SKYBOX SECURITY AND

MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

Tech Brief

Today's enterprises are challenged with managing the security of complex networks that are distributed across physical and virtual environments. These environments are evolving at a rapid rate, which leaves them prone to attack.

Microsoft Defender Advanced Threat Protection (ATP), a leader in endpoint detection and response, helps enterprises prevent, detect, investigate and respond to advanced threats in an easy–to–manage, cloud–powered solution. Skybox's integration with Microsoft Defender ATP gives you a centralized view of your environment for automating processes, assessing vulnerabilities and managing remediation efforts.

Full Passive/Active Discovery on the Network

- Workstations, servers, cloud assets and operational technology (OT) devices
- Collection from active scanners
- Full coverage of all platforms, operating systems and vendors

Enhanced Prioritization and Risk Identification

- Network-based context highlighting indicators of exposure (IOE) such as open access or no mitigating controls
- Exploitability based (e.g., noted as exploited in the wild through cyber threat intelligence)
- Activity based representing the indicators of compromise (IOC) and attack (IOA) as reported by Microsoft
- Business context driven by automated tagging

Compliance, Remediation and Mitigation

- Threat mitigation through non-patch mitigating controls (e.g, IPS, firewall, EDR)
- Streamline remediation process, joining security and IT under a unified workflow
- Patching prioritization based on urgency and risk

BETTER TOGETHER: MICROSOFT DEFENDER ATP AND SKYBOX SECURITY

Skybox's integration with Microsoft Defender ATP gives you a centralized, access–controlled environment for automating processes, assessing deficiencies and managing remediation efforts.

- Complete, continuous and non-intrusive vulnerability **discovery**
- Risk–based **prioritization** leveraging network context and cyber threat intelligence
- Process-driven, automated and urgency-based **remediation**
- **Oversight** of a risk–based vulnerability management program across hybrid networks

How it Works

The inclusion of critical data from Microsoft Defender ATP enhances Skybox's vulnerability detection capabilities, thereby expanding vulnerability management for enterprises that continue to deploy workloads across hybrid and cloud network environments. This integration also provides Microsoft Threat and Vulnerability Management (TVM) users with the benefit of:

- Enhanced vulnerability prioritization considering network, threat and business context
- Risk and exposure analysis derived from multiple perspectives of vulnerabilities, assets and groups
- Comprehensive detection of vulnerabilities in hybrid environments by leveraging Skybox's other 140+ device integrations
- Flexible risk scoring, where each organization can decide which factors - exposure, exploitability, CVSS and asset criticality along with their respective weight - will be included in the risk formula.

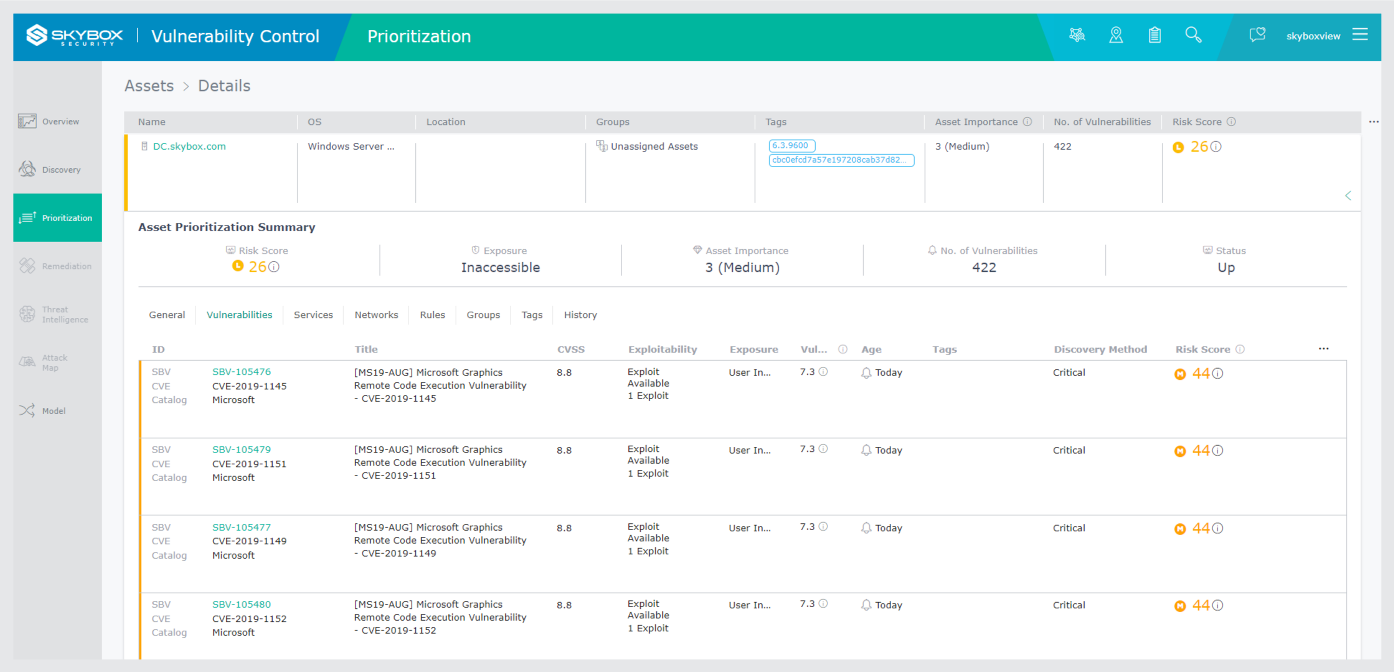
Skybox collects data from Microsoft Defender ATP and incorporates it into a model with other asset data collected from sources such as vulnerability scanners. This model provides the foundation for overall visibility and automated vulnerability management processes.

