HEAT software

EMSS Features Summary

Common Platform Features

- **Intelligent, workflow-based console** (single console, dashboards, pre-defined views)
- **Role-based access control** (granular controls, distinct views)
- **Active Directory LDAP integration** (RBAC, applying policies to directory users/groups)
- **Built-in asset discovery and agent deployment** (discovery, remote push, schedules)
- **Flexible endpoint management** (agent policies, SSL comm., client hardening)
- **Effective inventory management** (HW, SW, OS, network)
- **Enhanced Wake-on-LAN** (zero-touch patching, WOL relays)
- **Virtual infrastructure aware** (auto-tagging/grouping, RBAC)
- **Remote systems management/system tools** (RDP, VNC, PuTTY, PING, NSLOOKUP)
- **Integrated reporting** (widgets, standard/LRS templates)
- **Expandable in future** (additional licenses, more modules)
- **Scalable** (10K-15K per server, Caching Proxy, Internet-facing)

Patch and Remediation Features (PR)

- **Single Solution for Heterogeneous Environments:** Vulnerability audits and remediation with wide support across major OS platforms (Windows, including Windows 10 and Server 2012 R2, etc.; Linux; Solaris; HP; Mac OS; etc.) — all from one single console
- **Industry's Largest Microsoft and Non-Microsoft Application Vulnerability Content:** Includes Microsoft security and non-security content, and the largest repository of Adobe vulnerability content.
- **Simplified Entitled Content Rights Management Across Supported Entitled Platforms:** Seamlessly manage 3rd party vendor credentials via an integrated Credentials Manager for Red Hat Linux, Oracle Linux, SuSE, Solaris, and HP-UX.
- **Distributed Patch Payload Caching:** Deploy patches to a distributed endpoint environment via elevated distribution points.
- **Vulnerability Management for both Physical and Virtual Assets:** Virtual awareness provides confidence in successfully managing your virtual datacenter infrastructure.
- **Advanced Patch Deployment and Reboot Control:** Customize patch deployments with advanced tools, e.g. chain multiple patches, set custom flags, control reboot/dismiss options.
- **Policy Baselines for Automation of System Management Tasks:** Automate time-consuming tasks across the entire network, including automated scheduling of disk defragmentation tasks, and policy enforcement for account, device control, domain, network, and system policy security settings.
- **Flexible Operating Hours:** Administrators can define specific days and intervals of time during which the agent can communicate with the server and perform operations, in granular half hour increments.
- **Software Deployment and Removal:** Policy-based installation of new and updated software packages. Quickly identify installed software on endpoints. Automatic removal of outdated or unauthorized software. Ongoing monitoring and baseline enforcement.
- **Custom Content Wizards:** Extends the capabilities of Patch and Remediation with custom scripting capabilities. Custom detection, deployment, patching, and remediation of 3rd party and in-house content. Create custom checks and remediation to detect and alleviate security risks and operational efficiency issues

in your environment. Examples include: making sure AV is installed, distributing 3rd party patches, following application deltas, and more.

- **Power Management:** Leverages your Patch and Remediation infrastructure to centralize management and enforcement of power policies across complex environments. Policies include: standby, hibernation and sleep timing setting based on user and system inactivity.
- **Continuous Policy Enforcement of Patches, Remediations and Configurations:** Automatically enforces patches, configurations, remediations and other custom and repetitive tasks. Baseline policies can be easily exported and applied across multiple groups and servers for consistency.
- **Multi-Patch Deployments:** Delivers multiple patches to multiple computers in one distribution.
- **Custom Patch Lists:** Create lists of patch content in your enterprise useful for many scenarios, including content that is used frequently in your enterprise, content that will only be deployed once, cache patch content from the Global Subscription Service, as well as reporting purposes.
- **Do Not Patch Feature:** The Do Not Patch feature allows you to exclude patch deployment for endpoints or groups that you choose. This feature can be used to prevent patches that negatively impact an endpoint from being deployed to it. It also allows you to track the reason that you've excluded the patch.
- **Subscription Service:** Automatic and secure identification and notification of the latest patch vulnerabilities across multiple platforms and applications.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

