CUSTOMER STORY

STRENGTHENING CYBERSECURITY IN THE FOOD & BEVERAGE RETAIL INDUSTRY_

> Keeping our customers' data safe is non-negotiable. With Gatewatcher, we can protect what matters most without cutting corners on service.

#SUPPLYCHAIN #CUSTOMEREXPERIENCE #NDR #RETAIL

> “ *A breach wouldn’t just have financial consequences— it would severely damage trust and brand reputation.*

01

WHAT ARE THE SPECIFIC AND UNIQUE CYBERSECURITY CHALLENGES FACED BY NATIONAL FOOD RETAIL CHAINS?

Cybersecurity in the food and beverage retail industry extends far beyond point-of-sale transactions. Our organization manages **thousands of personal records, financial transactions, and a complex digital infrastructure** that spans everything from point-of-sale systems to supply chain management platforms. With such a fragmented ecosystem, **securing every entry point** is a major challenge.

Protecting customers and financial data is a top priority. Our online ordering, loyalty programs, and retail platforms handle vast amounts of personal information and payment details, making them a target for cybercriminals. A breach wouldn’t just have financial consequences—it would severely damage trust and brand reputation.

Beyond digital risks, our **inventory management systems, third-party vendor networks, and distributed digital infrastructure** add further complexity. Whether it’s securing restaurant network access, preventing unauthorized intrusions, or ensuring compliance with food safety and data protection regulations, we must constantly adapt to evolving threats to keep our operations secure.

02

HOW DO HIGH-VOLUME PERIODS INCREASE CYBERSECURITY RISKS?

Peak periods like holidays bring a surge in digital traffic and a heightened risk of cyber threats. With millions of online orders processed across hundreds of locations—**our network must support secure payment systems, inventory tracking, and customer data management,** all while remaining resilient against potential attacks. Imagine inventory tracking systems failing during a critical shopping period—disrupted supply chains, lost revenue, and customer dissatisfaction.

A cyberattack on real-time inventory and order management could disrupt operations, compromise food safety tracking, and erode customer confidence. The national and increasingly global reach of our retail operations makes us an even bigger target. Cybercriminals may attempt to interfere with supply chain communications, overload our digital infrastructure, or exploit vulnerabilities in payment and ordering systems.

The sheer **diversity of point-of-sale** devices, mobile apps, and connected systems adds to the challenge, increasing the **risk of unauthorized access or data breaches**.

*Cyber challenges_*

Ecosystem
fragmented digital ecosystems with a need for global, consolidated coverage across point-of-sale systems, inventory management, supply chains, and loyalty programs.

Manage
the integration of diverse connected systems, including IoT devices, mobile apps, and IT/OT convergence, securely.

Mitigate
risks linked to third-party suppliers, distributed vendor networks, and vulnerabilities in the supply chain.

Ensure
continuity of operations during high-volume periods, such as holidays, while safeguarding food safety tracking and operational resilience

Safeguard
sensitive customer data, financial records, and intellectual property from cybercriminals and unauthorized access

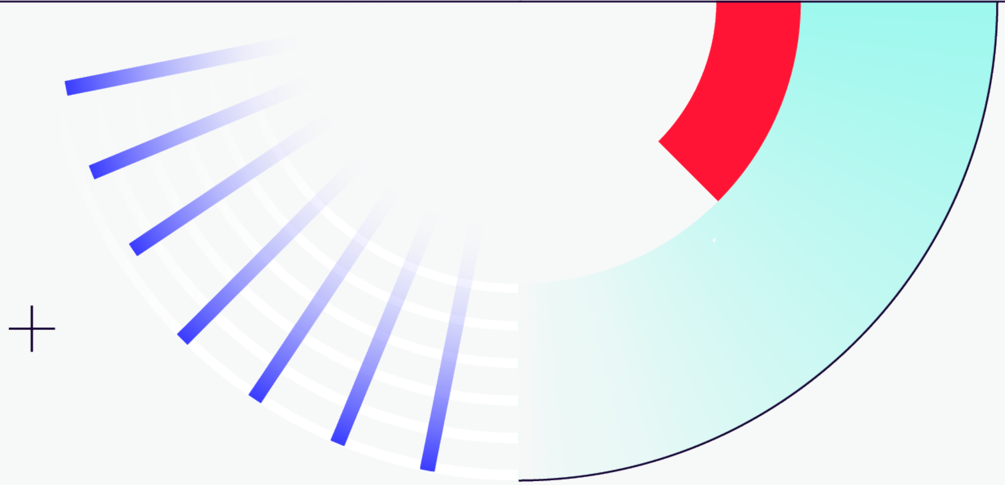
Each restaurant location, each delivery platform, and each digital touchpoint represents **a potential security vulnerability that must be continuously monitored and protected**.

03

HOW IS OUR NETWORK ARCHITECTURE STRUCTURED, AND HOW WAS THE NDR SOLUTION DEPLOYED?

Our organization operates a **segmented network, ensuring retail operations and administrative systems remain separate.** The retail network supports point-of-sale systems, inventory management, and customer-facing platforms, while the head office network handles financial transactions, internal communications, and corporate management. This separation is essential, as administrative environments are more vulnerable to cyber threats due to human factors.

