BULLWALL

CUSTOMER STORY

BULLWALL HELPS THE GREEK MINISTRY OF DIGITAL GOVERNANCE CONTAIN RANSOMWARE AT THE STORAGE LAYER

HELLENIC REPUBLIC
Ministry of Digital Governance

Industry
Public Sector

Location
Greece

FILESHARE INFRASTRUCTURE

Cloud & on-premises

OVERVIEW

The Ministry of Digital Governance of the Hellenic Republic runs Greece's national digital transformation strategy and delivers online government services to citizens and businesses. It wanted an extra layer of protection against ransomware, working with longstanding Ricoh partner Doxiadis Graphotechniki S.A.

After assessing EDR and XDR options, the Ministry deployed BullWall Ransomware Containment for real-time, agentless containment across its cloud and on-premises storage. Within days of deployment the solution was returning actionable insight into data access patterns and had flagged several instances of potentially malicious activity.

THE GAP PERIMETER DEFENCES COULD NOT CLOSE

Ransomware is a particular concern for public-sector organisations. A single undetected breach could mean catastrophic loss of sensitive data, prolonged downtime for government services, and eroded public trust.

The Ministry had robust measures in place but identified two gaps. Manual security monitoring was impossible during out-of-office hours, which left a window of vulnerability. There was also no dedicated containment solution to stop a ransomware attack if it slipped past the network perimeter.

Director General Aristeidis Meletiou notes that no approach is infallible. The Ministry set out to add real-time automated detection and containment across its critical storage, so it could stop sophisticated attacks at the earliest point and keep essential services running uninterrupted.

WHY CONTAINMENT AT THE STORAGE LAYER

EDR and XDR solutions protect endpoints, but ransomware can still evade those measures and target on-premises and cloud storage repositories. Ransomware Containment takes an agentless approach and contains ransomware in real time at the storage layer, working alongside the Ministry's existing tools rather than replacing them.

The Ministry's IT team worked with experts from Doxiadis Graphotechniki and BullWall to integrate the solution across both storage environments, set customised detection thresholds, and build incident response playbooks. Because the architecture is agentless, there was no need to deploy software on individual endpoints, which reduced complexity and deployment time.

The Ministry also tested the real-time alerts and automated containment before going live. The tests returned strong results and confirmed the solution could isolate a threat the moment malicious encryption began.

For the Ministry, the case was clear.

ROUND-THE-CLOCK CONTAINMENT, A LIGHTER LOAD ON IT

Today the solution monitors the Ministry's storage landscape around the clock and immediately isolates an endpoint or user when malicious encryption is detected, which stops the threat from spreading. The early detection has already allowed the team to remediate potential vulnerabilities before bad actors could exploit them.

The automated detection and containment has also reduced the burden on the IT and security team. Instead of manually monitoring the storage environment for suspicious activity, the team now spends its time on strategic, higher-value work.

Feedback from the IT and security teams has centred on the intuitive dashboard, the granular monitoring and alerting, and the confidence that a ransomware attack can be contained automatically. The Ministry reports that Ransomware Containment integrates cleanly with its other security tools and that the agentless architecture has minimal impact on network performance.

According to Director General Aristeidis Meletiou, Ransomware Containment has strengthened the Ministry's overall security posture and given it confidence that essential services stay protected. He says the Ministry would recommend the solution to any public-sector organisation looking to strengthen its ransomware defences and safeguard public trust.

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting critical IT infrastructure from ransomware. We provide rapid containment of active attacks, and safeguard servers by preventing unauthorized intrusion.

Learn more at www.bullwall.com.

BULLWALL