Content Wizard Features (CW)

- **Flexible Content Creation and Management:** Easy-to-use wizard-based creation of custom software patch remediation packages as well as local security policy and system management configurations. Custom detection, deployment, patching and remediation packages can be created to address a wide range of software and configuration threats, distribute or remove applications and files, enforce configuration policies, and more.
- **Wizard-based Content Authoring:** A process-driven tool that guides users through the patch upload process and automatically creates the fingerprints for the patch being uploaded.
- **Centralized Endpoint Power Management Policy Wizard:** Centralizes management and enforcement of power policies across complex environments, including standby, hibernation and sleep timing setting based on user and system inactivity.
- **Custom Script Management and Development:** Centrally deploy, manage and report on all new and existing IT scripts. Automatically monitor and report on scripting actions taking place throughout your environment. A template based approach to the creation of remediation scripts which allows novice users to quickly author remediation scripts (VBScript, JavaScript, command line) to remedy identified system problems.
- **Enforcement of Local Security Configuration Policy:** New policy wizard simplifies setting and enforcement of local security configuration policies, such as: disabling guest accounts, turning off unnecessary services, enforcing password complexity and length and forcing unattended systems log off. Sets policies based on industry best practices template with 24 pre-configured checks and policy elements that can be added and modified based on your specific security policies.
- **Software Distribution and Removal:** Policy-based installation of new and updated software packages. Quickly identifies installed software on endpoints. Automatically removes outdated or unauthorized software. Ensures ongoing monitoring and baseline enforcement.

- **Content Community:** Facilitates content exchange and information sharing within the corporation via a company internal ftp site accessed through Content Wizard.
- **Patch Search by Title:** Provides rapid intuitive search of existing patches.
- **Display Fingerprint Type based on OS:** Filtering based on OS enables quick location of relevant fingerprints.
- **Flexible Content Management:** Allows the deletion of obsolete patches.
- **Rapid Content Development:** Intuitive, easy-to-use interfaces allow the development custom packages in minutes to react to the latest threats.
- **Content Creation Across Heterogeneous Environments:** Content Wizard allows development of packages across a multitude of Operating Systems.
- **Immediate Content Distribution:** Content is seamlessly ported into your Patch and Remediation repository for automated, enterprise-wide deployment.
- **Continuous Monitoring:** Custom packages created with Content Wizard can be continually monitored and reported on through the Patch and Remediation interface.
- **Windows Firewall Management:** Defines and enforces firewall policies to provide consistent firewall configurations for Windows endpoints, enabling better compliance reporting and visibility.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

AntiVirus Features (AV)

- **Full Signature Matching Capabilities:** Recognizes, blocks and removes viruses, worms, Trojans and other types of malware such as keyloggers, hijackers and rootkits.
- **Variant and Exploit Detection:** Includes DNA Matching or partial signature matching that can detect components of malware that have been re-used from previous attacks. Exploit Detection detects and stops hidden malware that has been injected into otherwise benign file types such as .PDFs.
- **Behavioral Analysis Detection:** SandBox behavioral analysis runs suspect executables in a safe emulation to look for malicious behavior and identify sophisticated zero-day malware.
- **Potentially Unwanted Applications (PUA) detection:** These are applications the user consents to installing, yet annoy, or comprise privacy and security. These include adware, toolbars, and other browser add-ons. PUA detection capability is provided.
- **Rootkit Detection:** Rootkits, which are software that give unauthorized users full access to your endpoints while completely concealing their existence from the OS, can be detected.
- **Real-time Scanning:** Enables malware scanning of files as they are being opened for reading, writing, or execution.
- **Scheduled Scanning:** Enables malware scanning of entire endpoints on a predetermined schedule.
- **On-demand Scanning:** Enables malware scanning of specific endpoint on an as-needed basis.
- **Granular AV Policy Management with CPU Throttling:** Provides the ability to create and schedule multiple AV scans per endpoint with different scan settings at different times (e.g., daily scan with light scan settings and weekend scan with heavy scan settings).
- **Smart Cache Capability**: This feature will keep track of the known-good files not changed since the last scan, and will skip scanning them for extremely enhanced performance.
- **Comprehensive Malware Removal:** Removes or quarantines any malware identified on endpoints.
- **Automatic Signature Updates:** Downloads the latest signatures and automatically updates endpoints via optimized configuration settings.

