eScan™
Anti-Virus & Content Security

eScan Corporate 360

(with MDM & Hybrid Network Support)

Transforming Enterprise Mobility into Reality

www.escanav.com

sales@escanav.com

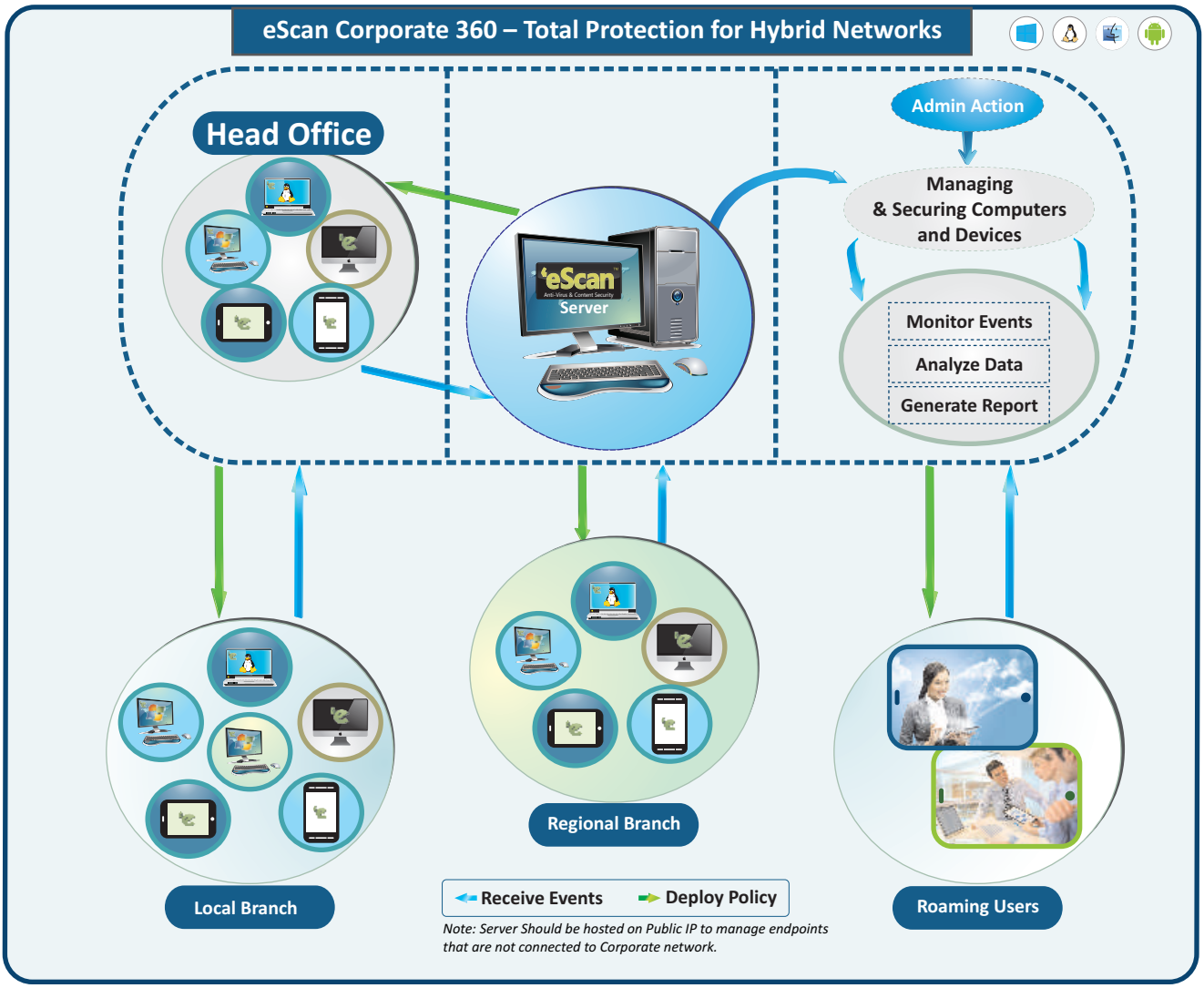
Copyright Information

The Marketing Department
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334, USA.
Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024.
Web site: www.escanav.com
E-mail: marketing@escanav.com

