Case Study

ThreatDown
Powered by Malwarebytes

Sealing the Gaps: How Contarini Leopoldo Strengthened Security at Scale

Contarini Leopoldo, a precision hydraulic cylinder manufacturer based in Italy's industrial heartland of Emilia-Romagna, operates in an environment where uptime is essential for meeting production schedules and exceeding customer expectations. With 270 employees across two locations and over 60 years of engineering expertise, the company produces custom hydraulic solutions for clients worldwide as part of the Interpump Group family.

Managing 180 client and server systems across their network, Contarini's four-person IT team oversees a complex infrastructure supporting both Windows and Linux environments. In a manufacturing setting where every endpoint connects to critical production systems, security isn't simply about protecting data—it's about ensuring operational continuity that keeps precision manufacturing lines running.

> "ThreatDown stood out as the clear winner in our evaluations. It delivered the malware detection strength we needed while dramatically reducing the management complexity that had strained our IT team in the past."
>
> **Stefano Lama, Head of IT Support**
> **Contarini Leopoldo**

When Reality Strikes

Contarini, like many industrial manufacturers, discovered a critical security gap only after facing a targeted cyberattack. "After experiencing a targeted cyber-attack, we recognized that our security infrastructure needed to evolve," said Stefano Lama, Head of IT Support at Contarini.

The breach exposed serious shortcomings in their existing endpoint protection. Their previous solution, Bitdefender, lacked centralized visibility and was cumbersome to manage—draining IT time without providing the control needed to respond quickly to modern threats.

CONTARINI

Customer-at-a-glance

Customer - Contarini Leopoldo
Industry - Manufacturing
Country - Italy
Displaced Solution - Bitdefender

ThreatDown Solutions

ThreatDown Advanced, including:

- Endpoint Detection & Response (EDR)
- Manged Detection & Response (MDR)
- Vulnerability Assessment and Patch Management

“Bitdefender was difficult to manage and didn’t provide the integrated approach we needed to stay ahead of sophisticated threats. The cyberattack made it clear: we had to both strengthen our defenses and simplify our operations,” Lama explained.

Finding the Right Partner

Instead of making a rushed decision in the wake of the cyberattack, Contarini took a deliberate and methodical approach to selecting a new security partner. Credible input from a trusted industry contact with deep expertise in anti-malware helped guide the team during this critical juncture.

Contarini evaluated three leading endpoint security vendors, including ThreatDown, against the real-world demands of their manufacturing environment. The criteria were clear: effective threat protection, simplified management, built-in support for security services like MDR.

> “The operational improvement was immediate and measurable. ThreatDown streamlined our endpoint monitoring processes and significantly accelerated our patch deployment cycles across the entire infrastructure.”
>
> **Stefano Lama, Head of IT Support**
> **Contarini Leopoldo**

Results

- **Streamlined security management** from fragmented tools to unified console
- **Improved monitoring efficiency** and faster update processes
- **24/7 expert threat hunting** and incident response coverage
- **Comprehensive operational intelligence** for IT infrastructure management
- **Reduced administrative burden** on 4-person IT team
- **Enhanced malware detection** and elimination capabilities
- **Access to specialized security expertise** without additional hiring

The company approached vendor selection systematically by testing different combinations before conducting a full head-to-head evaluation of all three options. “ThreatDown stood out as the clear winner in our evaluations. It delivered the malware detection strength we needed while dramatically reducing the management complexity that had strained our IT team in the past,” Lama shared.

Unified security management transforms daily operations

The ThreatDown implementation immediately addressed Contarini’s most pressing operational challenges. Instead of juggling multiple disconnected tools, the IT team gained an integrated platform that brought together endpoint protection, patch management, CVE tracking, and system monitoring—all within a single interface.

“The operational improvement was immediate and measurable. ThreatDown streamlined our endpoint monitoring processes and significantly accelerated our patch deployment cycles across the entire infrastructure,” said Lama, adding, “With ThreatDown’s unified console, we now have centralized oversight and control across the entire environment.”

