Software Execution Control with HEAT Endpoint Security (CPA)

Security Compliance made easy

Many endpoint security compromises occur when new or unknown software executes on endpoints. Often users are able to execute software or utilize applications that are not managed and secured by administrators.

Software Execution Control solutions allow administrators the ability to limit the applications and services that are allowed to run on a particular platform, providing improved manageability and a reduced attack surface. It's a critically important component of a layered defense strategy and complex task for any IT organization.

To reduce this complexity yet assure security compliance, HEAT Endpoint Security has achieved Commercial Product Assurance by the UK National Technical Authority CESG, and has been successfully verified against the Software Execution Control Security Characteristic at Foundation Grade.

HEAT Endpoint Security is used to limit which software applications and services are able to run on an operating system and controls the attack surface of a platform by reducing the number of potential vulnerabilities, to help mitigate the impact of attacks. And it's made even more powerful with the CPA Add-On that provides easy to follow checklists and the easy button to enforce security compliance.

"Easy Button" option to achieve security compliance

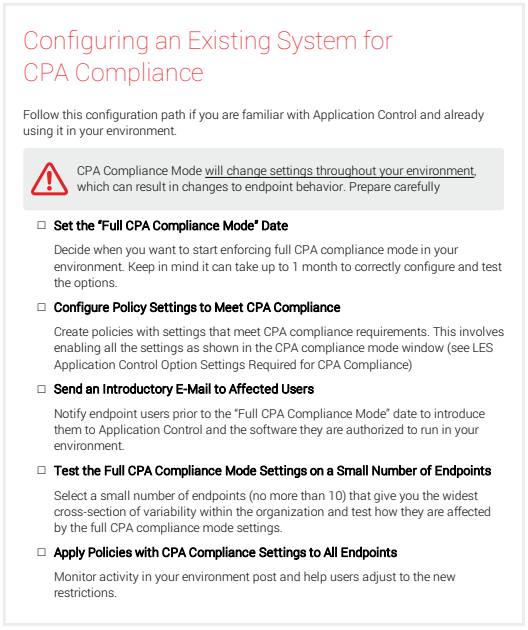
HEAT Endpoint Security CPA offers an "easy button" solution that immediately achieves a secure configuration as recommended for CESG compliant endpoints. When enabled, endpoints are security compliant.

CPA build standard

The CPA build standard describes the principles and practices for building the product right and provides assurance that products are designed with security and quality in mind. The build standard covers aspects including:

- Configuration management
- Build process
- Bug reporting and remediation
- Test process
- Coding standards
- Change control
- Physical security
- Network security
- Personnel security

While the CPA build standard is about building the product right, the CPA security characteristic is about building the right capabilities into the product.



Configuring an Existing System for CPA Compliance

Follow this configuration path if you are familiar with Application Control and already using it in your environment.

CPA Compliance Mode will change settings throughout your environment, which can result in changes to endpoint behavior. Prepare carefully

- ☐ **Set the "Full CPA Compliance Mode" Date**

  Decide when you want to start enforcing full CPA compliance mode in your environment. Keep in mind it can take up to 1 month to correctly configure and test the options.

- ☐ **Configure Policy Settings to Meet CPA Compliance**

  Create policies with settings that meet CPA compliance requirements. This involves enabling all the settings as shown in the CPA compliance mode window (see LES Application Control Option Settings Required for CPA Compliance)

- ☐ **Send an Introductory E-Mail to Affected Users**

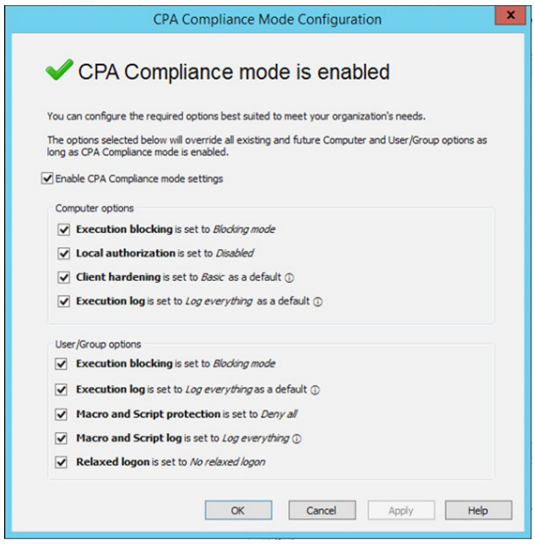
  Notify endpoint users prior to the "Full CPA Compliance Mode" date to introduce them to Application Control and the software they are authorized to run in your environment.

- ☐ **Test the Full CPA Compliance Mode Settings on a Small Number of Endpoints**

  Select a small number of endpoints (no more than 10) that give you the widest cross-section of variability within the organization and test how they are affected by the full CPA compliance mode settings.

- ☐ **Apply Policies with CPA Compliance Settings to All Endpoints**

  Monitor activity in your environment post and help users adjust to the new restrictions.



Security Characteristics for Software Execution Control

Software Execution Control forms a key component of a well-configured endpoint by providing system administrators the ability to configure and constrain the software that is running on systems. In order to meet the requirements of the Software Execution Control security characteristic, products are evaluated against a range of criteria including:

- Stack protection
- Data execution protection
- Address space protection
- Administrator authentication
- Policy enforcement
- Default deny
- Enforcement code protection
- Logging of execution attempts

One of the challenges faced by IT organizations trying to create a secure environment is that security solutions are highly configurable and it can be difficult to configure them correctly and eliminate risk. In order to be compliant with the security characteristic requirements, IT must ensure the product is securely deployed and thereby eliminate any security risk associated with misconfiguration. In summary, compliance with the security characteristic ensures that best practice security configurations are adhered to.

Download a free trial of Endpoint Security for CPA compliance now!

HEAT software

HEAT Software USA Inc.
490 N. McCarthy Blvd. Milpitas, CA 95035 USA
P. +1 800.776.7889 or +1 408.601.2800