Document Version – eCorp360USP14.1

Release Date – September, 2014

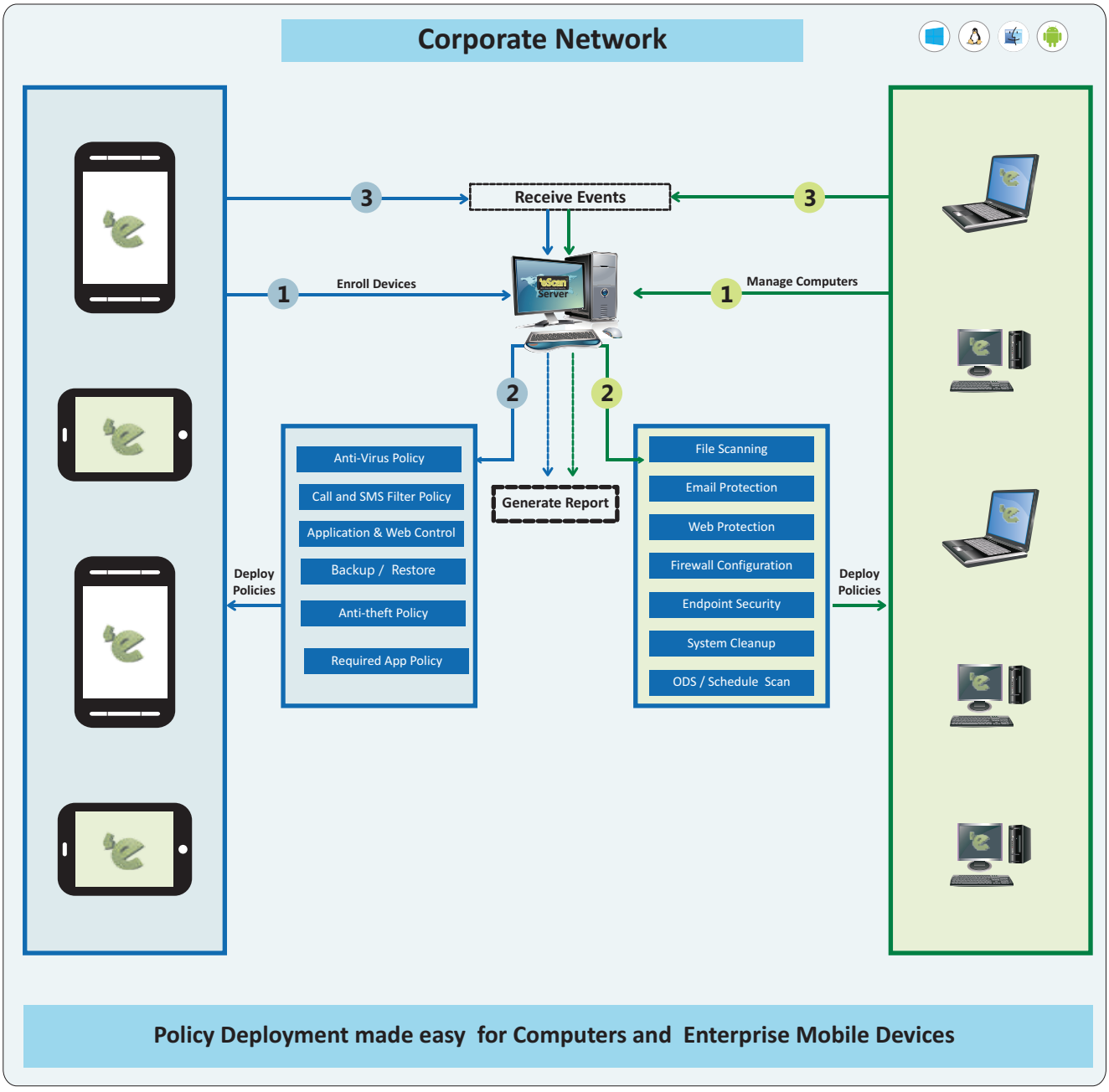
One Solution, One Cost, Total Security



Business world is no stranger to their transformation towards Enterprise mobility and with advancement in technology, progressive incorporation of laptops, smartphones, tablets and hybrids into companies is now a reality. eScan Corporate 360 facilitates Administrator to view security status as well as configure policies and tasks on all endpoints with Windows, Mac, Linux or Android operating systems. eScan increases protection and helps lower your total cost of ownership by reducing administrative overhead as well as the costs associated with managing multiple endpoint security products. It provides a single client that is administered via a single centralized management console on to the endpoints connected to the corporate network. This simplifies endpoint security administration and provides operational efficiencies such as single software updates and policy updates, unified and central reporting, and a centralized licensing and maintenance module. It is a revolutionary product with advanced security features that guarante maximum security to endpoints connected to your corporate network.

eScan offers advanced IT management through comprehensive Asset Management, managing Print Activity and customized real-time Reporting modules for all endpoints. It neutralizes requirement of any other third party software for meeting your specific requirements in managing, monitoring and controlling security on computers and Android devices through its state of the art secured and web based management console. Entire functionality is incorporated in single console so you don't have to allocate any extra budget for bringing in IT security risks in-line with your business objectives.

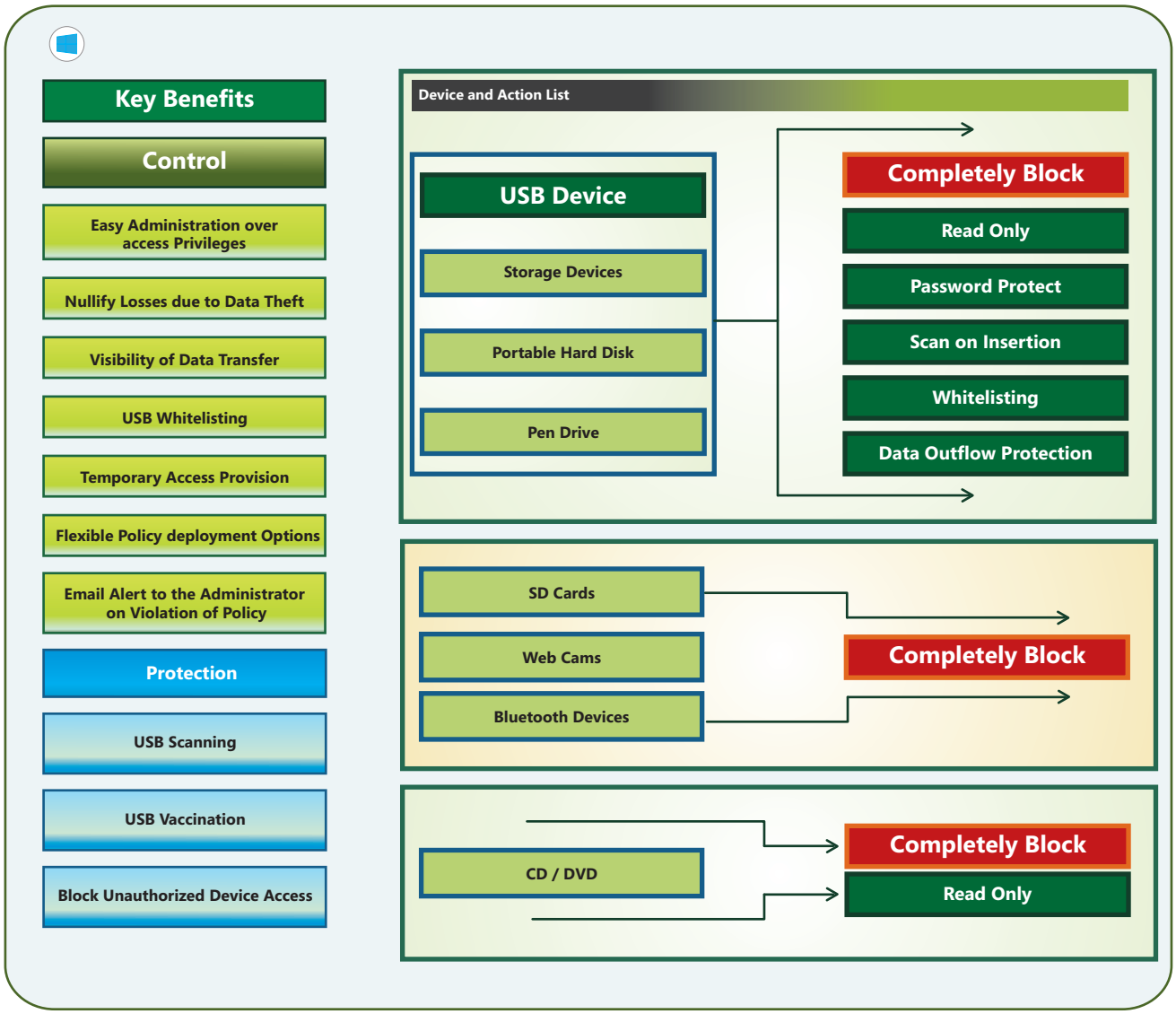
Secure, Easy, and Scalable Policy Deployment



eScan Corporate that includes mobile device management, facilitates deployment of security policies on computers as well as devices through an easy-to-use web based eScan Management Console. These policies are the rule sets that ensure total security of Devices as well as computers where eScan is installed, facilitating centralized management and providing visibility into various IT assets in the enterprise.

Advanced Application, Device and Web Control

Device Control



eScan's advanced device control feature helps in monitoring USB devices that are connected to Windows or Mac endpoints in the network. On Windows endpoints, administrators can allow or block access to USB devices such as webcams, CD-ROMs, Composite devices, Bluetooth devices, SD Cards or Imaging device.

Unauthorized access to USB devices can be blocked using password protection, thus preventing data leakage and stopping malware infection through USB devices.

On Mac endpoints, administrators can block USB access.

Data theft Notification

Many times access to the USB port is misused and data pilferage becomes a common occurrence causing potential damage to the organization as intellectual property falls into wrong hands. A sub-feature in eScan's Device Control enables to send notifications to the administrator of the web-console when any data (which is not read-only) on the client system's hard disk is copied to the USB. Device Control, thus ensures that data theft is completely eradicated leaving no scope for misuse of confidential data.

