CASE STUDY · NOVEMBER 2024

Florida Sheriff’s Office Reduces Costs and Strengthens Endpoint Security

An anonymous Florida sheriff’s office replaced Sophos with Microsoft Defender for Endpoint and Intune in under one month, eliminating a separate licensing expense and centralizing security management.



Conceptual illustration only; not the customer’s production environment.

How Microsoft Defender for Endpoint and Intune simplified protection and management. The agency and county are anonymous. Timeline and outcomes are reported in the supplied November 21, 2024 project account; no dollar savings, compliance certification, or guaranteed protection is asserted.

A Florida county sheriff’s office needed to strengthen endpoint security while controlling technology costs. Its existing Sophos antivirus deployment required separate licensing and management alongside the agency’s Microsoft 365 environment.

In under one month, the agency transitioned to Microsoft Defender for Endpoint, automated deployment and policy enforcement through Microsoft Intune, and standardized endpoint security settings. The project eliminated Sophos licensing costs and simplified ongoing administration.

At a glance

Category	Details
Industry	Law enforcement and public safety
Previous solution	Sophos Antivirus
New solution	Microsoft Defender for Endpoint with Microsoft Intune
Existing environment	Microsoft 365 G3 subscriptions
Implementation timeline	Under one month
Reported results	Eliminated Sophos licensing costs, automated management, and more consistent endpoint protection

Microsoft 365 G3 describes the agency’s existing environment, not a claim that all deployed Defender capabilities are included in that subscription. Available capabilities depend on the applicable licenses and configuration.

The challenge

The sheriff’s office relied on Sophos antivirus to protect endpoints supporting public safety and law enforcement operations. While the solution provided protection, maintaining it alongside Microsoft 365 created additional licensing expenses and separate administrative processes.

IT staff worked across disconnected management consoles, and endpoint security policies were applied inconsistently. The agency wanted to consolidate security management, reduce redundant work, and improve integration with its Microsoft environment.

The objective was to reduce costs while establishing a more consistent approach to protecting sensitive law enforcement information.

The solution

Massive IT migrated the agency’s endpoints from Sophos antivirus to Microsoft Defender for Endpoint and used Microsoft Intune to automate deployment and enforce security policies.

Workstream	Documented approach
Transition endpoint protection	Replace Sophos with Microsoft Defender for Endpoint across agency endpoints, consolidating protection within the Microsoft ecosystem.
Standardize security policies	Apply Microsoft-recommended Attack Surface Reduction policies to establish consistent settings designed to reduce exposure to ransomware and other advanced threats.
Automate deployment and enforcement	Use Intune for centralized deployment and policy management, reducing manual effort required to maintain endpoint configurations.
Prepare IT staff for ongoing management	Train the agency’s IT team to administer endpoint protection and security policies within its Microsoft environment.

The transition was completed in under one month.

The outcomes

Eliminated Sophos licensing costs

Retiring the previous antivirus platform removed a separate licensing expense. The supplied account does not quantify savings or establish the total cost of the replacement licensing.

Reduced administrative overhead

Automated deployment and centralized policy enforcement streamlined routine endpoint management.

Strengthened endpoint security

Standardized Attack Surface Reduction policies improved consistency across devices and strengthened the agency’s protection against cyber threats.

Simplified management and reporting

Consolidating endpoint security within the Microsoft ecosystem reduced reliance on separate tools and administrative workflows.

A more sustainable security strategy

The sheriff’s office established an integrated approach to endpoint protection that supported both its security and operational priorities. By replacing Sophos with Microsoft Defender for Endpoint and automating management through Intune, the agency reduced redundant costs, improved IT efficiency, and strengthened protection for sensitive law enforcement data.