G00231773

A Buyer's Guide to Endpoint Protection Platforms

Published: 17 April 2012

Analyst(s): Peter Firstbrook, John Girard

Endpoint protection platforms offer a diverse array of features. This guide lists the most advanced features to help buyers differentiate solutions.

Key Finding

- A wide array of endpoint protection platform solutions are currently available (see "Magic Quadrant for Endpoint Protection Platforms"), with significant differentiation among vendors. No single vendor leads in all functional areas, so buyers need to prioritize their requirements to address the needs of their specific business, technical and regulatory environments.

Recommendations

- Phase out point products for antivirus, anti-spyware, host-based intrusion prevention systems (HIPSs) and personal firewalls.
- Enterprise organizations with more than 5,000 seats should put more emphasis on manageability.
- Demand to know which non-signature-based techniques are included in the base client and the road map. Deploy more advanced capability, including application control, for high-security machines, but anticipate some increased administration requirements.
- Favor solutions that look at the holistic security status of a machine and go well beyond just the status of their agents, and those that provide real-time interaction with a cloud data source to keep solutions in tune with rapidly changing malware trends.
- Seek out vendors that are expanding management capability and protection to new platforms, such as virtual desktops, tablets and mobile devices. Several endpoint protection platform (EPP) vendors have ventured into the mobile device management (MDM) market (see "Magic Quadrant for Mobile Device Management Software").Enterprises that have not already embarked on a mobile data protection program involving encryption for mobile clients should do so immediately for laptops with sensitive data. Common management, established client-side presence and suite pricing make encryption from the enterprise's incumbent EPP vendor attractive.

- Consider the needs of DLP projects when considering endpoint protection. The ability to simplify client-side agents with a common management framework is an advantage, but broader enterprise DLP requirements often outweigh these advantages.
- Resist vendor packaging that includes gateway protection with endpoint protection. Focus on client and server as one domain and gateways as a separate domain. Resource-constrained small and midsize businesses (SMBs) may want to consider the advantages of centralized management of both domains, but must put a higher priority on the unique requirements of each domain.

Table of Contents

Analysis

Basic component technologies in EPP suites include antivirus, anti-spyware, rootkit detection (collectively referred to as "anti-malware"), HIPSs and a personal firewall. Advanced EPP suites will also include data protection technologies, such as data loss prevention (DLP) and encryption. The demanding management needs of large enterprises and the desire to proactively reduce the attack surface are also forcing EPP suites to replicate some PC operations infrastructure, such as security configuration management, patching and comprehensive application management. As the form factor of endpoints expands beyond the traditional Wintel PC to virtual desktops, tablets, Macintosh and mobile devices, the need to provide appropriate security utilities for these diverse platforms is expanding. By combining multiple technologies into a single management framework, EPPs have the promise of increasing security, while lowering complexity, cost and administrative overhead (see "Endpoint Protection in the Age of Tablets and Clouds").

Organizations should initially evaluate their needs across five critical capabilities:

1. Malware effectiveness — How effective is the solution at blocking and cleaning malware?
2. Manageability — How adequate is the management capability for the organization? Smaller organizations may be looking for simple set-and-forget functionality with limited options, while larger organizations may be looking for more complete capability that will be more agile.

3. Solution completeness — Does the candidate solution have the appropriate components to satisfy current and future needs?
4. Support and service — What is the ability of the vendor to provide the appropriate level of support?
5. Strategic vendor status — What is the vendor's ability to service other security needs to reduce vendor management and provide future opportunities for integration and cost savings?

The major functionality components of EPP suites are listed below, with a review of the advanced capabilities of each. Organizations should use these features to build RFPs and/or scorecards to differentiate products under evaluation. No product will have all these features, so buyers must focus on features they deem valuable for their enterprise. This list is not intended to be comprehensive. It is intended to be representative of advanced functions that when investigated will help identify more-sophisticated solutions (see "Endpoint Protection in the Age of Tablets and Cloud").