- **Action Center Integration:** It is integrated with the Windows Action Center so that it will show status of antivirus and antispyware.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

Application Control Features (AC)

- **Application Control/Whitelisting:** Identifies and controls what applications are currently in your IT environment or can be added to your IT environment. Automatically identifies trusted software that is authorized to run and prevent all other applications from executing – whether they are malicious, untrusted or merely unwanted. Supports all executables including typical .EXEs, .DLLs, .COMs, etc.
- **Advanced Memory Protection:** Provides integrated protection against memory injection attacks by validating all new processes, even those initiated by approved running applications.
- **Application Reputation Scoring:** The Endpoint Integrity Service (EIS) provides explicit identification and application risk rating information at both admin and end user levels.
- **Easy Auditor:** Allows administrators to observe and audit whitelisting policies to ensure business needs and security considerations are achieved before enforcement actions are applied. Ensures business needs and security considerations are achieved before enforcement actions are applied.
- **Easy Lockdown:** Takes an automated "snapshot" of each endpoint, which is used to create a whitelist and begin enforcement of whitelist policies. Creates a local whitelist immediately and begins enforcement of whitelist policies.
- **Automated Trust Engine:** Automates whitelist updates based on trust policies, including Trusted Publisher, Trusted Updater, Trusted Path, and Local Authorization.
- **Local Authorization:** Provides users with the ability to self-authorize new applications not already on whitelist or in denied apps group.
- **Application Library:** Aggregates all data collected by local snapshot scans and provides grouping and filtering options for application policy management.
- **Denied Application Policy:** Discovered applications in the Application Library can be easily added to a denied application policy and prevented from executing (blacklist).
- **Application Event Log:** Provides powerful log analysis and reporting while delivering necessary visibility into endpoint events, including All application events; All applications added by trusted updaters, paths and publishers; All denied application events; Easy Auditor (applications blocked when enforcement is enabled); and Most frequently denied applications.
- **Flexible User- and Machine-based Policy Enforcement:** Active Directory support; User-based policy enforcement; Machine-based policy enforcement; and Hybrid user and machine based policy enforcement.
- **Offline Computer Protection:** Enforces whitelist on endpoints, regardless of whether or not they are connected to the network.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

Device Control Features (DC)

- **Per-Device Permissions:** Granular permissions to control access at device class (e.g., all USB flash drives), device group, device model and/or even unique ID levels; for instance, restrict access rights to a specific device of a company-approved model.

