Efficient threat management across Microsoft Defender

A large government organization faced significant challenges in managing Microsoft Defender at scale. Operating across multiple departments and agencies, each with distinct security needs and operational priorities, the organization needed a solution to streamline security operations while maintaining robust threat management and compliance.

VOSS

THE CHALLENGE

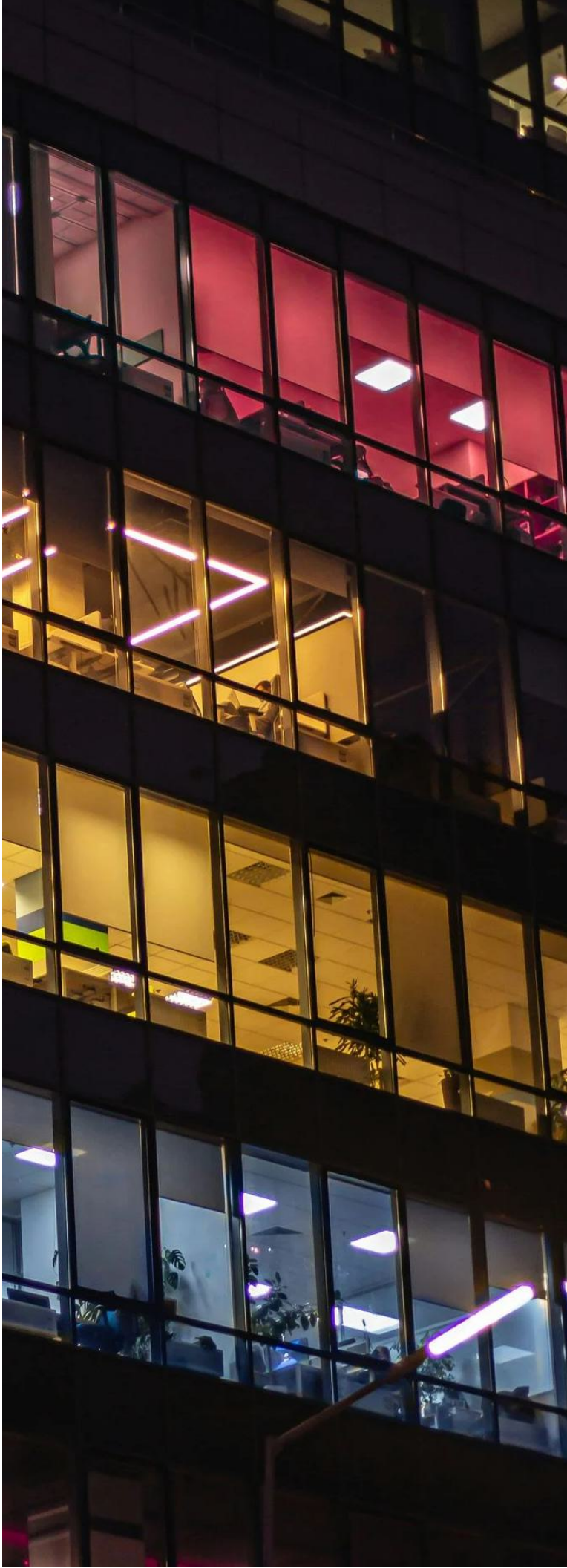
Managing security threats in a dynamic, multi-unit environment

The government relied heavily on Microsoft Defender to detect, investigate, and respond to security threats across a range of topics, including applications and end points, plus Office and Teams collaboration. However, with thousands of users and devices spread across multiple agencies, managing security incidents through a centralized approach created numerous challenges.

THE CHALLENGE

- **Limited role-based access**: A small central security operations (SecOps) team held global admin access, with much of the work undertaken on privileged access workstations, making it difficult to delegate tasks efficiently while maintaining visibility and control.
- **Slow incident response**: High-priority threats were often delayed as the SecOps team faced backlogs in reviewing and acting on quarantine items.
- **Lack of segmentation**: Without granular access controls, agencies couldn't independently manage low- and medium-priority incidents, resulting in bottlenecks.
- **Poor user experience**: False positives and low-priority incidents overwhelmed the SecOps team, leading to frustration and slower threat resolution.
- **Inefficient workflows**: Security data was siloed, making collaboration and visibility across departments challenging.

The organization needed a solution to distribute security responsibilities, optimize workflows, and ensure quicker threat resolution without compromising security oversight.



THE SOLUTION

VOSS for agile, role-based Defender management

To address these challenges, the government deployed VOSS to enhance the management of Microsoft Defender. By providing intelligent automation, proactive monitoring, and role-based access control, VOSS empowered local teams to manage their own security incidents while maintaining centralized oversight.

- **Granular role-based access**: VOSS enabled agencies to handle their own low- and medium-priority incidents, while reserving high-priority threats for central SecOps review.
- **Automation and orchestration**: Routine tasks like reviewing false positives and managing quarantine items were automated, significantly reducing response times.
- **Visibility and control:** The central SecOps team retained a global view of all security events, ensuring compliance and efficient oversight, with the ability to navigate down into lower levels of the organization to review detail.
- **Seamless integration**: VOSS integrated with the organization's existing SOC and ticketing systems, providing real-time insights and improving collaboration.
- **Localized empowerment**: Departments gained autonomy to resolve incidents rapidly without waiting for central approval, enhancing operational resilience.

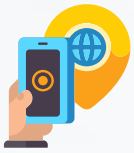
THE BENEFITS

Faster response times and improved operational efficiency

By implementing VOSS, the government organization achieved tangible improvements across its security management operations:

ENHANCED VISIBILITY

SecOps maintained a global view of security incidents while gaining deeper insights into agency-level activity.

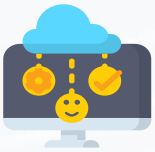


LOCALIZED CONTROL

Agencies could resolve incidents independently, reducing pressure on the central team and speeding up threat response.

OPERATIONAL EFFICIENCY

Automated workflows minimized manual tasks, improving accuracy and reducing response times.



IMPROVED USER EXPERIENCE

Quicker incident resolution reduced disruption for end-users and built confidence in security operations.

STRONGER SECURITY POSTURE

By streamlining workflows and enabling real-time threat management, the organization minimized security risks and ensured compliance.

With VOSS, the government organization redefined its Microsoft Defender management strategy. By empowering agencies to act swiftly while maintaining centralized oversight, they achieved a scalable, secure, and efficient solution for threat management.

Addressing a growing security challenge

As cyber threats evolve, managing Microsoft Defender at scale becomes increasingly complex. VOSS provides the tools to segment large, multi-unit environments, streamline security operations, and ensure visibility across all levels of the organization. By automating key security workflows, delegating control with precision, and enabling proactive threat management, VOSS helps organizations strengthen their cybersecurity posture while reducing operational overhead. If your organization is facing similar challenges, get in touch to learn how VOSS can help you enhance security, improve efficiency, and maintain compliance with confidence.

VOSS

voss-solutions.com
info@voss-solutions.com
+1 469 206 0441