DATA SHEET

ThreatDown™
Powered by Malwarebytes

APPLICATION BLOCK

Prevent application threats; promote productivity

Add Protection—Not Complexity

Every Windows application is a potential entry point through which cyberpunks can waltz in and wreak havoc. In a seemingly legitimate application, wannabe intruders can embed malicious code, which an end user can unwittingly execute simply by launching the application. Or, black-hat hackers can exploit an application with a vulnerability that hasn't been patched. Left unchecked, applications expose you to the risks and costs associated with cyberattacks and might also leave you facing fines for non-compliance with data protection regulations.

ThreatDown Application Block helps you better prevent cyberattacks and comply with governance regulations. This capability empowers you to easily identify and block (or "blacklist") untrusted or undesirable Windows applications without increasing the complexity of security management. Once activated, ThreatDown Application Block is immediately accessible, extending the power of the cloud-based cybersecurity platform you already trust for endpoint protection and remediation.

Application Blocking: We Keep It Simple

Time, budget, expertise, and staff—all of your cybersecurity resources are tight. We get it: that's why every ThreatDown, product is designed from the ground up with simplicity in mind. ThreatDown Application Block is no exception to this rule; it adds another layer of protection to your endpoints without adding to the complexity of managing endpoint protection. And for simplicity, Application Block is now included in all ThreatDown bundles.

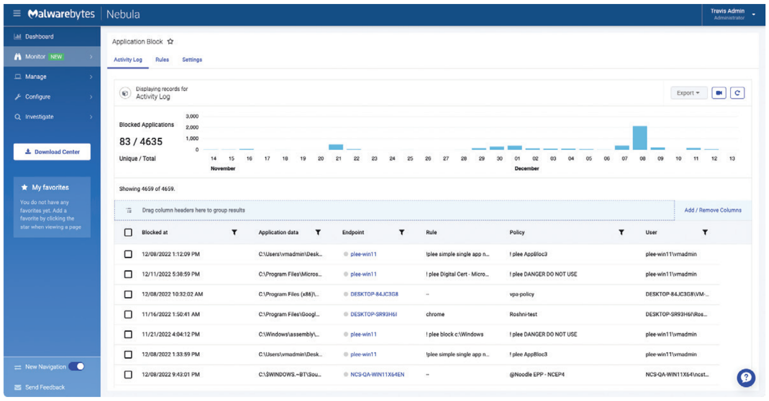
Block Untrusted Applications

ThreatDown Application Block easily blacklists unsafe, outdated and unused applications across all of your Windows endpoints from a single, central location.

- Ensures that blacklisted applications cannot be run or launched from Windows laptops, desktops or servers (when licensed).
- Offers a simple alternative to the sometimes time-consuming task of uninstalling outdated applications or those you no longer use organization wide: blacklist the application in Nebula, and you're done.
- Prevents cybercriminals from exploiting blacklisted applications, which cannot be used to sneak malware into your digital environment.

Challenges

- Your organization's small- to midsize (<1000 employees) does *not* protect you from cyberattacks.
  - Cyberattacks targeting SMBs increased 170% during the last year[1]
  - The smallest firms (<10 employees) experienced a near four-fold rise[2]
- SMBs are attractive targets because they are known to have resource constraints, so they are considered easier to breach
- Left unprotected, Windows applications expose SMBs to the risk and cost of cyberattacks and also to fines associated with data protection regulation violations
- Some application-blocking solutions increase the complexity of cybersecurity management
- SMBs need to increase protection of Windows applications without increasing management complexity



Showing 4659 of 4659.