Today, Lama’s team runs a streamlined daily routine that covers all the essentials: monitoring suspicious activity, assessing CVE impacts, managing patches, and tracking network coverage trends—without the overhead that once bogged them down. For Contarini, this operational efficiency translated into real-world impact: it frees up time for IT staff to focus on keeping production systems running smoothly.

Strategic evolution: Adding managed detection and response

After a year of success using ThreatDown, Contarini made a strategic decision to add ThreatDown's Managed Detection and Response (MDR) services. The move was a strategic expansion based on the company's need for comprehensive 24/7 coverage.

"The business case for adding MDR was compelling," Lama explained. "We had proven ThreatDown EDR's effectiveness over a full year, and the cost-to-value ratio for extending our capabilities with 24/7 expert monitoring was clearly justified."

The MDR service addressed a fundamental challenge for Contarini's small IT team: providing round-the-clock security monitoring and response capabilities without hiring additional specialized staff. "MDR strategically fills critical gaps in our security coverage. It extends both our technical expertise and our operational capacity beyond what our internal team could realistically maintain," Lama explained.

For a manufacturing company where security incidents can occur at any time, having expert-level threat hunting and response capabilities available 24/7 provides Contarini critical operational insurance. "Round-the-clock security expertise represented a critical capability gap that we couldn't realistically address with internal resources," Lama noted. "Having ThreatDown's specialized MDR team available gives us confidence that security issues will be handled by experts, regardless of when they occur."

"We had proven ThreatDown EDR's effectiveness over a full year, and the cost-to-value ratio for extending our capabilities with 24/7 expert monitoring was clearly justified."

Stefano Lama, Head of IT Support
Contarini Leopoldo

Operational intelligence: Beyond basic endpoint protection

One of the most significant advantages Contarini discovered was ThreatDown's ability to provide comprehensive operational intelligence about the company's IT infrastructure.

"ThreatDown's centralized endpoint management delivers comprehensive operational intelligence that extends far beyond basic security monitoring," Lama explained. "We gain real-time visibility into our entire IT infrastructure—user access patterns, hardware inventories, system configurations, and security status—all through a single interface."

This operational visibility has proven particularly valuable in a manufacturing setting where knowing the exact configuration and status of every endpoint can impact production planning and maintenance scheduling. "ThreatDown's data integration capabilities are outstanding. We can easily export our security and operational intelligence, which streamlines integration with our wider IT workflows and reporting processes," said Lama.

Building confidence through expert support

Beyond the technical capabilities, Contarini's experience with ThreatDown has been defined by the quality of human expertise and support they receive. "Our customer experience with ThreatDown has been exceptional across the board," Lama said. "From account management to engineering support, the team is consistently available for training, solution guidance, and rapid incident response. That level of accessibility and expertise is genuinely rare in enterprise security."

The quality of the MDR service has reinforced this positive experience. "The ThreatDown MDR team consistently demonstrates both technical competence and genuine helpfulness. It feels like we have an extension of our internal team," Lama said.

This level of vendor engagement has been particularly valuable as Contarini expands their use of ThreatDown's capabilities. "We're continuously adopting new security features as the ThreatDown platform expands," Lama noted. That momentum reflects their trust in the platform's ability to grow with their needs.

Demonstrating security value through reporting

For Contarini, ThreatDown's reporting capabilities have made it easier to communicate the value of their security investments to leadership. Detailed weekly and monthly reports go beyond threat counts—they highlight blocked attacks, patch compliance, endpoint health, and system stability, tying security performance directly to business outcomes.

"The reports clearly show the work ThreatDown is doing behind the scenes—threat prevention, system health, compliance— all in a format that makes it easy for our leadership to understand the impact of our security program," said Lama.

ThreatDown™
Powered by Malwarebytes

threatdown.com

sales@threatdown.com