HOLM SECURITY

PRODUCT COMPARISON

Microsoft Defender Vulnerability Management & Holm Security VMP

Version 1.6

HOLM SECURITY

TABLE OF CONTENTS

This document compares Microsoft Defender Vulnerability Management with Holm Security VMP.

MICROSOFT DEFENDER VM

HOLM SECURITY

What is Microsoft Defender Vulnerability Management?

Microsoft Defender Vulnerability Management is a feature of Microsoft Defender, a security solution provided by Microsoft mainly for Windows devices. It is designed to help organizations identify and fix vulnerabilities in their systems and networks to prevent cyberattacks.

Vulnerability Assessment

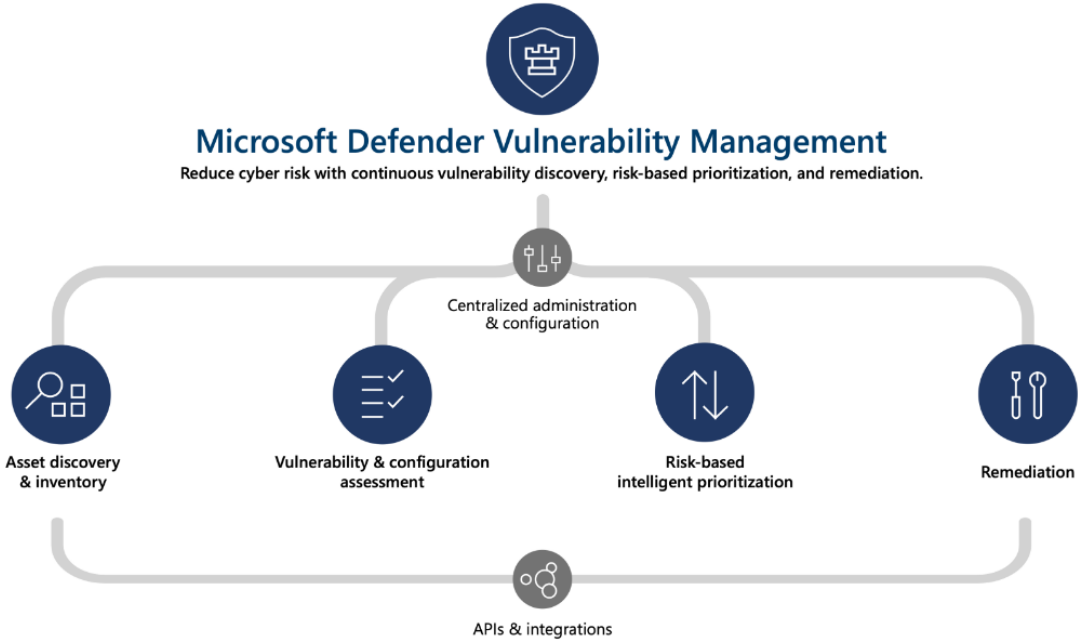
Defender for Identity is not an anti-virus product and should not be confused with Microsoft Defender, which provides anti-malware and anti-virus capabilities for the Windows 10 operating system. The ATP product is mainly a post-breach solution that complements Microsoft Defender.

Patch management

This helps organizations apply patches and security updates to fix vulnerabilities in their systems. Microsoft Defender Vulnerability Management provides notifications when new patches are available and allows organizations to deploy them to the relevant systems.

Remediation

This involves implementing actions to fix vulnerabilities. Microsoft Defender Vulnerability Management provides recommendations for remediation based on the severity of the vulnerabilities and the potential impact on the system.



HOLM SECURITY VMP

HOLM SECURITY

What is Holm Security VMP?
Holm Security VMP is a modern and cost-effective vulnerability management platform with all the tools you need to make your business secure. Continuously detect vulnerabilities and protect your organization against cyber security attacks anytime, anywhere.

Unparalleled attack vector coverage
Our all-in-one platform offers unparalleled attack surface coverage, covering systems, cloud infrastructure and services, local and remote computers, network equipment, IoT, OT/SCADA, web applications, APIs, and users.

Unification & unified risk score
Our platform provides truly unified views and risk scoring, allowing you to understand the full context of each exposure and focus on high-risk technical vulnerabilities and users. Maximize your efforts and reduce business-critical risks with the least amount of effort.

Covers technical assets as well as human
As 50% of all ransomware attacks originate from phishing email attacks, a modern vulnerability management platform should cover not only technical assets but also human assets.

