

## DATA SHEET

# **Malwarebytes Nebula**

Cloud-hosted security platform maximizing team resources and simplifying endpoint protection

When it comes to managing endpoint protection, companies need a simple solution that frees up IT resources and offers quick visibility into prioritized issues and emerging threats. IT teams also need a platform that makes it easy to push out updates and understand the state of every endpoint—*even* when they're off the corporate network—so they can develop a strong security posture for the organization.

# Malwarebytes Nebula overview

Malwarebytes Nebula is a cloud-hosted security operations platform that allows you to manage control of any malware or ransomware incident—from alert to fix. Integrating all Malwarebytes products into a single view, Malwarebytes Nebula augments our solutions with a guided user interface, next generation threat intelligence, brute force attack protection, and integration capabilities that maximize your security investments across the organization.

### Manage all your products

Malwarebytes Nebula comes standard with your Malwarebytes endpoint security solution, allowing you to manage the following Malwarebytes products from a single cloud-based user interface (UI):



### **Malwarebytes Incident Response**

threat detection and remediation tool that scans networked endpoints for advanced threats and thoroughly removes them



### **Malwarebytes Endpoint Protection**

advanced endpoint threat prevention solution that uses multiple detection techniques for full attack chain protection



### **Malwarebytes Endpoint Detection and Response**

modern endpoint detection and response (EDR) that makes it easy to quickly investigate, isolate, remediate, and recover from threats

# Up your security game

Intuitive automation transforms the complicated into the simple.

Malwarebytes	Endpoints				☆ ♥₂ № ↓ Josh Pederson Super Admin
■ Dashboard ■ Endpoints	Displaying records for Endpoints in All Groups		Add Endpoints	Delete Move	Actions *
n Detections ♥ Quarantine	Showing 6 records for: Status: Remediation	Required X Clear Filters	[	IP Address/CIDR v Search	by IP/CIDR
Suspicious Activity	Endpoints 🔺	▼ Status ▼ Operating System ▼	Group <b>T</b> P	olicy T	Last Seen
Reports	Bogdans-MacBook-Pro.local	All the MacOS	FRENCH In	cident Response and Asset	Today
9 Events	DESKTOP-541H0UI	👬 🔿 Windows	Dallas, Texas E	ndpoint Protection	3 days ago
Tasks Downloads	DESKTOP-OKOI2GQ	Scan Needed ows	Default Group D	efault Policy	6 days ago
Settings ^	DESKTOP-SUFPPEU	Last Scan: 9 days ago Click icon for more options ows	Alan IR Group A	lan IR Policy	Today
Policies	EPR-bdemidov.mb.lab	<sup></sup> 通四	Tallinn EPR B	ogdan EPR Policy	2 weeks ago
Exclusions	STUDENT00	👬 🚥 💠 Windows	GOH EP GROUP G	OHEP	3 months ago
Groups					
Users					
Syslog Logging					
Single Sign-On					

#### **Guided UI streamlines administration**

- Intuitive controls and guided workflows accelerate your task completion
- Multiple 1-click deployment options streamline new endpoint onboarding

#### **Threat activity replay**

- Charts infection spread across your organization's domain, enabling you to clearly understand threat patterns and make informed decisions on how to best prevent future infections
- Analysis of response and remediation outcomes across endpoints helps you identify areas for security improvements

#### **Expanded security coverage**

- Automated protection against brute force attacks targeting Remote Desktop Protocol (RDP) connections
- · Set-and-forget configuration, minimizing your team's maintenance needs

# Master the threat lifecycle

Situational awareness from detection to remediation.

Malwarebytes	× +								
$\leftarrow$ $\rightarrow$ C $\triangleq$ cloud.m	alwarebytes.com/b3e5b97a-3c5d-4c0a-8aed-bf54d309f24b/dashboard					07	☆	<b>*</b> 2 ()	1   🦢 1
<b>⇔alware</b> bytes	Lill Dashboard								ederson ~
🔟 Dashboard	NUMBER OF DETECTIONS     Occurrences per day			MALWARE	• PUP	РИМ (	RANSO	MWARE	EXPLOIT
🖵 Endpoints	200								
賽 Detections	200								
Quarantine	180								
Suspicious Activity	100								
Reports	50								
<b>່ວ</b> Events	0	Dec 31	Jan Jan Jan Jan Jan	Jan Jan J 7 8	an Jan 9 10	Jan Jan 11 12	Jan 13	Jan J	lan Jan
📑 Tasks	17 18 19 20 21 22 23 24 25 26 27 28 29 30	31	1 2 3 4 5 6	7 8	9 10	11 12	13	14	15 16
🛓 Downloads	SUSPICIOUS ACTIVITY     Past 24 hours		TOP 10 ENDPOINTS WIT	TH DETECTION	NS				
Settings ^	Total : 0		Name					D	etections
Policies	High	0	DESKTOP-NLDB9RL						3,550
Schedules	Medium	0	ClaudioMB1.claudiolab.local						318
Exclusions									
Groups	Low	0	claudioEPR						242
Users			STUDENT00						189
Syslog Logging	All Suspicious Activity	>	DESKTOP-541H0UI						93
Single Sign-On	TOP 10 SUSPICIOUS ACTIVITY DETECTION RULES     Past 24 Hours		Past 90 Days	CTIONS					
	Name Co	ount	Name					D	etections
Send feedback	No data to display		Trojan.MalPack.VB						256

#### **One-click policy updates**

- Provides guided, intuitive 1-click controls for teams to adjust policies and settings relevant to specific phases of the threat lifecycle, and rapidly deploy across endpoints
- Contextual information within the UI educates staff on the meaning of policy settings

#### State of the endpoint, simplified

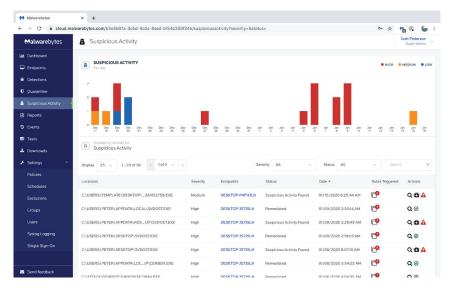
- Quickly discover insights into the health and status of individual endpoints
- Broad OS-level metadata includes OS version, location, software, license state, and more, enabling deeper visibility into the endpoint

#### Drive better decisions, faster

- Pre-built and customizable reports provide flexible control over dimensions, timing, and content, driving rapid and effective decisions
- On-demand and scheduled reports are available in the dashboard UI or via email

# Leverage cloud performance

Light-weight agent and powerful cloud detection that streamlines endpoint processing.



#### **One billion goodware comparisons**

- Goodware comparisons are made in the cloud, eliminating endpoint resource drain and reducing false positives
- Cloud storage ensures new goodware files are continually added for reference, without adding bloat to the agent

#### **Rapid detection of obfuscated malware**

- New threats from packaged and polymorphic malware are detected as they arise and before they can wreak havoc on a user's device
- Seamless communication between cloud and endpoint agent compares behavior and identifies potential threats in near real-time

#### **Cloud sandbox to investigate unknown files**

- Provides a cloud-based sandbox environment that analyzes and reviews unknown files
- Cloud-computing power rapidly analyzes and informs on the true nature of suspicious files

LEARN MORE					
To learn more about Malwarebytes Nebula, visit: www.malwarebytes.com/nebula					
malwarebytes.com/business	corporate-sales@malwarebytes.com	1.800.520.2796			

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at <u>www.malwarebytes.com</u>.

Copyright © 2020, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.