One Time Password

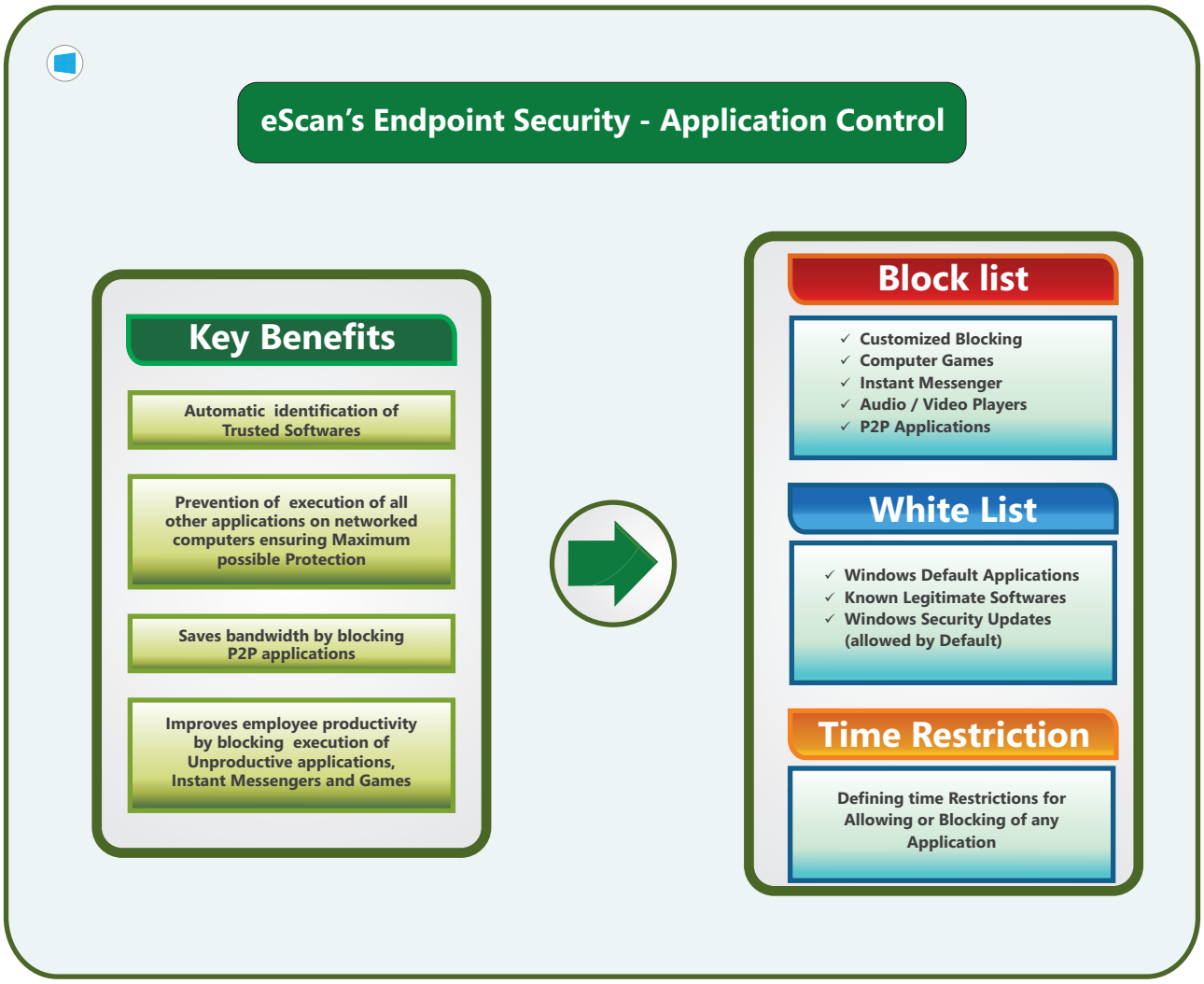
eScan's password protection restricts user access from violating a security policy deployed in a network. For example, the administrator has deployed a security policy to block all USB devices, but someone wants to access it for a genuine reason, for example – making a sales presentation residing on a USB pen drive. How would an administrator give the user an access without violating the current security policy? OTP is the answer for the same, by generating one time password for a specified period of time for that specific client computer to disable the module without violating existing policy.

USB Vaccination

For preventing spread of autorun -based malware infection eScan provides an advanced USB Vaccination feature that replaces the autorun.inf file present on any USB Drive with its own autorun.inf file that cannot be modified or deleted manually or by any malicious program. This file is created in such a way that it does not allow malicious program to execute on any system to which the USB Drive is mounted on, irrespective whether the said system is protected by AV or not. The vaccinated drive can be used normally for copying and transferring files from one computer to other without any concern for malware spreading through USB drives even if the PCs are not protected by any antivirus. The drive will remain vaccinated till it is formatted by the user or de-vaccinated using eScan.

USB vaccination is an advanced protection offered in conjunction with the USB whitelisting / black-listing feature, which ensures that the corporate security policies are adhered to even when the white-listed USB is used on systems which are not under the active protection of the Corporate Antivirus. Users may find this feature convenient as the perceived threat from USB based malware is nullified by the virtue of Vaccination.