When deploying Network Detection and Response (NDR), our priority was **ensuring visibility across both environments without adding complexity.** We chose the **cloud-based option of the solution** as it aligned better with our need. It directly provided centralized traffic monitoring without interfering with daily operations. This approach, leveraging our virtualized infrastructure, made **deployment and integration into our existing security framework straightforward** while allowing for easy scalability. It enabled real-time monitoring across both networks, ensuring **efficient threat detection and response.**



04

WHAT LED US TO IMPLEMENT AN NDR SOLUTION, AND HOW DOES IT INTEGRATE WITH EXISTING SECURITY TOOLS?

When we assessed our cybersecurity landscape, we realized that **the network was our biggest blind spot.** We had endpoint protection **(EDR) covering user devices and XDR securing servers and applications,** but network activity remained largely invisible. Without a way to detect anomalies in real-time, **we were vulnerable to hidden threats** moving undetected across our infrastructure. Let's be transparent, **cost was also an important factor in our decision.** Many NDR solutions come with a high price tag, often reflecting brand recognition rather than functionality.

While exploring various NDR solutions, what stood out was the agility and adaptability of Gatewatcher. Instead of forcing us into a predefined framework, **they were willing to evolve with us,** helping to address specific vulnerabilities as they emerged. For us, the priority was finding a solution that delivered real value. While some competitors turned to established vendors, **we saw an emerging leader with strong capabilities.**
For a food and beverage retail organization, security needs to be fast, seamless, and tailored to our unique environment. The NDR solution **integrates smoothly with our existing security stack,** enhancing visibility without disrupting daily operations.

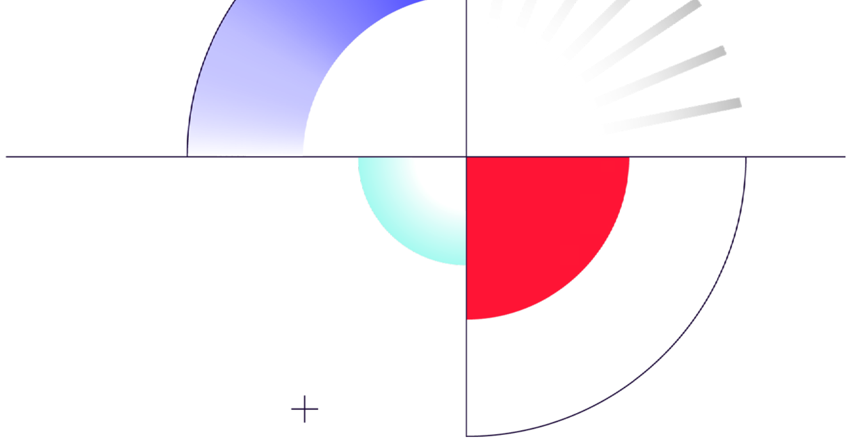
BUSINESS SECTOR
Regional Food and Beverage Retail Chain

REVENUE
> £ 1.5 billion

LOCATION
450 outlets across England, Scotland, Wales, and Northern Ireland

DIVERSE ENVIRONMENTS
Drive-thru locations, regional commissary kitchens, online ordering systems, delivery apps, etc.

GLOBAL EXPOSURE
> Ingredients from *15+ countries*,
> International logistics
> Customer data for global loyalty programs



05

WHAT WERE THE KEY BUSINESS AND OPERATIONAL METRICS YOU AIMED TO IMPROVE WHEN EVALUATING NDR SOLUTIONS LIKE GATEWATCHER?

When we evaluated Network Detection and Response technologies, **Gatewatcher emerged as a transformative solution** that fundamentally reimagined our approach to cybersecurity. Our primary objective was visibility—not just passive monitoring, but **intelligent, contextual insights that could differentiate between noise and genuine threats.** Security tools are only effective if they provide clear and actionable insights—otherwise, they generate too much noise, overwhelming teams with false positives.

The fragmented technological ecosystem of food and beverage retail creates unique cybersecurity challenges. Gatewatcher NDR platform targets **Shadow IT**—where operational units implement unauthorized technological solutions outside centralized IT governance.

In our industry, this manifests through critical scenarios: distribution centers with independent inventory systems, franchise locations using custom point-of-sale solutions, and marketing teams deploying unauthorized data collection platforms. **These technological improvisations create potential security vulnerabilities that traditional monitoring approaches cannot detect.**

By **mapping assets** and **monitoring communications** across IT and OT environments, it uncovers hidden technological endpoints. The platform transforms Shadow IT from a potential weakness into a manageable, transparent ecosystem, providing real-time visibility into technological interactions from cold storage systems to e-commerce platforms.

> “
>
> *Our primary objective was visibility—not just passive monitoring, but intelligent, contextual insights that could differentiate between noise and genuine threats.*

06

HOW DID YOU INTEGRATE GATEWATCHER INTO YOUR EXTENDED DETECTION AND RESPONSE STRATEGY?

