

Fashion hub case study

Fashion companies, like many organizations, are highly vulnerable to a wide range of cyber threats. Given the valuable and sensitive nature of the information they handle, such as customer data, payment information, intellectual property, and supply chain details, fashion brands are lucrative targets for cybercriminals. Some of the most common cyber threats faced by the industry today include data breaches, phishing attacks, ransomware, AI-driven scams, and supply chain vulnerabilities. Within their overall cybersecurity posture, it is crucial that fashion companies implement strong endpoint protection solutions to prevent malware infections, detect malicious activity early, and provide the incident response capabilities needed to quickly investigate and remediate security events. These measures help fashion brands minimize the damage from cyberattacks and maintain customer trust in an increasingly digital and interconnected market.

The Challenge

Prior to deploying Deceptive Bytes, the fashion hub faced several security challenges, including:

Lack of Proactive Defense - The existing security solutions focused mainly on detection and response, but there was no deception-based mechanism to mislead attackers and reduce their effectiveness.

Limited Resources & Time Constraints – The IT security team struggled to manually analyze and mitigate threats efficiently, requiring a solution that could automate and enhance security processes.

Industry: Fashion & Retail

Location: Italy

Headcount: 150

Revenue: >€30M

Requirements:

- ✓ Effective endpoint protection
- ✓ Easy to install and manage
- ✓ Suitable for small IT staff

Solutions:

- ✓ Active Ransomware Prevention for Windows
- ✓ Active Ransomware Prevention for Windows Servers
- ✓ Active Ransomware Prevention for Linux Servers

No. Endpoints: 250

Summary:

- ✓ Quick, simple & seamless deployment
- ✓ Minimal impact & disruptions on IT environments
- ✓ Improved security posture
- ✓ Added value to the customer

"By integrating Deceptive Bytes, our endpoint security challenges were effectively mitigated through proactive deception & ransomware perception distortion, real-time threat prevention, and improved visibility, allowing the security team to work more efficiently and focus on high priority threats"

Remì C, ICT Specialist

About

In today's rapidly evolving threat landscape, ransomware and advanced cyberattacks are becoming more stealthy and sophisticated, targeting vulnerabilities that traditional security tools often miss. Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware's perception of the environment, breaks ransomware logic and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2025 - All Rights Reserved