Application Control

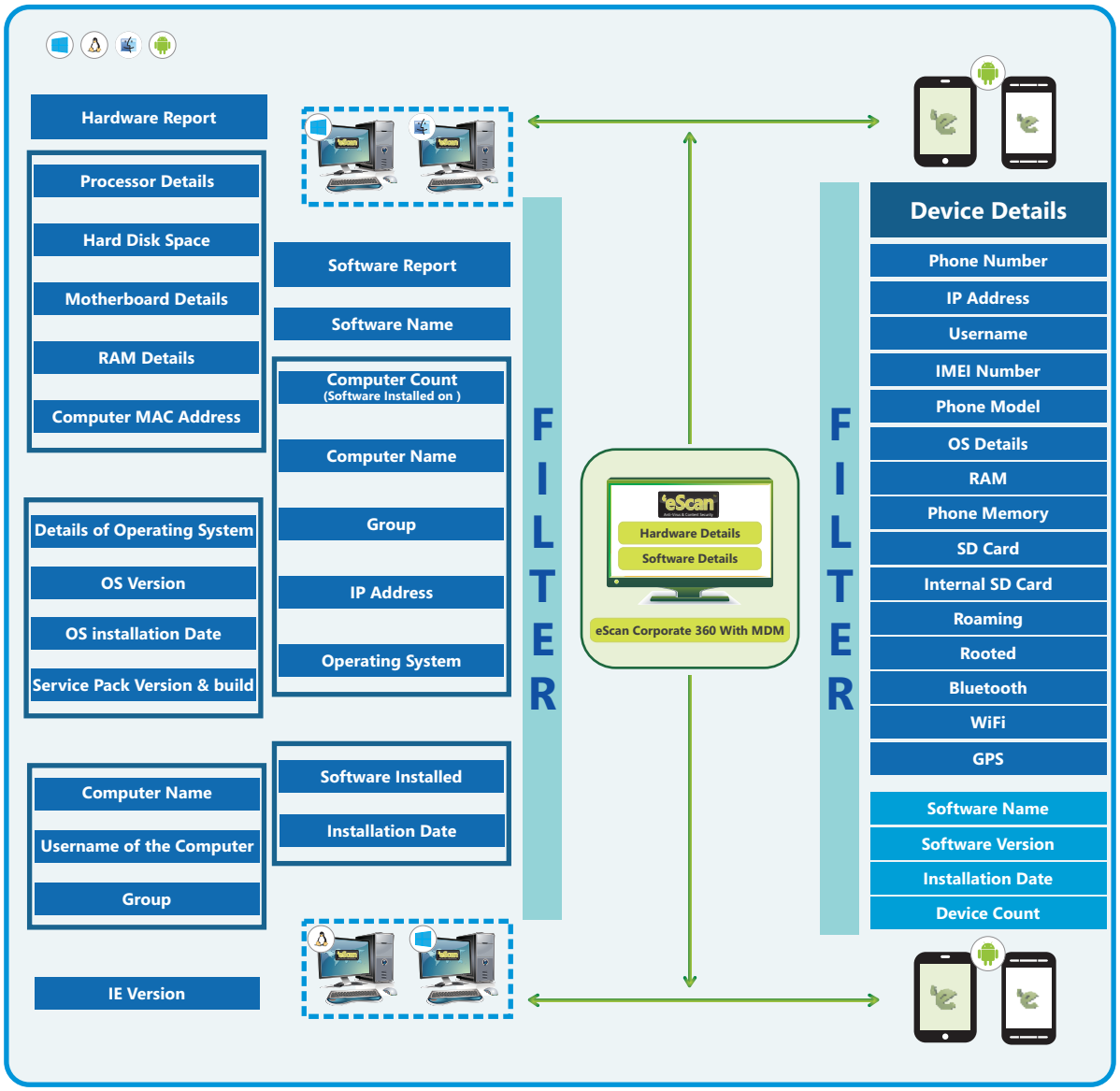


eScan's effective Application Control module allows you to block/whitelist and define time restrictions for allowing or blocking execution of applications on Windows endpoints. It helps in accessing only the whitelisted applications, while all other third-party applications are blocked. On Android endpoints, by default all downloaded applications are blocked and are allowed only by entering password. Clubbed together, these features enhance the application control functionality which leverages maximum control over the usage of applications.

Advanced Web Protection

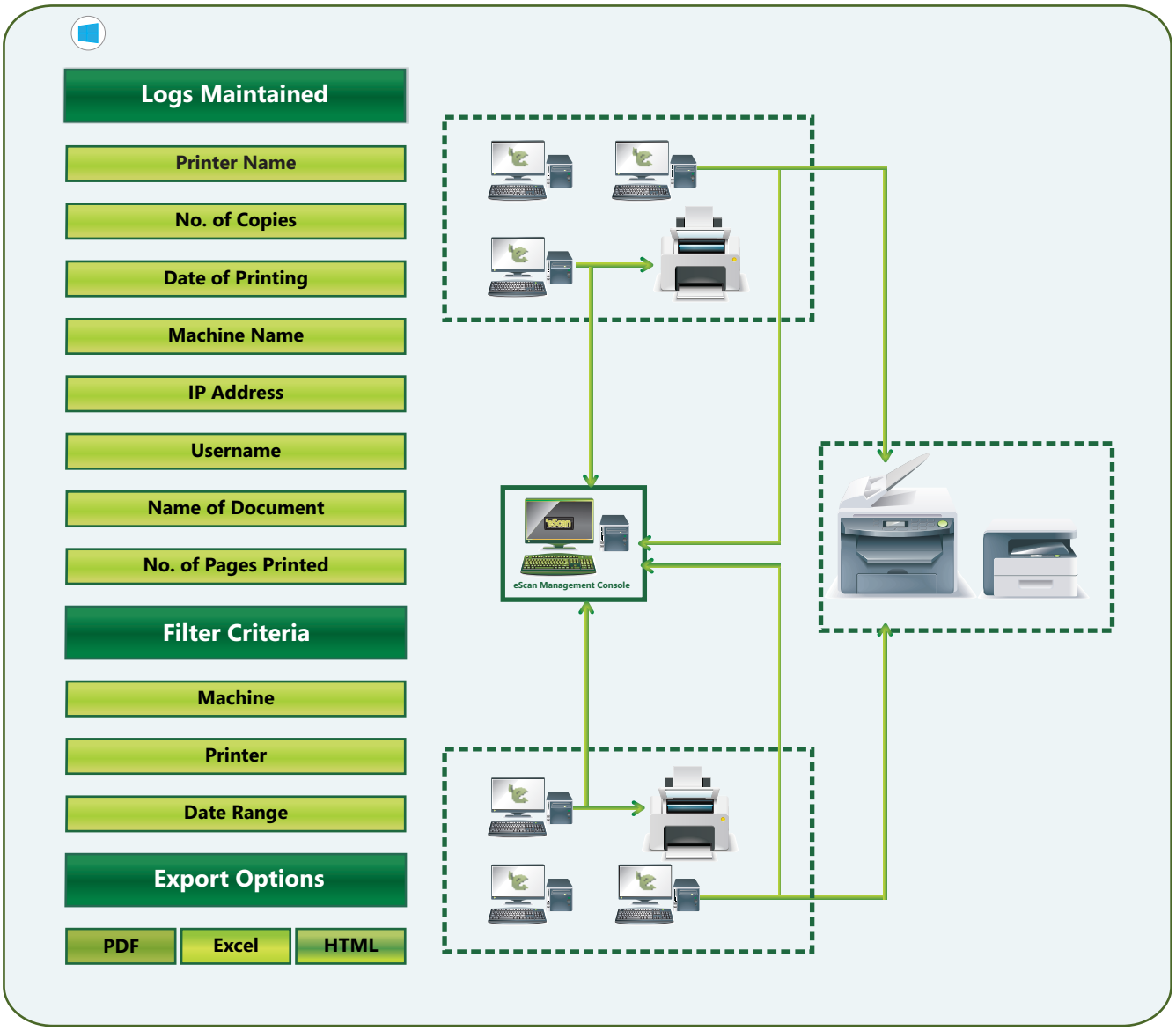
It uses highly advanced algorithms based on the occurrence of specific words or phrases in the web site content and to block Web sites containing pornographic or offensive language. Using this module administrator can configure / customize settings for the employee's access to the internet. He can easily define websites / online content categories to be allowed or to be blocked. It also facilitates to log violations. Administrators can use this feature to prevent employees from accessing non-work-related web sites during work hours.