Gatewatcher has become the cornerstone of our XDR strategy, bridging critical security domains with unprecedented sophistication. **Where traditional solutions create fragmented security silos, Gatewatcher's technology creates a unified, intelligent security ecosystem that correlates data across endpoints, cloud environments, and network infrastructures.**

The solution's ability to seamlessly integrate with **our existing security tools while providing a centralized,** comprehensive view of our digital landscape is nothing short of revolutionary. Gatewatcher **doesn't just fill security gaps**—it transforms how **we conceptualize and implement cybersecurity in a rapidly evolving digital landscape.**

> *We are not only optimizing our security infrastructure to meet today's operational needs but also proactively preparing for the risks of tomorrow.*

07

HOW DOES GATEWATCHER ALIGN WITH YOUR STRATEGIC SECURITY OBJECTIVES?

The Gatewatcher NDR solution transcended traditional security paradigms by offering a holistic approach to network protection. Their technology doesn't merely detect threats—it interprets them within the complex context of our operational landscape. By integrating advanced **AI-driven analysis,** Gatewatcher provides **a level of threat intelligence that transforms our security from a reactive defense to a proactive intelligence mechanism.**

What distinguished Gatewatcher was their commitment to creating a solution that speaks the language of our specific business environment. Their NDR tool doesn't just monitor; **it understands the intricate communication flows** between our supply chain management systems, point-of-sale platforms, and corporate infrastructure.

Gatewatcher secures point-of-sale systems and customer data, empowering retailers to tackle cyber threats **without sacrificing efficiency or service.** We're proud to support an industry built on trust and resilience.

08

HOW DOES THIS LAY GROUNDWORK FOR THE FUTURE?

As our industry continues to evolve, this partnership lays a solid foundation for future innovation in cybersecurity. **Gatewatcher's modular and flexible solutions** position us to address emerging threats while maintaining the adaptability needed for the dynamic challenges of the food and beverage retail sector.

By embracing a culture of continuous improvement, we are not only optimizing our security infrastructure to meet today's operational needs but also proactively preparing for the risks of tomorrow.

With Gatewatcher's advanced network detection technologies, we have the confidence to protect our retail operations, safeguard customer trust, and ensure the long-term security **and resilience of our industry.**

> *Gatewatcher secures point-of-sale systems and customer data, empowering retailers to tackle cyber threats without sacrificing efficiency or service. We're proud to support an industry built on trust and resilience.*

*Your benefits_*

Gatewatcher technology enables:

Securing a distributed ecosystem

Provides real-time monitoring across stores, supply chains, and online platforms.

Managing high-demand periods

Detects and neutralizes threats during peak sales, holidays, and special events.

Controlling exposure spikes

Tracks and analyzes connected devices and network interactions in-store and online.

Enhancing visibility on targeted threats

Identifies attacks exploiting vulnerabilities in payment systems, customer data, and inventory management.

Correlating security signals efficiently

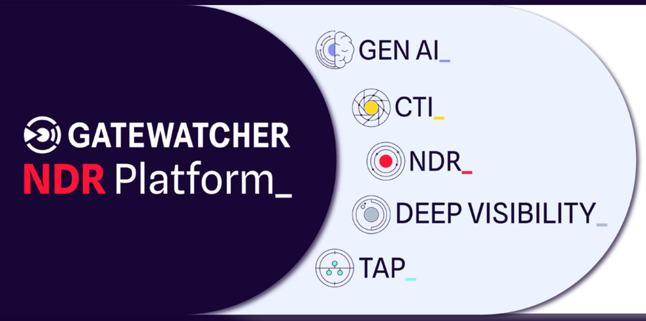
Unifies alerts across IT and operational systems for rapid threat detection.

Reducing operational disruption

Adapts to high-traffic environments without compromising service quality or performance.

Flexibility of the solution

NDR technology can be used on premise or in the cloud, depending on the level of sensitivity of the entities to be protected



Gatewatcher NDR platform offers cyber-threat mapping and behavioral analysis to ensure enhanced detection of targeted attacks, even in the case of encrypted data flow. It combines machine learning with static and dynamic analysis.

GATEWATCHER

Want to *learn more?*_

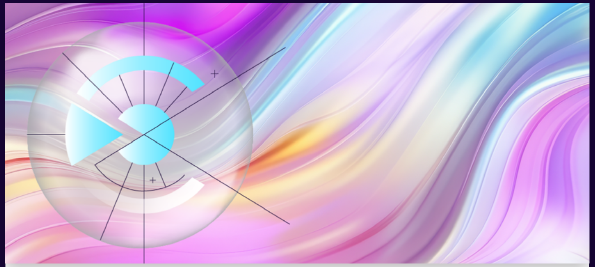
[VIDEO]
Easy as NDR:
What is the R of NDR?

NDR Insight_

The essential guide for CISO and CIO.

Why and how NDR can be an essential brick to strengthen your cyber defense system.

[GUIDE]
Discover our latest NDR Insight guide.



[USE CASE]
Safeguard Against
Supply Chain Attacks.

*Easy as_*

NDR_ CTI_ TAP_ GEN AI_ DEEP VISIBILITY_

Contact us today ⟶