

Case Study: State Enterprise Odessa Sea Trade Port

Executive Summary

State Enterprise "Odessa Commercial Sea Port" manages critical maritime infrastructure, handling real estate assets, warehousing, towing, transport, and fleet maintenance. To protect high-stakes dispatch workstations from operational downtime caused by ransomware, the port enhanced its endpoint defenses with Deceptive Bytes. Deployed seamlessly alongside existing antivirus software, Deceptive Bytes delivered zero successful data encryptions, safeguarded legacy operating systems that could not be upgraded, and introduced proactive prevention without increasing daily administrative workload.

Industry: Maritime Infrastructure

Location: Ukraine

Headcount: 475

Revenue: ~ $7M

Requirements:

- ✓ Fast Ransomware prevention
- ✓ Lightweight

Solutions:

- ✓ Active Ransomware Prevention for Windows & Windows Servers

No. Endpoints: 200

The Challenge: Critical Workstations and Single-Layer Vulnerabilities

In the logistics and maritime transport sectors, operational continuity is paramount. Downtime on dispatch workstations translates directly to missed shipments and immediate financial loss.

Prior to deploying Deceptive Bytes, the port relied on centrally managed antivirus software, built-in Windows protections, and group policies. However, several systemic challenges left the IT team concerned:

- **Evasive Threat Vectors:** Traditional defenses struggled to proactively counter fileless loaders, malicious PowerShell scripts, and living-off-the-land techniques using native system binaries.
- **Legacy Operating Systems:** Roughly half of the workstation fleet ran older Windows operating systems that could not be upgraded due to legacy production software constraints, creating persistent security blind spots.
- **Single Layer of Failure:** In 2022, multiple peer logistics organizations, including a direct competitor with a matching software stack, suffered crippling ransomware attacks. An internal review confirmed that despite proper antivirus configuration, the port depended on a single defense layer to halt unknown execution payloads.

The Solution: Proactive Prevention via Deceptive Bytes

Rather than adding resource-heavy traditional Endpoint Detection and Response (EDR) tools that produce excessive alert noise, the port sought a proactive prevention-first solution.

Deceptive Bytes was selected due to its core defense logic: instead of relying on pattern matching, allowlists, or known signature databases, it modifies the runtime environment so malware loses expected footholds and cannot carry out its attack chain.

Never Let Your Business Down

© Copyright of Deceptive Bytes Ltd., 2026 - All Rights Reserved

Validation and Rollout

- **Rigorous Scenario Testing:** The IT team validated the platform against controlled attack simulations, including fileless payloads, native system utility abuses, and encryption attempts in test folders, verifying precise interception stages.
- **Phased Wave Deployment:** The platform was rolled out sequentially over two weeks, beginning with a pilot group, moving to the head office, and concluding with remote operational units.
- **Minimal Resource Expenditure:** Initial configuration across all 200 endpoints required only 25 to 30 person-hours.
- **Zero Software Friction:** Deceptive Bytes ran concurrently with the incumbent antivirus suite without software conflicts, module disablement, or performance degradation on mission-critical dispatch software.

Business & Operational Impact

1. 100% Ransomware Prevention

Across the entire deployment period, the port recorded zero successful data encryption events, despite a marked increase in targeted cyberattacks across the logistics sector.

2. Runtime Hardening for Legacy Systems

Workstations running legacy operating systems achieved complete defense parity. Threats that older operating system controls could not mitigate were neutralized directly at the runtime layer.

3. Noise-Free Operations and Operational Savings

Day-to-day administrative overhead remained virtually zero. The platform provided high-context, actionable logs on blocked activity, eliminating alert fatigue and allowing the internal IT service to focus on core operational priorities.

4. Seamless Contractor Security

The solution allowed the IT service to maintain a unified layer of protection on third-party contractor machines connecting to the port network, without requiring complex administrative coordination.

Customer Perspective

"This solution gives your environment protection that works without an allowlist, without signatures and without prior knowledge of the threat, so it protects you from what you have not yet seen. For a small security team, it is a convenient way to raise resilience to new threats without increasing the daily workload."

- Andrii Tyndiuk, Head of Information Technology Service, Odessa Commercial Sea Port

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 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., 2026 - All Rights Reserved