Asset Management



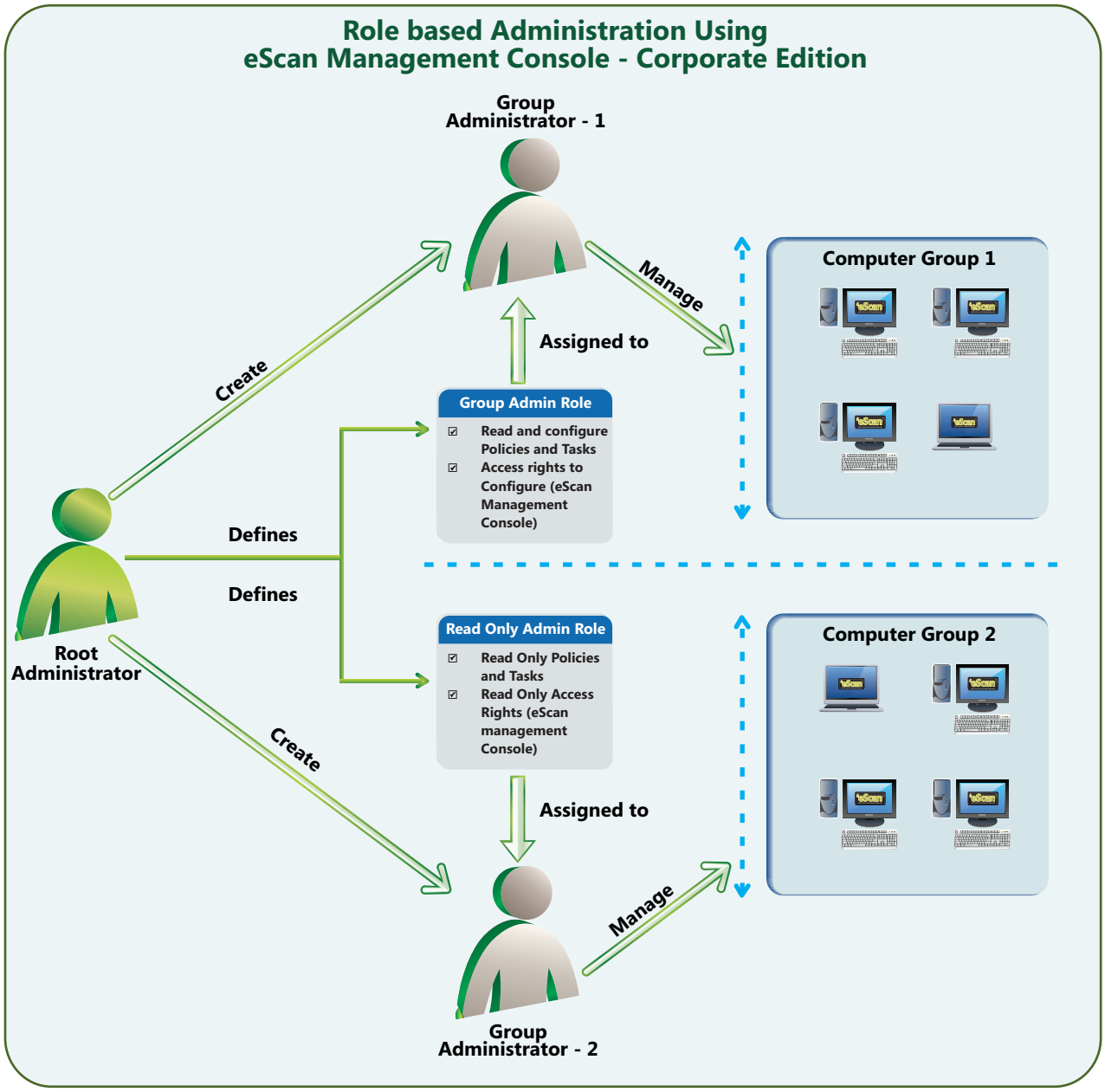
Gone are the days of manually keeping score—walking from desk to desk, taking inventory and affixing asset tags. The modern IT environment is in a near constant state of change. Users continually download and install software from the Web be it a PC, Laptop or a Smartphone. Operating systems, browsers, anti-virus programs and other applications update themselves on a regular basis. By the time an IT department could possibly complete a manual inventory these days, the information would be hopelessly out of date and of little to no value. For these reasons, companies require automated solutions for managing their IT assets. eScan Corporate 360's Asset Management module provides the entire hardware configuration and list of softwares installed on endpoints with Windows, Mac, Linux or Android in a tabular format. Using the module, a track of all the hardware as well as software resources installed on all the managed endpoints connected to the network can be kept. The administrator is notified when any change in hardware configuration or any new software is installed on the managed endpoints. Based on different search criteria, information can easily be filtered as per requirement. It also allows exporting the captured information available through this module in PDF, Excel or HTML formats. Armed with complete, accurate data and features to convert it into actionable knowledge, this will help them plan, maintain, upgrade and retire their IT assets—to help meet operational requirements.

Print Activity Management



In companies there is always a possibility of Information leakage via network printers. There is always a potential risk of printouts being left uncollected at these devices. Using eScan, you can monitor and log printing tasks carried by all managed client computers through any printer connected to the network. You can generate granular reports of who print what and how much? All generated reports can be exported in PDF, Excel or HTML formats. The log report generated keeps the log of number of copies printed through any printer, the document name of the printed file, the date on which print was taken (client machine), machine name, along with the username of the computer and its IP address. It gives you total control and monitoring of the prints taken by any employee through the printers thus reducing chances of data leakage as well as unnecessary cost on stationary.

Role Based Administration



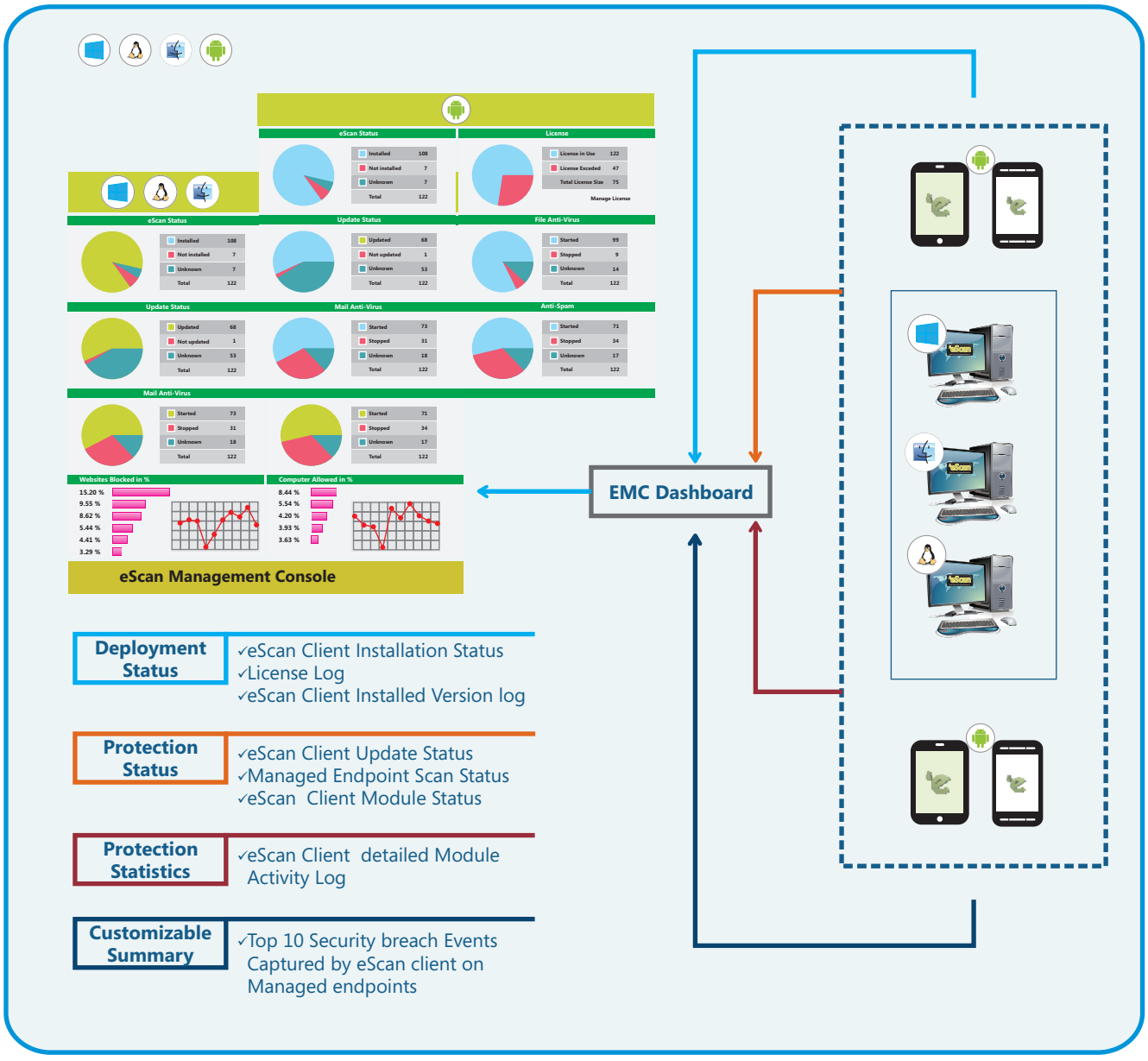
Role based Administration through eScan Management Console enables you to share the configuration and monitoring responsibilities for your organization among several administrators. Using this feature one or more senior administrator can have full configuration privileges for all computers while one or more junior administrators can have less configuring and monitoring authority over group of computers allocated to them. You can assign administrators with pre-defined roles, each with its own set of rights, permissions and groups.