Below is a brief description of how Microsoft Defender ATP data is collected:

- Skybox collector pulls the asset and vulnerability data from the Microsoft Defender ATP tenant through its API
- The Skybox server runs a continuous process to enrich the host information with the following:
    - Directly, indirectly or no exposure flags
    - Access path data from any origin to any destination in the network
    - Non-patch remediation data such as IPS signatures needing update or access rules that need to be closed to block access to the service
    - Firewall device or rules that can be closed to block access to the service

The synthesized and modeled data allows organizations to:

- Centralize and enhance vulnerability management processes from discovery to prioritization and remediation
- Harness the power of data — from vulnerabilities and asset data to network topology and security controls
- Use network modeling and attack simulation to find exposed vulnerabilities
- Contextualize vulnerability data with up-to-date intelligence of the current threat landscape



Assets > Details

Name	OS	Location	Groups	Tags	Asset Importance	No. of Vulnerabilities	Risk Score
DC.skybox.com	Windows Server ...		Unassigned Assets	6.3.9600 cbc0efcd7a57e197208cab37d82...	3 (Medium)	422	26

Asset Prioritization Summary

Risk Score	Exposure	Asset Importance	No. of Vulnerabilities	Status
26	Inaccessible	3 (Medium)	422	Up

General | Vulnerabilities | Services | Networks | Rules | Groups | Tags | History

ID		Title	CVSS	Exploitability	Exposure	Vul...	Age	Tags	Discovery Method	Risk Score
SBV CVE Catalog	SBV-105476 CVE-2019-1145 Microsoft	[MS19-AUG] Microsoft Graphics Remote Code Execution Vulnerability - CVE-2019-1145	8.8	Exploit Available 1 Exploit	User In...	7.3	Today		Critical	44
SBV CVE Catalog	SBV-105479 CVE-2019-1151 Microsoft	[MS19-AUG] Microsoft Graphics Remote Code Execution Vulnerability - CVE-2019-1151	8.8	Exploit Available 1 Exploit	User In...	7.3	Today		Critical	44
SBV CVE Catalog	SBV-105477 CVE-2019-1149 Microsoft	[MS19-AUG] Microsoft Graphics Remote Code Execution Vulnerability - CVE-2019-1149	8.8	Exploit Available 1 Exploit	User In...	7.3	Today		Critical	44
SBV CVE Catalog	SBV-105480 CVE-2019-1152 Microsoft	[MS19-AUG] Microsoft Graphics Remote Code Execution Vulnerability - CVE-2019-1152	8.8	Exploit Available 1 Exploit	User In...	7.3	Today		Critical	44

FIG 2: Relevant vulnerabilities for the selected workstation, showing exposure, exploitability, the vulnerability details, and risk.

Learn More

Dive deep into Skybox's unique approach to vulnerability management with these resources:

- Risk-Based Vulnerability Management E-Book
- Comprehensive Vulnerability Discovery Solution Brief
- Intelligent Vulnerability Prioritization Solution Brief

Beyond vulnerability management, discover the variety of use cases supported by Skybox, including unified security policy management across hybrid networks, at our website.

About Skybox Security

At Skybox Security, we provide you with cybersecurity management solutions to help your business innovate securely. We get to the root of cybersecurity issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you're able to control security without restricting business agility. Skybox's comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your business forward, faster.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060