



Faronics
ANTI-EXECUTABLE™

Stop Threats Before They Start by Blocking Unauthorized Executables

Today's sophisticated threats like zero-day attacks, mutating malware and advanced persistent threats necessitate an approach that goes beyond a traditional antivirus solution. By ensuring only approved applications are allowed to run on a computer, Faronics Anti-Executable blocks such unknown threats that can bypass your antivirus solution.

Staged Deployment

Learn from users interactions and build a comprehensive control list and move from audit mode to partial or full protection mode.

1 AUDIT

2 ENFORCE

3 MONITOR AND REMEDIATE

- ▣ **Cutting Edge Security**
Protects users from unknown threats such as zero-day attacks, mutating malware, advanced persistent threats and sophisticated attacks.
- ▣ **Granular Control**
Allows organizations to enjoy the benefits of application control such as publisher-based approvals, policy-based control, and protection at the local machine level.
- ▣ **Ransomware Prevention**
Optimizes system settings to overcome vulnerabilities and get maximum prevention from ransomware attacks.
- ▣ **Boosts IT Productivity**
Accelerates IT productivity with an automated initial set-up, standardized configuration, central management, and reduced IT support tickets.
- ▣ **Operational Savings**
Ensures computers, systems and bandwidth are used for intended purposes.
- ▣ **Manage with a Web-based Console**
Management, deployment and configuration are made possible via a single web-based console or a mobile app.

Did You Know?

It takes

11.6 days

for antivirus vendors to catch new malware.

- Cyveillance

“Faronics Anti-Executable is crucial to preserving mission-critical law enforcement systems to ensure reliability and security with minimal downtime and with the least reliance on IT personnel.

- Los Angeles Police Department Information and Communication Services Bureau



Faronics Anti-Executable provides security beyond an antivirus by blocking unauthorized programs – whether malicious, unlicensed or simply unwanted – from ever executing.

Key Features



Application Control

Application whitelisting to prevent malware, ransomware, and zero-day attacks. Authorize or prevent the execution of files, including .exe, .scr, .jar, .bat, .com, .vbs, .dll, .ps1 based on hash value, digital signatures and publishers.

Interactive Dashboard

Review application violation information in the context of individual files or computers and take informed actions using dynamic and filterable widgets and grids. Make informed decisions on when to switch deployment stages.



Audit Mode

Log all application launches and software installations, without enabling protection. Use the Staged Deployment option to move to partial or full protection only after a comprehensive control list is built.

Did You Know?

The average consolidated total cost of a data breach is **\$3.8 million**, while the cost incurred for each lost or stolen record containing sensitive and confidential information is **\$154**.

- Ponemon Institute



Real-time Alerts

Define alert thresholds so administrators can receive proactive notifications for any unauthorized or malicious activity. Receive notifications via the management console, email, or mobile app.



Execution Control List

Use multiple levels of control to create a list of allowed or blocked applications, either centrally across different policies or locally on the computer.



Trusted Publishers

Automatically authorize all updates from a specific publisher like Microsoft or Adobe.



Comprehensive Reporting

Generate reports of all violations, blocked programs, and activity, including which programs are causing the most violations and which computers have the highest number of violations.



Trusted Users & Groups

Ensure power Windows users or groups are free from restrictions while others are restricted with applied policies.



Deep Freeze & AV Integration

Automatically switches to Maintenance Mode upon a Deep Freeze maintenance event. Integrates with Faronics Anti-Virus to ensure the initial installation scan is free from malware.

“Extensive testing of Faronics Anti-Executable reveals it to be an excellent product with well thought out features

- Cognetic Systems, Inc.

To learn how your computing environment can benefit from Faronics Anti-Executable, visit www.faronics.com

System Requirements

Faronics Anti-Executable works with any computer running Windows XP SP3 (32-bit), Windows XP SP2 (64-bit), Windows Vista (32/64-bit), Windows 8.1 (32/64-bit), Windows 10 (32/64-bit).



USA

5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA
Call Toll Free: 1-800-943-6422
Fax Toll Free: 1-800-943-6488
sales@faronics.com

CANADA

1400 - 609 Granville Street
PO Box 10362 Pacific Centre
Vancouver, BC, V7Y 1G5
Call Toll Free: 1-800-943-6422
Call Local: 1-604-637-3333
Fax Toll Free: 1-800-943-6488
sales@faronics.com

EUROPE

8 The Courtyard, Eastern
Road, Bracknell, Berkshire,
RG12 2XB, United Kingdom
Call Local: 44 (0) 1344 206 414
sales@faronics.eu

SINGAPORE

6 Marina Boulevard
#36-22 The Sail At Marina Bay
Singapore, 018985
Call Local: +65 6509 4993
Fax Local: +65 6722 8634
sales@faronics.com.sg