Automation & continuity
Holm Security VMP is built on the principle of minimizing manual work to allow continuity. Therefore, most of the processes in the platform are fully automated and require no manual work.

Easy to implement & maintain
Holm Security VMP can be implemented within a few hours, and the process is simple and straightforward. Using Scanner Appliances, you can cover your entire IT environment.

Supports the entire workflow
The platform is managed using Security Center. Security Center provides full support for asset management, prioritization and management of vulnerabilities, remediation, and out-of-the-box integrations with common systems like communication and SIEM platforms, ticketing and access management systems, and CMDB.

Extensive support
Holm Security provides extensive support with the platform to guarantee a successful implementation and maintenance of the vulnerability management platform.

ATTACK VECTOR

HOLM SECURITY

Attack vector:	Description:	Product:	
		Microsoft Defender Vulnerability Manager:	Holm Security VMP:
Systems & servers	Assessment of systems like Windows and Linux systems.	ⓘ Agentless for Microsoft-based systems. Requires manually installed agent for Linux. Limited to systems that are supported by the agent.	✓ Agentless for all platforms.
Computers	Assessment of Windows and Linux-based computers.	ⓘ Agentless for Microsoft-based systems. Requires manually installed agent for Linux.	✓ Agentless for all platforms.
OT/SCADA & IoT	Assessment Operational Technology and SCADA.	ⓘ Requires additional subscription with the IoT sensor that monitors/sniffing network traffic that comes with several requirements. Limited to a set of protocols only,	✓ Supports all OT/SCADA systems.
Network equipment	Assessment of network equipment such as switches, routers and firewalls.	ⓘ Limited to a set of network vendors with a limited pulling of information. Currently supports Cisco IOS, IOS-XE, NX-OS, Juniper JUNOS, HPE ArubaOS, Procurve Switch Software, and Palo Alto Networks PAN-OS.	✓ Supports all types of network equipment and vendors.
Cloud infrastructure	Traditional servers and services running in cloud platforms, such as AWS and Azure.	⊘ Not possible to scan cloud infrastructure.	✓ Supports all cloud platforms.
Cloud services (CSPM)	Assessment of services and resources in cloud-native environments, such as Microsoft Azure, AWS, Google Cloud and Oracle Cloud.	ⓘ Doesn't support Oracle Cloud.	✓ Supports all common cloud platforms.
Websites & and web apps	Assessment of all types of websites and web applications.	⊘ Not supported.	✓ Fully supported.
APIs	Assessment of APIs (Application Programming Interface).	⊘ Not supported.	✓ Fully supported.
Users	Phishing simulation and awareness training.	ⓘ Microsoft has a product for phishing attack simulation training with limited functionality.	✓ Fully supported.

TECHNOLOGY

HOLM SECURITY

Technology:	Description:	Product:	
		Microsoft Defender Vulnerability Manager:	Holm Security VMP:
Unauthenticated scanning	System and network scanning from the outside, without access to the system.	⃠ Not supported.	✓ Fully supported.
Authenticated scanning	Authenticates against scanned targets and performs deeper analysis of vulnerabilities from installed applications and packages.	ⓘ Not supported.	✓ Fully supported.
Policy scanning (CIS Benchmarks)	CIS Benchmarks best practices for the secure configuration of a target system. Holm Security is certified by CIS (Center for Internet Security).	ⓘ Supported for Windows operating systems.	✓ Fully supported.
Agent-based scanning	Light-weight endpoint extracting all software installed in a computer to find vulnerabilities. Track devices in dynamic networks and computers that are not within your reach.	✓ Fully supported for Windows, Linux, and MacOS.	ⓘ Supported for recent Windows operating systems.
Discovery scanning to find blank spots	Identify active assets running within a network.	ⓘ Possible by using a monitor/network traffic sniffer.	✓ Fully supported.
Remote assessment	Assessment a public network from the outside.	ⓘ You need to host an external scanner yourselves in an offsite datacenter.	✓ Fully supported using a Scanner Appliance or Cloud Scanners.

