HEAT Endpoint Security Device Control

Enforce Security Policies for Removable Devices,Media and Data

Data leakage caused by the accidental or sometimes malicious use of removable devices and/or removable media has reached alarming levels. In fact, according to Verizon, 2011 boast[ed] the second-highest data loss total since we started keeping track in 2004.[1]

Organization-wide Device Management

To enhance productivity, organizations need to provide employees and partners access to data. With more employees working remotely, access is required from outside the network. But the potential impact of data loss, be it accidental or malicious, is a very real concern. And today, removable media / devices are the most common data leakage routes – no file copy limits, no encryption, no audit trails and no central management.

The information contained in customer and corporate data, such as personally identifiable information (PII) and intellectual property (IP), is worth billions to some. And the costs for recovery of data and lost business are rapidly rising as well with the average yearly cost over the 2009 – 2013 timeframe now estimated to be $200 per record.[2]

Introducing HEAT® Endpoint Security Device Control:

- Enforces security policies on removable device usage and data encryption
- Centralizes management of devices and data using a whitelist / "default deny" approach
- Enables secure use of productivity-enhancing tools while limiting the potential for data leakage and its impact
- Provides additional layer of protection malware introduced via physical means
- Allows for monitoring of all file transfers to printers and physical media

Key Features

- Whitelist / "Default Deny"
- Policy Enforced Encryption for Removable Storage
- Data Copy Restriction
- File Type Filtering
- Temporary / Scheduled Access
- Context-Sensitive Permissions
- Centralized Management / Administrators' Roles
- Role Based Access Control
- Tamper-proof Agent
- Flexible / Scalable Architecture

Key Benefits

- Protects Data from Loss / Theft
- Enables Secure Use of Productivity Tools
- Enhances Security Policy Enforcement
- Delivers Precise Control with Access Limits
- Prevents Malware Infiltration via Physical MeansMapping of centralized and decentralized management structures

"One of the main benefits in deploying HEAT Device Control is its whitelist feature, which ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in. Flash memory USB devices represent a significant risk with the potential to steal company data or introduce "malware", which could render the computer unusable and quickly infect other PCs on the same network. Device Control is really strong, easy to use product which is why Barclays chose this solution."

Paul Douglas
ADIR Desktop Build Team Manager
Barclays

[1]Verizon, 2012 Data Breach Investigations Report (April 2012)
[2]Ponemon Institute, 2014 Cost of a Data Breach Study (May 2014)

How HEAT® Device Control Works

1. Discover: all removable devices that are currently or have ever been connected to your endpoints.

2. Assess: all "plug and play" devices by class, group, model and/or specific ID and define policy through a whitelist approach.

3. Implement: file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.

4. Monitor: all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.

5. Report: on device and data usage to document compliance with corporate and/or regulatory policies.

Key Features

Whitelist / "Default Deny"

Assigns permissions for authorized removable devices and media to individual users or user groups; by default, devices / media and users not explicitly authorized are denied access.

Policy Enforced Encryption for Removable Storage

Centrally encrypts removable devices (such as USB flash drives) and media (such as DVDs/CDs), plus enforces encryption policies when copying to devices / media.

Data Copy Restriction

Restricts the daily amount of data copied to removable devices and media on a peruser basis; also, limits usage to specific time frames / days.

File Type Filtering

Controls file types that may be moved to and from removable devices / media on per-user basis; helps limit malware propagation.

Centralized Management / Administrators' Roles

Centrally defines and manages user, user groups, computer and computer groups access to authorized removable devices / media on the network; by default, those devices / media and users not explicitly authorized are denied access.

Temporary / Scheduled Access

Grants users temporary / scheduled access to removable devices / media; used to grant access "in the future" for a limited period.

Context-Sensitive Permissions

Access / usage policies remain enforced regardless of connection status, and can be tailored to whether the endpoint is connected to the network or not.

Role-based Access Control

Assigns permissions to individual users or user groups based on their Windows Active Directory or Novell eDirectory identity, both of which are fully supported.

Tamper-proof Agent

Installs agents on every endpoint on the network; agents are protected against unauthorized removal – even by users with administrative permissions. Only Device Control Administrators may deactivate this protection.

Flexible / Scalable Architecture

Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.

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