Manageability and Scalability

Reduced administration overhead is one of the top concerns of endpoint protection platform administrators. An effective task-oriented graphical user interface (GUI) and comprehensive management interface will offer lower total cost of ownership. Gartner recommends creating a list of the top 10 to 20 most common or critical tasks (see Note 1), and using this list as a guideline for comparison testing and demonstration of solutions. Required management capabilities will depend heavily on the enterprise's specific needs and available technical skill sets. Advanced capabilities will include:

- A home page dashboard of real-time events and trending information that enables rapid troubleshooting of event or server issues. Ideally, dashboard elements should be actionable so that clicking on an event or graph will initiate steps to better understanding the issues. More-advanced management interfaces allow for easily clicking through from the dashboard to more detail and problem resolution options.
- The range of client information that can be collected and reported to the management server is a growing differentiator. Most EPP suites will collect information only about the status of the EPP suite. However, as endpoint hygiene becomes more critical, the status of patch levels, configuration information software inventory and vulnerability information is becoming more important (see "Make Optimizing Security Protection in Virtualized Environments a Priority").
- A "wizard"-type installation mechanism that provides optimal default settings for different-sized environments.
- The ability to natively distribute the full client agent and remove competing products is a differentiator; some solutions simply provide an .msi file for distribution by other software distribution tools.

- A task-based (not feature-based) management GUI, which simplifies management by hiding complexity but also gives more technically skilled users the ability to drill down into granular detail for more-technical users (see Note 2).
- Look for solutions that provide native management server redundancy — for example, load-balancing, active/active clustering within and across LANs, or automatic active/standby failover — without a single point of failure.
- Centralized management with automatic configuration and policy synchronization among management servers in large deployments.
- Threshold alerting capabilities — including email, Short Message Service (SMS) and Simple Network Management Protocol (SNMP); and threshold alerts for dashboard statistics and policy thresholds alerts.
- Granular, role-based administration, ideally with both predefined roles and the capability to customize and add and remove options. It should be possible to limit data visibility to only groups that the role is managing.
- The ability to create different management GUI workspace views (for example, administrator or help desk view), with the ability for users to adjust their default views a plus.
- A task/context-based help function, with recommendation settings for Web configuration options.
- Configuration backup and configuration preservation between version upgrades.
- Multiple directory integration options (i.e., application development [AD], Lightweight Directory Access Protocol [LDAP]) and the ability to integrate with multiple directories and traverse directories to find users groups and authentication information.
- Policy (see Note 3) should be all in a single page with intelligent drop-down pick lists and fields that change based on previous optional selections. Avoid solutions that have multiple popup windows or require visiting several tabs to create a single policy.
- Policy creation should be object-oriented so that policy elements can be created once and used in multiple policy instances (see Note 4). For example, the definition of off-LAN can be created once and reused in multiple policies such as firewall/Wi-Fi policy and update server location. Policies should also be able to inherit the attributes of higher-level policy without recreating the higher-level policy, as well as the ability to break this inheritance when necessary. This makes exceptions easer to create and manage.
- Solutions should offer a human-readable printable policy summary for audit and troubleshooting purposes.
- EPP solutions should have a complete audit log of policy changes, especially those with extensive role-based administration and delegated end-user administration.
- A customizable "toolbox" element should allow the consolidation of common tasks into a single user-defined menu.

- Globalization: In addition to global support and centralized management and reporting, look for local language support for the management interface and end-user interface.
- Suite vendors often grow by acquisition. Consequently, the degree of management and reporting integration into a common centralized management console will vary. Consider the look and feel of management pages and the ability to transition from dashboards to the configuration of different elements.
- The management server should be able to collect client status information in real time, rather than in scheduled delta updates. The ability to collect information from mobile endpoints that are not connected to the network that hosts the management server is a significant differentiator.
- The management system should be able to automatically detect new/rogue endpoints that do not have an EPP client installed. This function may be integrated into network access control (NAC). However, it should not be dependent on NAC and should be able to detect clients that have already joined the domain.
- Modern malware is significantly more complex than that of previous generations, often involving multiple components with sophisticated keep-alive routines. Malware removal services and support assistance can be beneficial. However, the wisest course is often to simply reimage machines.
- Some solutions offer a software as a service (SaaS)-based managed console that eliminates the need for a dedicated server for managing endpoints. This feature is more useful for SMBs and regional offices. Ensure that vendors are clear on the level of integration between the SaaS management and on-premises management servers. Also insist on a list of the functional difference between SaaS-based consoles and on-premises-based ones. For example, SaaS consoles cannot typically find rogue machines that do not have the client installed.
- The typical ratio of management servers to clients in practice and the factors that affect this ratio are important considerations for large enterprise and will impact the total cost of ownership (TCO). For smaller organizations, the management server should work on a shared server or a virtualized server.
- Specific features and licensing for virtualized environments such as VMware, Citrix and Hyper-V are rare but of increasing importance for servers and desktops. For example, obtain clarity on what is actually supported and which back-end processes have been changed. Make sure that the vendor's support staff is trained, the labs are configured and their software products are certified with virtualization. Most host-based software provides no protection for the hypervisor layer.
- The ability to stage and phase the rollout of signatures or policies and to roll back changes quickly is important, as fewer users test signatures before deploying them.
- The number of required clients and the client disk and memory footprint are good indicators of the level of integration between EPP components, as well as the efficiency of the client. Ideal solutions will provide a single consolidated agent that has component parts that can be remotely enabled and disabled.

