infopulse

Microsoft Defender for Endpoint EDR Implementation for ATB-Market

Client: **ATB-Market** Industry: **Retail** Location: **Ukraine**

Employees: **60,000+** Website: **www.atbmarket.com/en**

Client Background

ATB-Market is the largest retail operator in Ukraine that focuses on the production and sales of food items and other essential commodities. The client's retail chain includes 1200+ grocery stores across 24 regions of Ukraine, which are visited by more than 4 million customers every day. The company's approach to logistics, quality control, and customer service secures its position as Ukraine's leading retailer in terms of inventory turnover, paid income tax, and the number of customers.

Business Challenge

Infopulse has a long history of collaboration with the ATB-Market, which includes a preceding Microsoft Sentinel pilot implementation and other joint IT projects. This time the client decided to implement an Endpoint Detection & Response (EDR) solution to ensure the robust security of both company-owned and personal employee devices that are utilized outside of the corporate network.

ATB-Market approached Infopulse and requested security consulting services to help them select the perfect EDR solution that would suit various operating systems and tackle a range of fundamental business challenges, such as:

- Strengthen the overall security posture of the organization by eliminating blind spots and profoundly reducing the attack surface
- Proactively detect and prevent sophisticated cyber threats that cannot be identified by antiviruses and firewalls
- Effectively safeguard a large pool of corporate and BYOD endpoints for employees who work remotely from different locations in Ukraine and abroad

Solution

Realizing that EDR is important, yet insufficient to ensure full-scale protection against the evolving cyber threats, Infopulse encouraged ATB-Market to consider the implementation of an Extended Detection & Response (XDR) solution. Our team offered to test Microsoft Defender for Endpoint – an integrated endpoint security platform that features advanced ML-driven behavioral analytics, powerful digital forensics, and smart automation.

The project started with an introductory workshop where Infopulse familiarized the client with Microsoft Defender for Endpoint and its key capabilities. Consequently, our experts conducted a brief PoC on their laptops to demonstrate the solution in action and confirm that it meets the client's business needs.

The next stage involved a series of test cases to verify whether Microsoft Defender for Endpoint complied with the expected technical requirements. In close cooperation with ATB-Market, Infopulse formed a test

group of users with corporate devices and designed numerous test cases to assess the solution performance on Windows 10/11, macOS, and Linux. In addition, our team designed a test case for the automated deployment of the solution on Microsoft Intune – cloud-based mobile device management (MDM) service.

Besides executing conventional test cases, Infopulse performed a set of simulated cyberattacks to assess the established endpoint defense system, showcase the full scope of XDR capabilities in practice, and help the client prevent potential cyber risks by demonstrating real-life attack scenarios.

After successfully completing all the testing, ATB-Market had no doubts that Microsoft Defender for Endpoint was the best fit for their business case and Infopulse proceeded with the full-scale implementation of the solution for the retail chain. As a result, the client received a cutting-edge XDR platform with a broad spectrum of valuable features:

- Two possible operational modes for laptops, tablets, and smartphones – agentless for Windows 10/11 and agent-based for macOS, Linux, iOS, and Android
- Comprehensive user behavior analytics that rapidly uncovers anomalous activities, such as unauthorized access attempts, hidden scripts, or corrupted files
- Digital forensics that collects, processes, and investigates complex malicious patterns, including fileless threats launched in random-access memory (RAM)
- Full-scale automation of different security workflows, including threat intelligence, file checks, transfer to quarantine, blocking of compromised communication channels, etc.
- Semi-automatic mode, where the solution automatically performs security analytics and reports the findings to the respective experts prior to blocking a file or process
- Web content filtering and control via category-based URL blocking
- Network hardening capabilities and an integrated network vulnerability scanner – Qualys
- Vulnerability assessment of any software installed on endpoints, including notifications about important security patches/updates.

To further reinforce the client's security perimeter, our specialists offered to integrate Microsoft Defender for Endpoint with the client's SIEM tool – IBM QRadar. As a result, the combination of XDR and SIEM empowered ATB-Market with centralized, real-time threat detection across all attack vectors.

Moreover, to flatten the learning curve for the client's security experts, Infopulse hosted multiple training sessions to help them configure and master digital forensics, reporting, and other functionalities.

Technologies

Microsoft Defender for Endpoint

Qualys

Business Value

To summarize, the implementation of Microsoft Defender for Endpoint along with the extra tailored services has helped ATB-Market to bridge the existing skill gaps, excel at cyber resilience, and provided the following benefits for the retail chain:

- Robust 24/7 protection of 1,500+ corporate and BYOD endpoints against any forms of cyber risks
- ML-powered user behavior analytics that precisely detects any anomalies, thus preventing potential cyberattacks or insider threats
- Automated incident investigation and response that allows focusing on more sophisticated threats or other important strategic tasks
- Minimal learning curve and improved readiness to mitigate and combat sophisticated security exploits
- With in-depth threat intelligence analysis at hand, the client's security team can determine the best-case remediation activities and reduce false positives.

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Norwegian Oil and Gas Association, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL +48 (221) 032-442

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com