eScan Management Console provide administrators with a streamlined view that is customized to their specific role—showing only what they need to do their job. It is helpful in large organizations where installing and managing eScan client on large number of computers in the organization may consume lot of time and efforts. Using this option you can allocate rights to other administrators to manage selected computer group which will allow them to install eScan and implement Policies and tasks on computers, it also allows them to view eScan reports of the computers in their respective groups. eScan allows you to create Group Administrators with variable rights to manage computers in their group. These rights may include a read only right to access eScan Management Console and Policies and Tasks implemented on managed computers or Read and Configure Policies and tasks as defined by you.

Security Information and Event Management (SIEM)

SIEM technology provides real-time analysis of security alerts generated by hardware and applications. eScan Corporate 360 is equipped with variety of features that facilitate real-time monitoring, correlation of events, notifications and console views and provides long-term storage, analysis and reporting of log data.

Reporting and Analytics



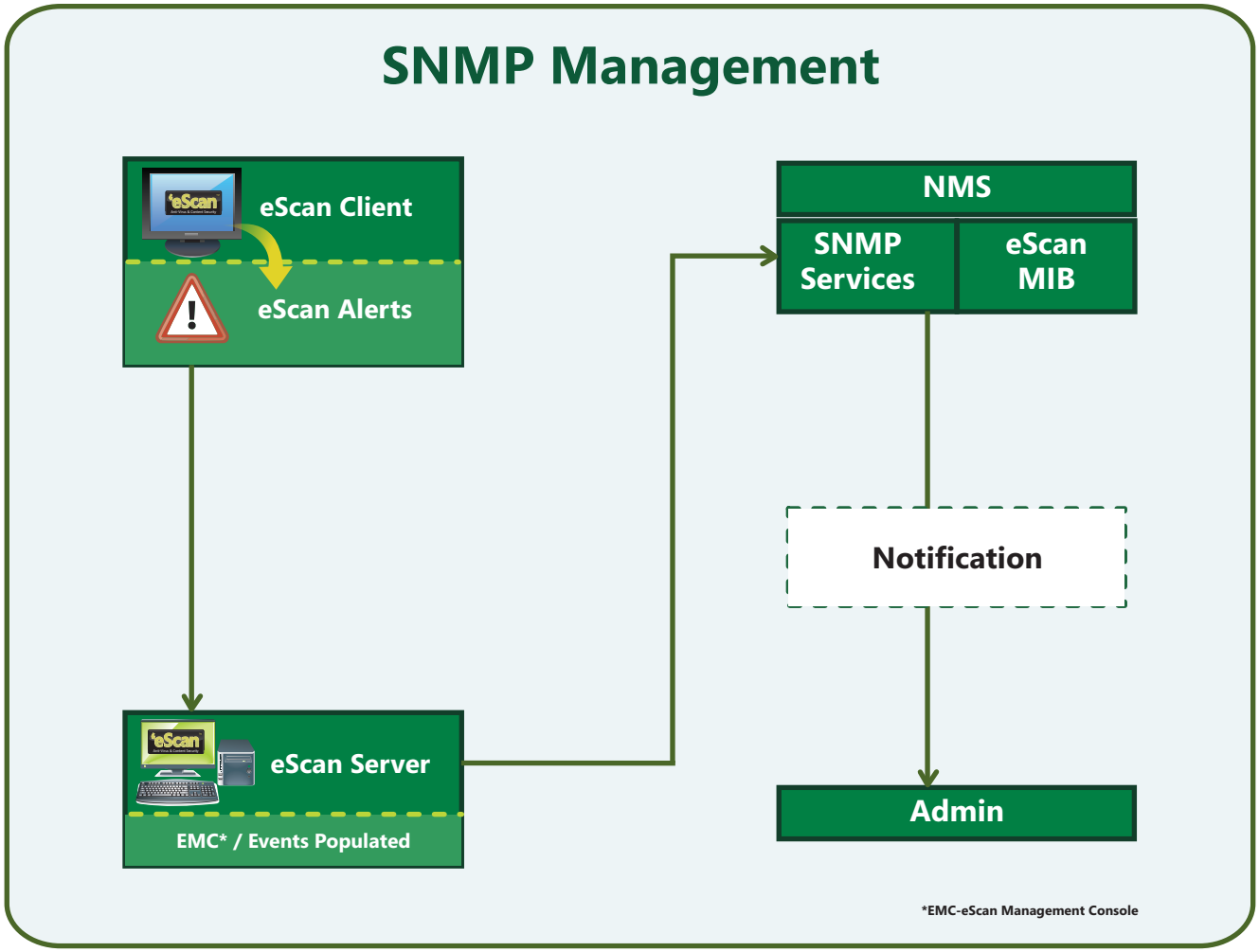
Event Management through Client Live Updater

Events related to eScan & security status of all client computers are captured and recorded/logged and can be monitored in real-time. Also the events can be filtered to retrieve exact required information to closely watch security level on all managed computer on a real – time basis. Thus ensuring total security on all managed computers. It also facilitates Export of the report in Excel that can further be used for audit compliance.