DEPLOYMENT

HOLM SECURITY

	Technology:	Description:	Level of complexity:
Microsoft	MS Defender Agent	Higher level of security review as an agent is required to be running and installed on devices with high privilege.	**High**
	MS Defender Agent for network devices	Higher level of security review as an agent is required to be running and installed on devices with high privilege. Requires software installation on servers provided and managed by the customer.	**Very high**
	MS Defender IoT Sensor	Requires in-depth network competence as sniffing/monitoring of network packages is required. Higher risk of business impact as it involves active monitoring and has access to all network packages, including potentially sensitive data.	**Expert knowledge required**
Holm Security	Holm Security external scanning	No deployment is required, ready from the start.	**Low**
	Holm Security Scanner Appliance	Deployment of a virtual machine image that is de facto-standard at all companies.	**Medium**
	Holm Security Device Agent	Higher level of security review as an agent is required to be running and installed on devices with high privilege.	**Very high**

LICENSES & COSTS

License:	Description:	Example:	Price:
Microsoft E5	E5 is a prerequisite for the Microsoft Defender Vulnerability Management.	500 users	E5 with Microsoft Defender Vulnerability Management: $340,000/year E5: $328,500/year ($54,75/user/month) Microsoft Defender Vulnerability Management add-on: $12,000/year ($2,00/user/year)
Holm Security VMP	System & Network Security	250 systems License volume based on average for company with 500 employees.	Total per year: $11,478 Per IP/month: $3,83
Holm Security VMP	Full platform	System & Network Security: 250 systems, 500 computers Web Application Security: 15 web apps Phishing Simulation & Awareness Training: 500 users	Total per year: $32,226

Source: Microsoft 2025-01-01

CONCLUSION

A competent product
Microsoft Defender Vulnerability Manager is a cyber security product integrated with mainly Microsoft-based platforms. It's mainly focused on asset discovery, risk-based assessments, and remediation. It's a new product that will need some time to become more mature and competent.

Traditional vulnerability management
The core and great benefit of traditional vulnerability management are how easily it's deployed, but at the same time, you get major asset coverage. You can scan your entire IT environment (systems/servers, computers, network equipment, IoT, OT/SCADA, web applications etc.) without any system requirements, specific hardware, or software. This makes it possible to find vulnerabilities in every single system – even if the system is unmanaged or even unknown. When new systems are deployed in your network, they will automatically be discovered and scanned. In this process, you will find not only vulnerabilities but also blank spots.

A different & complex approach
Microsoft Defender Vulnerability Manager approach is significantly different because you will only find vulnerabilities in known systems that are managed. If you want to get a broader asset coverage, network sniffers are required, which comes with a high level of complexity to install and maintain - and you will still be limited to very specific systems.

Microsoft focus
Because of the manual process of covering non-Microsoft/Windows-based systems, Microsoft Defender Vulnerability Manager could be considered as mainly supporting Microsoft/Windows-based systems. Also notice that Microsoft Defender Vulnerability Manager requires the usage of the Microsoft ecosystem (Azure AD, Defender, etc.) and in-depth Microsoft expertise, as these technologies are very much coupled and tied together.

Self-assessments are questionable within cyber security
One of the rules of thumb within cyber security is not to have the vendor assess its own security. As Microsoft is a huge vendor, this is, of course, inevitable, but one should consider to what extent Microsoft's cyber security products should be used.

License cost
Microsoft Defender for Identity is only included in the E5 and P2 packages, which come with a significantly higher cost than the standard Microsoft 365 packages. If you don't have these packages, using Microsoft Defender Vulnerability Manager will cost considerably more than traditional vulnerability management solutions.

Guidance is needed
Vulnerability management has been around as a very powerful cyber security product for well over 20 years. One of the most essential experiences that industry experts can agree about is that organizations need support to set up a successful vulnerability management program. Accordingly, it's important to understand to what extent Microsoft will support your vulnerability management program.

ⓘ Summary: not traditional vulnerability management

Microsoft Defender Vulnerability Manager has some similarities with traditional vulnerability management, but they are very different products looking at coverage and implementation. Accordingly, these products should not be considered competing, but rather complementary. A large enterprise organization could consider using both products.

MORE INFORMATION

HOLM SECURITY

Content:	Description:
Microsoft Defender Vulnerability Manager	https://www.microsoft.com/en/security/business/threat-protection/microsoft-defender-vulnerability-management https://www.youtube.com/watch?v=G54f7lqUFMU https://www.linkedin.com/learning/controlling-cybersecurity-risk-with-defender-vulnerability-management/
Microsoft licensing for business	https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products
Microsoft enterprise licensing (E-packages)	https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans
Holm Security VMP	https://www.holmsecurity.com/platform