as payroll—a vital activity for the privately held organization and its thousands of hourly employees—were thrown into chaos. Leaders needed a solution now.

On the other end of the phone line—Deloitte, whose team of incident response professionals stepped in immediately. The team got the organization back to normal operations, quickly mitigating issues, establishing a recovery plan, and bringing a renewed sense of calm to the organization.

Within a matter of days, the organization was running smoothly again, but its leaders wanted more. They wanted to prevent such a disruption from happening again—and to do it in a way that did not require the company to invest heavily in internal cyber capabilities and tools. Instead, an "always on" turnkey solution—continuously managed by someone else—sounded ideal.

Factors in focus

- ✓ A need to ensure business continuity amid ongoing cyber threats
- ✓ A desire to rely on external operate services as a solution, rather than internal talent and tools
- ✓ A focus on positioning the business to address future needs, not just a one-time disruption

The way forward

The company believed that Managed Extended Detection & Response (MXDR) by Deloitte could meet all the requirements, letting the business take advantage of managed cybersecurity services and a fully Software-as-a-Service (SaaS)-based approach to incident management. MXDR by Deloitte provides a modular set of third party, market-leading technologies for threat hunting, detection, response, and remediation, which is combined with proven processes run by an experienced cybersecurity team who proactively pursues threats and mitigates business risks.

With the majority of cyber solutions existing in a Deloitte-managed cloud environment, MXDR by Deloitte would let the company avoid creating a new security operations center, investing in on-premises solutions, or acquiring in-house cyber talent. Instead, the company could focus more on its core business, handing off responsibilities for incident detection and response capabilities to Deloitte.

Before adopting MXDR by Deloitte, company leaders wanted to know if they could leverage their recent investment in cybersecurity solutions. In asking the question, they discovered that their existing solution was less mature in its detect and respond capabilities and ranked low in analysts' ratings. They decided to accept that their existing tool was a "sunk cost" and to move forward with MXDR by Deloitte—selecting the solution based on its superior risk mitigation functionality and ability to help keep company operations running despite ongoing cyber threats.

Insights to inspire

Expect the unexpected—and realize that the first moments after a cyber event are critical. Know exactly what your first response will be and who you will turn to for help.

Be prepared to write off recent technology investments and start over with a new solution—if it can provide significantly greater value for your business.

For any digital capability, consider managed Operate services that can allow you to worry less about technology solutions and focus more on your core business.

In addition to endpoint protection, MXDR by Deloitte is providing the company with proactive threat hunting, 24×7×365 monitoring, and response and remediation—all through an integrated suite of cloud SaaS offerings managed by Deloitte specialists in cyber threat intelligence, security engineering, and operations. The solution was delivered and managed by Deloitte as both an innovation and an outcomes-based "Operate" service.

The new solution, which was deployed in a matter of days, also provides flexibility and scalability through a modular, cloud-native approach, which can expand to include insider threat, cloud security, and identity capabilities.

With a single integrated set of leading cyber technologies—provided turnkey and as a managed Operate service—the organization has boosted its cyber resiliency and confidence, with an improved ability to prevent and recover from business-disruptive events. Moreover, it better positions the company to embed continuous advantage and address future needs, including new cyber demands or business expansions.

The achievements

A single integrated set of market-leading cyber technologies, provided turnkey and operated as a service.

24×7×365 threat hunting, monitoring, incident response, and remediation.

Cyber resiliency, with an improved ability to prevent and recover from business-disruptive events.

Modular, cloud-native approach to confidently support flexibility, speed, additional cyber needs, and business growth, including mergers and acquisitions.

Let’s talk cyber

How is your organization positioning itself to address today’s and tomorrow’s cyber threats? Discover how Deloitte Operate services and Deloitte’s worldwide team of industry-focused specialists can support you every step of the way—and help you respond with confidence no matter what the future brings. Contact us to get the conversation started.

www.deloitte.com/mxdr

www.deloitte.com/cyber

Deloitte.

Contacts

Kevin Urbanowicz
Managing Director
Deloitte & Touche LLP
kurbanowicz@deloitte.com

Curt Aubley
US Cyber Detect & Respond Leader
Managing Director
Deloitte & Touche LLP
caubley@deloitte.com

Nicola Esposito
Global Cyber Detect & Respond Leader
Partner, Deloitte Spain
niesposito@deloitte.es

Chris Richter
Global Detect & Respond Product Leader
Managing Director, Deloitte Global
chrichter@deloitte.com

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.