Email Notification

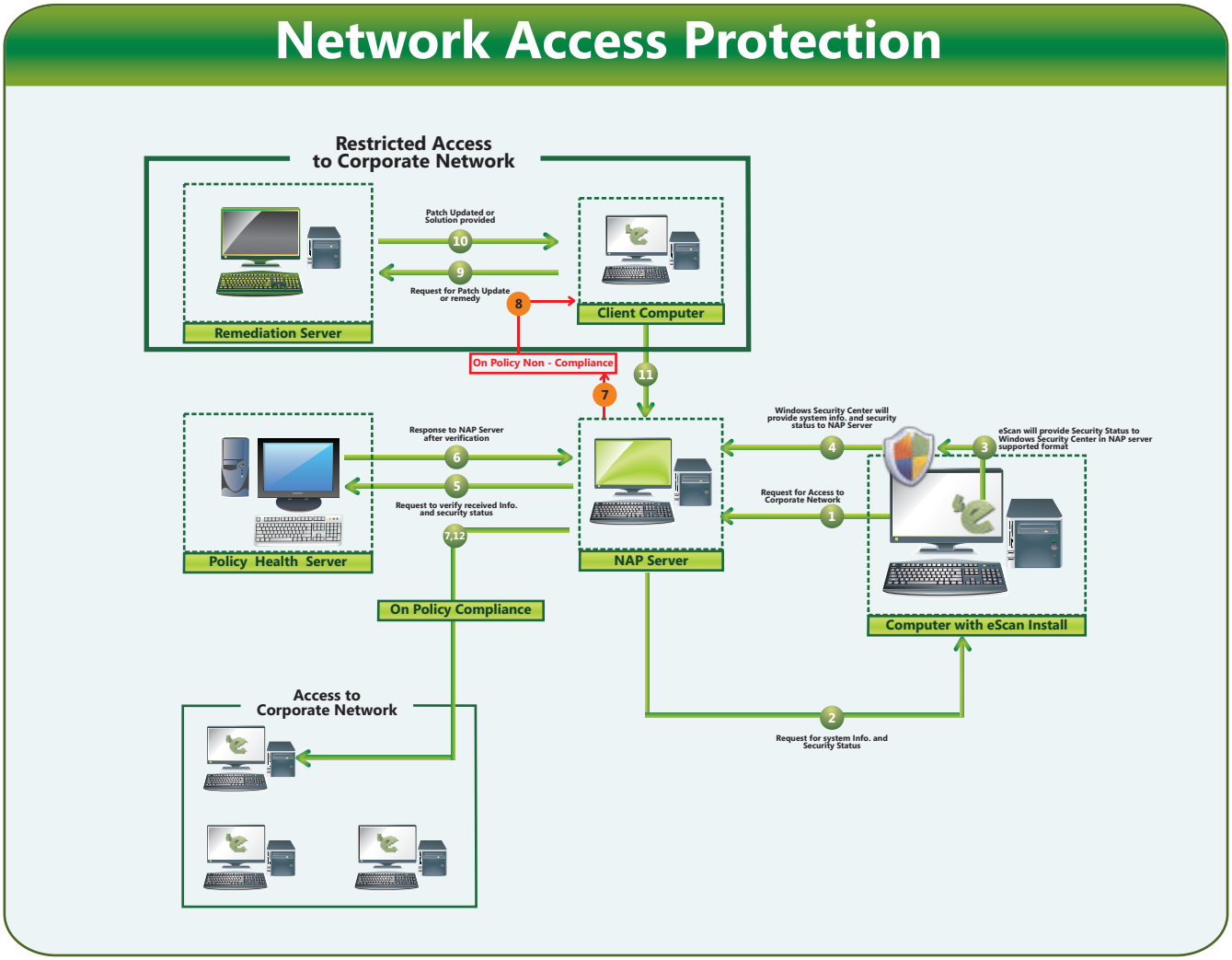
Get notifications on mail on occurrence of any event defined by you, such as installation of any third party software on any managed computer by the user without any prior information to you. These email notifications can also be configured for policy violations by the user or a warning mail to you if virus count on any computer is higher than the predefined limit thus helping you in monitor and control on security of managed computers on a real-time basis.

SNMP Support



SNMP is an internet protocol for managing devices on IP networks. eScan supports SNMP and Syslog Servers by capturing events from client computers and sending it to the SNMP or Syslog Servers providing advanced reporting and alert notification as defined by the Administrator. Based on the reports generated actions can be taken by the administrator to maintain standard security level on all managed computers, ensuring total security without any violation of the policies defined by the administrator.

NAP and Syslog Support



Network Access Protection (NAP) is a Microsoft technology for controlling network access of a computer host based on system health of the host, first introduced in Windows Server 2008. With Network Access Protection, system administrators of an organization's computer network can define policies for system health requirements. Examples of system health requirements are whether the computer has the most recent operating system updates installed, whether the computer has the latest version of the anti-virus software signature, or whether the computer has a host-based firewall installed and enabled. Connecting or communicating computers have their health status evaluated. Computers that comply with system health requirements have full access to the network. Administrators can configure health policies that make it possible to ensure that computers not in compliance with system health requirements have restricted access to the network. (Source – Wikipedia). eScan provides the Security status of the Computer to Windows Security Center in NAP supported format which is then forwarded to the NAP server, based on which restricted or complete access is provided to the computer. Similarly eScan also supports Syslog servers.

Proxy Setting Protection

Prevent unauthorized changing of Proxy Settings on any networked computer and prevent computers from targeted attacks. All access to the internet as well as to other resources connected to the network will be through proxy server configured by the Administrator so the access will be as per the permissions and rights allocated to the user by the administrator. It will restrict the user to change the proxy settings by himself leaving no loophole for misuse of network resources.

OS Vulnerability check

Most products in the market detect absence of critical OS updates and warn the user. eScan is the ONLY product which automatically DOWNLOADS these OS updates (from Microsoft Websites), if necessary, and remove the vulnerabilities.

Protecting Systems from Hacking attempts

Malware URL Filter

Socially engineered malware attacks pose one of the largest risks to individuals and organizations alike by threatening to compromise, damage or expose sensitive information. These are web pages with links to applications that appear to be safe and are designed to fool the user into downloading them, like a software update, screen saver application, video codec upgrade, Fake AV, etc. Additionally, the download link delivers a malicious payload that would lead to execution of malware. In other words, the web is increasingly being used to quickly distribute malware and evade traditional security programs. Considering the above, we have introduced a feature in eScan, which will BLOCK access of users to malicious websites / URLs. Malware URL Filter will further strengthen eScan on End points and will help users and systems-administrators to effectively mitigate loop-holes using which "UNKNOWN" malware enters into computers & networks.

Firewall

Firewall is a comprehensive feature that is designed to prevent unauthorized access to a computer or network that is connected to the Internet. It enforces a boundary between two or more networks by implementing access-control

policies (rules). The user can set rules to control incoming network traffic to their system as well as outgoing traffic from their system. The Firewall checks the rules and analyzes the network packets (small chunks of data) and filter it. If the packets fulfill the criteria to be allowed as defined in the Rules, they are allowed to pass through or else discarded. Within the firewall module of eScan are provided set of predefined rules that can be customized as per one's security needs. Users can define their own 'rules', and when they don't feel the need for any of the rules they have 'added', they can remove them. A rule is an instruction for allowing or blocking network connection or packet on the basis of certain conditions.