- The client interface should be adaptable to allow for a full range of delegated control for end users. Advanced solutions allow administrators to delegate or restrict any client option.
- Scheduled scans are one of the most annoying aspects of signature-based anti-malware. Options to limit the client impact of scheduled scans are a significant differentiator. Advanced features include the ability to delay scans based on battery life or running process or CPU utilization. More rare is the ability to "wake and scan" PCs in off hours. Scheduled memory scans should be independent of disk scans.
- EPP vendors are gradually adding PC life cycle tools, such as asset discovery, configuration management, vulnerability assessment and software management, as a means to inoculate PCs against unknown threats that target known vulnerabilities. Buyers should evaluate their needs with respect to the integration of these tools and consider the strategic direction of candidate EPP vendors.
- Administration is improved when solutions include support for a broad range of platforms, including Macintosh, Android and Linux, and specialized servers, such as SharePoint, Exchange and virtual servers.

Dashboarding and Reporting Capabilities

Reporting capabilities are a significant differentiator of EPP solutions and can affect the administration overhead of a solution. Buyers should consider both "point in time" reporting and real-time dashboard capabilities:

- The dashboard should provide a real-time graphical, prioritized and table-based view of system events. It should include system information, version information and actionable alerts.
- Dashboards that offer Really Simple Syndication (RSS) feeds with relevant external news, such as global malware activity, vulnerability information or other events, are desirable. External trending information enables administrators to better understand internal activity levels and compare them to global events.
- The dashboard should be administrator-customizable, so that information that is most relevant can move up to the top of the page, and display options (such as pie charts, bar charts and tables) should be configurable so that information can be displayed in the format that specific administrators need.
- Reports and dashboards should include trending information against customizable parameters. For example, create a dashboard view or report that shows percentage compliance against a specific configuration policy over time.
- Dashboards should be configurable for different roles so that each administrator can create a role-specific view.
- Dashboard information should always offer one-click detail to enable administrators to quickly drill down into detail, rather than forcing them to switch to the reporting application and manually select the appropriate report and recreate the parameters that include the condition they are interested in investigating.

- Dashboards should also offer quick links to remediation actions (i.e., clean, quarantine, patch or distribute software), as well as quick links to other resources, such as malware wikis, to resolve alerts.
- Solutions should include the ability to import or export data and alerts with security information management systems or other reporting systems.
- The reporting engine should have the capability to run on-box for smaller solutions or move to a centralized reporting server for consolidation and storage of multiple management servers' log information without changing the look and feel of the reports.
- It should have the ability to create custom reports — in HTML, XML, CVS and PDF output types — save them and schedule them for distribution via email or FTP, or move them to the network directory. The ability to put multiple reports together in a report package and schedule for distribution is a more advanced feature.
- The database must enable rapid report queries and the ability to store historical data for long-term storage in a standard format.
- Live reports should include active filters to narrow results to find specific events in longer reports.
- The reporting engine should include a facility for creation of completely ad hoc reports similar to SQL queries, rather than just modification of the parameters of predeveloped reports.
- More-advanced solution will include analytics cubes that enable very complex queries that answer specific questions — for example; "show number of users in Active Directory group 'finance' that have an unencrypted laptop that have had more than three infections in the last two years."

Malware Detection

As the anchor solution in EPP suites, the quality of the malware scan engine should be a major consideration in any RFP. The ability of most organizations to accurately test malware engines in real-world situations is limited at best. Moreover, none of the signature-based malware engines is even 100% effective at detecting known threats, and accuracy at detecting new threats is only 25% to 50%. Low distribution/targeted threats are even more elusive to signature techniques:

- Test results from organizations such as AV-Comparitives.org, Virus Bulletin, NSS Labs, PassMark Software and AV-Test are useful guides of scanning accuracy (including false positives) and scanning speeds. In the absence of other information, good test scores are better than poor results, but buyers should be aware that not all these tests accurately reflect how users encounter malware in the real world, and do not test all proactive techniques for blocking malware, such as non-signature-based techniques and vulnerability detection and configuration management.
- Signature databases should include all types of malware (such as spyware, adware, viruses, trojans, keystroke loggers, droppers, backdoors and hacking tools) in a single database with a single update mechanism and single scan engine agent.

