PGP® Endpoint Application Control

Protecting systems from unauthorized and malicious software

Part of the PGP® Encryption Platform

Benefits

- **Protects against unknown applications** – Proactive, automatic policy enforcement explicitly allows only trusted and authorized software to protect systems from the risks of unauthorized or malicious applications.
- **Reduces administrative and helpdesk burdens** – Whitelist approach to security eliminates the need to constantly update and maintain systems against unknown application threats.
- **Ensures business continuity** – Denial of unauthorized applications prevents proliferation of known and unknown application threats.
- **Enables compliance** – Audits of application execution attempts and policy changes helps organizations demonstrate compliance with industry and governmental regulations.
- **Transparent user experience** – Automatic, background operation does not affect user productivity.

PGP Customer Spotlight

"PGP solutions enable our employees to protect sensitive data and maintain our excellent industry reputation."

Rhonda Johnson
Program Manager
ACS

Efficient and automatic application threat protection

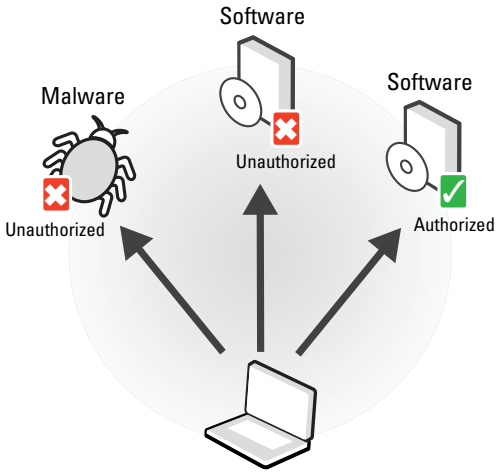
Unauthorized and malicious software poses a risk of compromising user privacy, affecting business continuity and the ability to demonstrate compliance. And each time a new malware threat appears or unsupported software causes a compatibility conflict, the IT group has to interrupt other projects to resolve the issue. They need ways to use technology to reduce the operational inefficiencies of continually updating antivirus signatures to protect systems and information are protected or re-imaging laptops because of software conflicts that lead to instability.

Automatically protect against known and unknown threats

PGP® Endpoint Application Control proactively protects systems from unauthorized or malicious software applications by automatically enforcing policies that explicitly allow only trusted and authorized software. PGP Endpoint Application Control uses whitelist technology to define authorized and trusted software applications.

Increase operational efficiency

PGP Endpoint Application Control improves operational efficiency by eliminating the burdens of continually updating and maintaining systems to protect against existing and new threats.



PGP® Endpoint Application Control

Proactive and Automatic Protection

PGP® Endpoint Application Control reduces the risk of data compromise caused by unauthorized or malicious software applications.

- **Automatic policy enforcement** – Protects systems from application threats without relying on user intervention.
- **No more signatures to update** – Whitelisting technology provides automatic protection and denies known and unknown application threats.
- **Automated application discovery** – Set up whitelists rapidly.
- **Script/macro protection** – Flexible policy definitions provide enforcement to protect script and macro operation.
- **Always-on protection** – Local hash and permissions ensure continual protection when systems are offline.

Business Continuity

Reduces helpdesk and administrative burdens and supports business as usual without worry about application threats.

- **Zero-downtime threat protection** – Prevents network proliferation of malicious application software.
- **Worry-free patch updates** – Flexible policies allow automatic authorization of Microsoft® application patches.

Supports Compliance

PGP Endpoint Application Control helps prove compliance in the event of an audit.

- **Detailed audit trails** – Provide detailed information about application execution attempts and actions, along with proof of software license compliance.

Transparent User Experience

After deployment of PGP Endpoint Application Control, operation is completely transparent to users.

- **Background protection** – Users continue to work as usual. The software automatically protects against unauthorized and malicious software applications, ensuring data protection without requiring user intervention.
- **Single Sign-on** – Integration with Microsoft Windows® Active Directory and Novell® eDirectory™ enable users to log in with existing credentials, providing data protection without requiring users to remember another set of authentication credentials.
- **Local authorization** – Users can authorize applications without compromising administrative oversight. Detailed logs and audit trails track all application activity.

Technical Specifications

PGP Endpoint Application Control supports Microsoft Windows 2000 Professional® (SP4 or later), Windows XP® (SP2 or later), and Windows Vista® (32- and 64-bit editions). PGP® Endpoint Administration Server supports Windows Server® 2000 and Windows Server® 2003. For complete technical specifications, please visit www.pgp.com.

PGP Corporation
www.pgp.com

PGP Corporate Headquarters
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308

EPTACDS090326