Block Portscan

A portscan can be defined as an attack that sends network connection requests to a range of ports on a host, with the goal of finding an active port on the host and exploiting a known vulnerability of the service running on the port. A port scanner is a software application designed to do the port scanning. Using the "Block Portscan" option in Firewall module you can block all Port scan attempts made by Hackers.

Anti-Spam

Anti-Spam module of eScan that scans content of emails received by you. This module filters all your junk and spam emails by using advanced technologies like NILP(Non – Intrusive Learning Pattern and DIRC (Domain and IP Reputation Check) and can send content warnings to recipient or the sender. It also provides you with options to customize the rules for filtering SPAM as per the organization's requirement. It helps you to filter out zero-hour spam.

Mobile Device Management

eScan facilitates effective Mobile Device Management that allows administrator to create different groups for different location, add devices, move devices from one group to another group, define rules/policies for Anti-Virus, setting Call and SMS Filter, Web Protection, Anti-Theft, Password, and Device Oriented policy. It also allows administrator to create New Task, Start an existing Task, create Group Task, define Task Settings, and Schedule Task at a desired period of time.

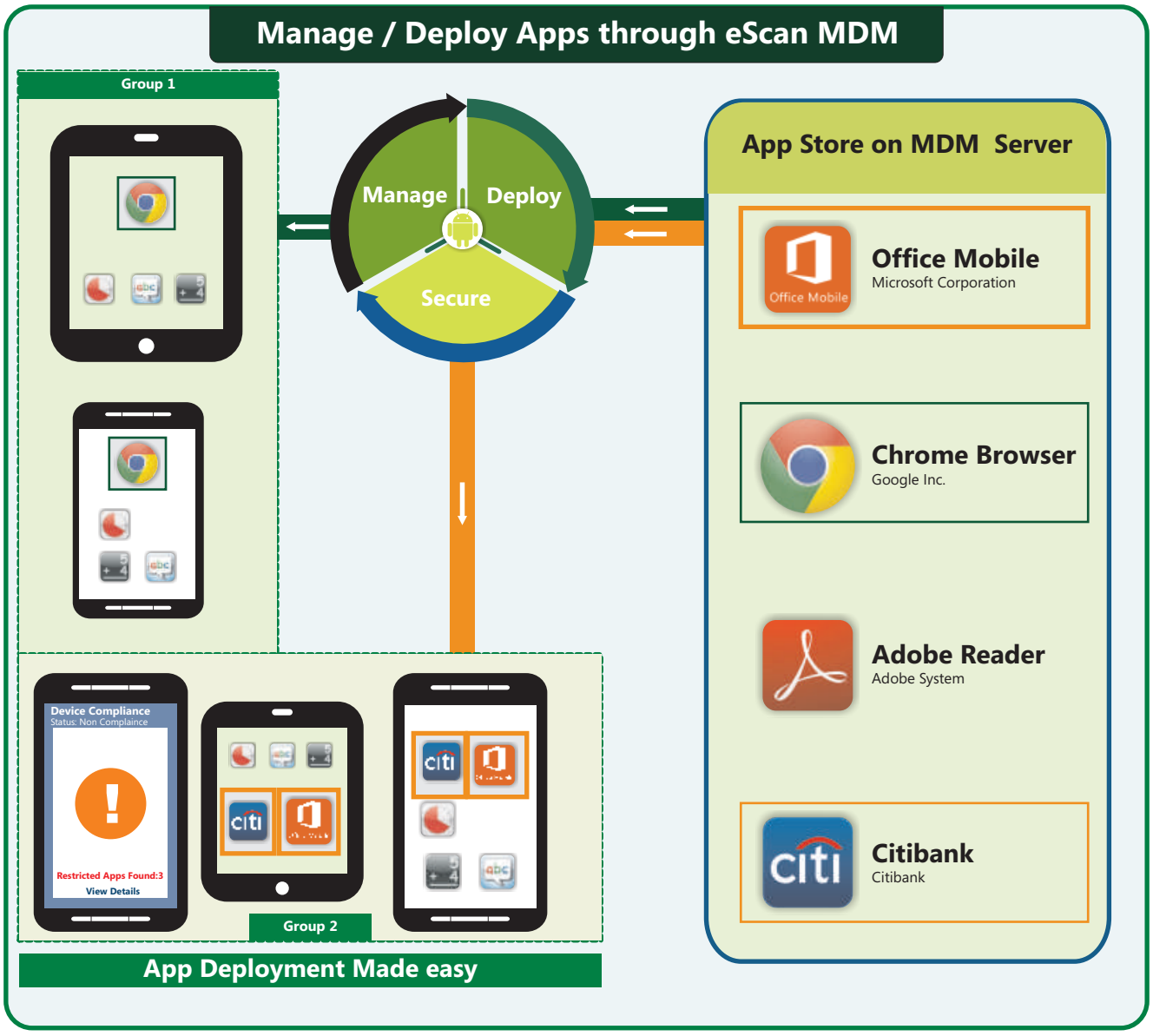
Core Elements of eScan Mobile Device Management

▪ Device Discovery	▪ Capture Live Events
▪ Call and SMS Filter	▪ Advanced App Store
▪ Anti –Theft	▪ Application Control
▪ Mobile Device Asset Management	▪ Advanced Anti Virus Scanner
▪ Deploying Group Tasks and Policies	▪ Device Compliance
▪ Advanced Web Protection	▪ Interactive Dashboard
▪ Privacy Advisor	▪ Multiple Device Enrolment at one go
▪ Centralized Content Library and Distribution Management	▪ Call Log Maintenance and Monitoring
▪ Privacy Advisor	

App Deployment Made Easy

eScan's App Store feature enables you to create a list of apps and deploy them on the enrolled Android mobile devices. Using the App Store you can Add apps to eScan's MDM console. After adding the apps to the App Store you can push these apps to the managed devices through policy deployment.

How it Works ?



Key Takeaways

- Device Discovery and over the air device enrolment.
- Easy configuration and deployment of security policies on enrolled devices.
- Simple backup and restore management of Contacts and SMS from devices to the MDM server and vice versa.
- Advanced Anti- Theft module that facilitates – Wipe Data, Block Device, Raise Alarm, Send Message and Locate Device remotely.
- Comprehensive Asset management giving complete visibility over enrolled devices.
- Advanced Reporting and Real time log management.
- Secured App Store for deploying Apps on enrolled devices.
- Advanced security features for malware detection, Web and Application control, Call and SMS Filter with strong policy deployment in accordance with the security policy compliance of the company.
- eScan maintians Incoming/Outgoing/Rejected call logs of all the enroled Android devices.
- Distrubute Files and Documents to Managed Mobile Device groups centrally using eScan MDM's Content Library.

Other Highlights

- Unified Console for Windows, Mac, Linux and Android
- Set advanced security policies
- License Management
- Export and Import of Settings
- Task deployment
- Manage updates
- File Reputation Services
- Safe Mode Boot Protection
- Sophisticated File Blocking and Folder Protection
- Rescue Mode
- Auto Back-up and Restore of Critical System files
- Malware URL Filter
- Inbuilt eScan Remote Support
- 24x7 FREE Online Technical Support through e-mail, Chat and Forums