- Real-time, cloud-based look-up mechanisms should provide extensive two-way communications that share computing objects, such as files and URLs, including metadata about these objects to improve the ability to detect and respond to new events. Cloud-based data should include verdicts on good and bad objects to minimize false positives and to improve performance. Vendors that offer real-time cloud-based interactions are better positioned to spot new trends and respond quicker than vendors that rely on traditional one-way database synchronization schemes.
- The capability to detect rootkits and other low-level malware once they are resident is a significant consideration. Some solutions are limited to catching only known rootkits as they install, while others have the ability to inspect raw PC resources seeking discrepancies that will indicate the presence of rootkits.
- Malware engines should also continuously monitor system resources (e.g., host file, registry, IE settings and dynamic-link library [DLL] changes) for changes that might indicate the presence of suspicious code.
- As more malware is shifting to Web distribution methods, EPP solutions should include client-based URL filtering to block clients from visiting websites that are security risks.

Advanced Host-Based Intrusion Protection

As previously mentioned, antivirus/anti-spyware databases are 90% to 99% effective at detecting well-known, widely circulating threats. However, they are only 20% to 50% effective at detecting new or low-volume threats. Security effectiveness is significantly enhanced by non-signature-based techniques, collectively categorized as host-based intrusion prevention systems or HIPSs, but there is no generally accepted method of testing the HIPS effectiveness of different solutions:

- HIPS techniques have no standard terminology. Consequently, it is essential for buyers to ask vendors to list and describe HIPS techniques so they can normalize the list of techniques and compare the breadth and depth of HIPS techniques across vendors. Buyers should also understand which techniques are included in the base client and those that are optional, and what, if any, additional charges are required for additional HIPS techniques. Vendors are adept at spinning minor HIPS techniques into invincible solutions. Pressure vendors to provide statistical information to illustrate the frequency at which these techniques detect unknown malware.
- A core principle is that the HIPS solution must enable the administrator to choose and tune the styles of protection he or she needs based on the requirements and resources of the endpoint, and configure protection to reflect the organization's overall tolerance for risk and administrative overhead.
- Notwithstanding the previous point, the best solutions will provide preconfigured "out of the box" templates for common application and system configurations, as well as a learning mode for enterprise environments and the ability to test policy in a log-only mode.
- Some vendors only offer binary control over HIPSs, allowing administrators to turn them on or off only. Although we do not expect IT organizations to agonize over each setting, it is important

to have granular control that allows them to turn off certain rules for specific applications to accommodate false positives.

- One very effective HIPS technique is "vulnerability shielding" — that is, the ability to inspect and drop attacks based on knowledge of specific vulnerabilities they are exploiting. This technique allows protection against attacks against known vulnerabilities before the vendor releases a patch, and to buy time for patches to propagate out to all endpoints.
- The simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code (e.g., using static analysis, simulation or reverse compilation techniques) is another deterministic technique, but can be very resource-intensive and should be selectively used for suspicious code.
- Buffer overflow memory protection is common but should address both heap and stack memory.
- Application control capabilities (e.g., application whitelisting, or lockdown) are gaining significant interest as the volume of malware begins to surpass the volume of "good" corporate applications (see "Financial Services Firm Deploys Application Control to Thwart Malware and Other Threats"). There is significant research and development in this area and this capability will be an important differentiator going forward. Application control features to investigate include:
  - How applications are identified and how they are prevented from executing (e.g., whether they block the installation of applications or just the execution).
  - The mechanisms available to create a whitelist will be critical for lowering administration overhead. For example, administrators should be able to automatically authorize applications that are properly signed, or come from trusted locations, trusted processes or trusted installers.
  - Ideally, solutions should provide signatures of known good application as a service similar to current malware databases.
  - Application control should extend to the execution of browser helper objects/controls within the context of Internet Explorer or other browsers (see "Application Control Market Update").