☐	Blocked at	Application data	Endpoint	Rule	Policy	User
☐	12/08/2022 1:12:09 PM	C:\Users\vmadmin\Desk...	plee-win11	!plee simple single app n...	! plee AppBloc3	plee-win11\vmadmin
☐	12/11/2022 5:38:59 PM	C:\Program Files\Micros...	plee-win11	! plee Digital Cert - Micro...	! plee DANGER DO NOT USE	plee-win11\vmadmin
☐	12/08/2022 10:32:02 AM	C:\Program Files (x86)\...	DESKTOP-84JC3G8	–	vpa-policy	DESKTOP-84JC3G8\VM-...
☐	11/16/2022 1:50:41 AM	C:\Program Files\Googl...	DESKTOP-SR93H6I	chrome	Roshni-test	DESKTOP-SR93H6I\Ros...
☐	11/21/2022 4:04:12 PM	C:\Windows\assembly\...	plee-win11	! plee block c:\Windows	! plee DANGER DO NOT USE	plee-win11\vmadmin
☐	12/08/2022 1:33:59 PM	C:\Users\vmadmin\Desk...	plee-win11	!plee simple single app n...	! plee AppBloc3	plee-win11\vmadmin
☐	12/08/2022 9:43:01 PM	C:\$WINDOWS.~BT\Sou...	NCS-QA-WIN11X64EN	–	@Noodle EPP - NCEP4	NCS-QA-WIN11X64\ncst...

[1] Verizon 2021 and 2022 *Data Breach Investigations Report (DBIR)*

[2] Hiscox. *Cyber Readiness Report 2022*. A commissioned Forrester consulting report.

Block Vulnerable Applications

2021 and 2022 were record years for the number of Common Vulnerabilities and Exposures (CVEs) reported. To protect your data, you need to lock those potential entry points. But even large enterprises with vast resources struggle to patch vulnerabilities across network endpoints. In conjunction with our Vulnerability Assessment capability, Application Block provides a simple, effective and safe alternative to the complex, time-consuming task of testing and applying patches:

- Use Vulnerability Assessment to identify applications with known vulnerabilities.
- Use Application Block to blacklist the applications with vulnerabilities that either don't have patches or that have a patch you don't have time to test and deploy.

By blocking unpatched applications with known vulnerabilities, you prevent cybercriminals from using those vulnerabilities to breach your network and encrypt, steal or disable your data.

Verify Data Protection Regulation Compliance

Depending on your industry, you might be responsible for complying with data protection regulations, such as these:

- Children's Internet Protection Act (CIPA), which applies to all libraries and schools
- Health Insurance Portability and Accountability Act (HIPAA), which applies to all HIPAA-covered entities, including SMBs that offer employer-sponsored health plans
- General Data Protection Regulation (GDPR), which applies to organizations that do business with a European country

Failure to comply with regulations can cost you. Schools that fail to verify compliance with CIPA don't qualify for E-rate discounts; HIPAA violators can rack up penalties of up to US$25,000; and GDPR non-compliance can result in fines of up to €20mn. With Application Block, you can view and save reports to easily demonstrate your compliance with data regulations. You can also use these reports to satisfy governance boards or to meet cyber insurance requirements.

Business Benefits

- Strengthen your cybersecurity posture
- Increase endpoint protection without increasing the complexity of cybersecurity management
- Identify and block untrusted applications with convenience and ease
- Minimize the risks and costs associated with cyberattacks by blocking untrusted applications and those that are known to be vulnerable and unpatched
- Avoid fines for non-compliance through reports that verify the effectiveness of your application blocking efforts
- Promote end user productivity by blocking Windows applications that serve only to distract and waste time

Promote End User Productivity

Employees know they should not be playing games or using their work computers for personal endeavors—but that doesn't mean they're following the rules. Application Block offers an easy way to prevent users from running or launching Windows applications that serve no business purpose. Used in conjunction with our DNS Filtering capability, you can easily ensure that users don't run Windows and web-based applications that only distract them.

Security Advisor Integration

Security Advisor complements Application Block to optimize the organization's security posture. It evaluates the security level, provides a health score, and recommends proper action for increasing the score.

Industry-Leading Technology

ThreatDown, powered by Malwarebytes, provides innovative capabilities for ransomware detection and remediation, including behavior-based detection and ransomware rollback. We leverage years of security expertise in remediation to provide you with solutions powered by threat intelligence from millions of ThreatDown-protected endpoints, both business and consumer. The ThreatDown API makes it easy to integrate our security products with SIEM, SOAR, and ITSM solutions to further drive automation and compatibility. ThreatDown, powered by Malwarebytes, ensures a high ROI and low TCO, and has a reputation for superior service and support.

ThreatDown™
Powered by Malwarebytes

https://www.threatdown.com/ corporate-sales@malwarebytes.com 1.800.520.2796