- **Device Whitelisting:** Assign permissions for authorized removable devices (such as USB sticks) and media (such as DVDs/CDs) to individual users or user groups; once in 'enforcement mode' only explicitly authorized devices/media/users are allowed access by default.
- **Flexible Policy with Granular Control:** Permission settings include read/write, forced encryption, scheduled/temporary access, online/offline, port accessibility, HDD/non-HDD devices and much more; can be set for individual and/or groups of users, machines, ports and devices.
- **Read-Only Access:** Define any device (e.g., a floppy drive, DVD/CD writer, USB external hard drive, and so on) as read-only; other device permissions include: write, and encrypt/decrypt restrictions.
- **Temporary/Scheduled Access:** Grant users temporary access to removable devices/media, which can be used to grant access "in the future" for a limited period. Also, limit device usage during a specific time period; allows for development of sophisticated security policies where certain devices can only be used at certain times (e.g., from 9 A.M. to 5 P.M., Monday to Friday).
- **Offline Enforcement:** Permissions/restrictions remain effective even when endpoint is offline; these can be the same as when online or different (see Context-Sensitive Permissions).
- **Uniquely Identify and Authorize Specific Media:** Authorize and manage DVD/CD collections, by granting access to specific users or user groups and encrypting removable media with unique IDs.
- **Context-Sensitive Permissions:** Apply different permissions/restrictions depending on network connectivity status. For example, disable WiFi cards when laptops are connected to the network, but enable them when the machine does not have a wired connection to the network.
- **Device Management:** Detect and manage all devices – including Plug-and-Play and non-standard/user-defined devices – "on the fly" within the system.
- **File Type Filtering:** Restrict and manage the types of files that are moved to and from removable devices (such as USB sticks) and media (such as DVDs/CDs); combine with forced encryption for added protection.
- **Data Copy Restriction:** Restrict the daily amount of data copied to removable devices (such as USB flash drives) on a per-user basis; can also limit usage to specific timeframes/days (e.g., only from 0900 to 1700 during weekdays).
- **Data Loss & Theft Prevention:** Provides organizations with the means to control the use of removable storage devices/media.
- **Extended Control over Portable Devices:** You can apply read-only access, file shadowing, and file copy limits to portable devices like mobile phones and media players that enter your environment.
- **Charging Mode for Portable Devices:** Users can charge their portable devices (mainly mobile phones) without you having to allow read/write permissions.
- **Detailed Forensics:** Provides the in-depth information required to understand the risk posed by data transfers, to report on it for compliance or forensics purposes, and to update policies as business needs dictate.
- **Malware Protection:** Provides an added layer of defense against malware, specifically those being distributed via removable devices like USB flash drives.
- **Keylogger Detection and Enforcement:** This feature protects against keyloggers which are becoming more common in enterprises especially financial organizations.
- **FIPS 140-2 level 2 Validated Encryption:** The HEAT Cryptographic Kernel (HCK), a stand-alone software cryptography module which delivers the core ciphering capabilities, has been FIPS 140-2 Level 2 validated.
- **Policy-based Encryption for Removable Storage:** Use central security policy to force FIPS 140-2 level 2 validated encryption of all removable devices (e.g., USB sticks) and media (e.g., DVDs/CDs) across all endpoints on network.

- **User-Enabled Encryption:** Allow users to encrypt removable devices/media locally using the strongest commercially-available encryption.
- **Portable Encryption:** Enforce policies which enable users to access encrypted devices outside the organizational network, or limit it to network-attached endpoints only.
- **Encrypted Device Browser:** Enable access to EMSS-encrypted devices/media from Mac OS X machines, enabling users to move data both from and to encrypted devices or media.
- **Enforce "Strong" Password Requirements:** Use existing password length and complexity rules in compliance with Microsoft® standards.
- **Password Lockout/Recovery:** Lock users out after five (5) failed attempts; administrators can recover access when passwords are forgotten or user leaves the organization.
- **Detailed Event Logging/Reporting:** Log all device usage and data transfer activity, including all (allowed/blocked) events; all policies by device, machine and/or user; and all file metadata (name, type, etc.) or complete file copy. Also view results via dashboard widgets, interactive reports, or email notifications.
- **Filename Tracking / Full File Shadowing:** Keep a complete copy (i.e., entire file contents) of all files that are read from and/or written to removable devices (e.g., USB memory drives) and media (e.g., DVDs/CDs) on a per-user (or user group) basis using the patented bi-directional shadowing technology. Alternatively, track just file metadata (name, type, size, etc.). Capture all events (e.g., device attached, data transferred, etc.) in logs which are accessible by admin at any time for compliance auditing/forensics.
- **Printed Content Shadowing:** The Printed Content Shadowing feature lets you view the activity of users with print permission. Use it to prevent users from printing confidential information.
- **Syslog Support:** All endpoint event logs are compliant with Syslog protocols.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

Reporting Services Features (RS)

- **Graphical:** Professional reports for the executive level. Effectively show your achievements to your Management.
- **Interactive & Drillable:** High-level data can be investigated & backed up within the same report.
- **Schedulable:** Reports can be automated and emailed.
- **Dynamic, Flexible & Customizable:** Pre-configured reports come out-of-the-box for ad-hoc reports. Reports are customizable to meet further needs.
- **Complementary:** Component of MS SQL – already installed with EMSS No additional investment of or integration with a stand-alone reporting tool.
- **Web-accessible:** Accessible online by any authorized user, with or without EMSS access.
- **Integration with Endpoint Management and Security Suite:** Integrates with other product modules on the Endpoint Management and Security Suite.