Personal Firewall

Basic personal firewall (PFW) functionality is available in Windows and Mac solutions. The Windows firewall is adequate for most desktop PCs that benefit from network firewalls and network-based intrusion prevention. Mac firewalls are adequate for most laptop usage scenarios. However, mobile devices with higher security requirements or those that need firewalls that adapt to multiple network contexts may want to augment this function with an add-on personal firewall. EPP firewalls are differentiated by the flexibility of their policy (i.e., autosensing location-based policy), breadth of application profile policy (i.e., preventing applications from unusual network behaviors), virtual

private network (VPN) integration, and the range of ports (i.e., USB, Firewire, Infrared, Wi-Fi, Bluetooth) they can protect:

- Given that some organizations will adopt the Windows firewall for fixed network-connected PCs, the ability to manage the Windows firewall in the same management console as the more-advanced personal firewall is a distinct advantage.
- Solutions should offer the ability to create different firewall policies based on connection type (i.e., different network interface cards [NICs] or different networks), as well as dynamically apply policy based on network location — for example, Wi-Fi policy, corporate LAN policy and public Internet policy.
- The integration of a client (IPsec) VPN is useful for enforcing remote-access policies. Ideally, solutions should allow unfettered Internet authentication and then enforce VPN startup to direct remote-access traffic back to the LAN.
- The ability to enforce a one-active-NIC-at-a-time policy to block network bridging is useful. Ideal solutions will have options to disable inactive NICs.
- A useful capability for application control is application profiles that define normal application behavior and can restrict network access for applications that are not approved or are potentially compromised.
- Firewalls must have the ability to block malicious attacks and end users attempting to disable them.
- Log data should be extensive — especially data related to security incidents — to enable forensic investigation. Log data should be searchable and accessible via the report engine.

Port Control

Companies are increasingly concerned about USB and other ports as a channel for accidental or malicious data loss or as an egress point for malware. Granular port control is becoming a common feature of the personal firewall and encryption component of EPP suites.

- Solutions should provide the ability to create policy to control the broadest range of devices (e.g., CD, DVD, USB, Bluetooth, 3G, GRPS) by device class at a minimum.
- The level of granularity to distinguish between classes of devices (i.e., mouse versus a data storage device) potentially down to specific devices by serial number or manufacturer is a differentiator.
- Ideally, policy will be file-type-aware, such that policies can allow or restrict by file type, and action — for example, allow "read only" or allow only certain file types, and restrict application execution such as blocking autoexecute or all execution from a data drive.
- When combined with encryption, port control solutions often allow policy to force encryption for files that are written to external storage for better data protection.
- To minimize help desk interaction, it is useful to enable remote workers to "self-authorize" device usage. That is, allow privileged end users to use devices, but warn them that it is against

policy and to log usage. At a minimum, solutions should allow remote help desks to activate ports for users with an administrator password.

- Advanced solutions will also include options to block cut/copy/paste/printscreen/and print commands to protect data.
- Solutions that have data loss prevention techniques should also be able to create policies based on the content of the files in use — for example, forcing encryption or blocking a file transferred to a USB drive if it contains sensitive of secret information.

Data Encryption and Data Loss Protection (DLP)

As organizations become increasingly concerned about data loss, many EPP vendors are advancing data protection through endpoint data encryption and DLP capability. Many EPP vendors are selling encryption in the related mobile data protection (MDP) market and are successful in selling both stand-alone and suite installations (see "Magic Quadrant for Mobile Data Protection"). Some EPP DLP solutions are components of broader enterprise DLP solutions, while others are stand-alone endpoint-only solutions. Endpoint DLP that is integrated into the EPP suite offers the promise of more content-aware port/firewall and encryption policies, simplified agent management and distribution, and lower cost. Stand-alone EPP DLP will likely satisfy many businesses' early needs but may not be suitable for more-ambitious future data protection plans. (see "Content-Aware Data Loss Prevention Evolves Into Channel and Enterprise Offerings"). Buyers should certainly evaluate prospective EPP DLP capabilities and the vendor's longer-term road maps to determine how well it aligns with business needs. Advanced endpoint DLP solutions will offer:

- The detection of specific corporate data or "registered data," such as specific database data or specific files by name, hashmarks or watermarks, and the ability to detect partial data matches to identify content that has been altered slightly but remains largely intact.
- A broad range of predefined dictionaries and lexicons — for example, lists of racist or sexist terms, obscenities, or terminology specific to healthcare and financial regulation or industry specific regulation, such as the Gramm-Leach-Bliley Act, Sarbanes-Oxley and Payment Card Industry (PCI).
- Dictionaries should be able to assign weightings to specific words, "wild card" operators and case-sensitivity/insensitivity indicators.
- Having "smart" number identifiers (for example, the ability to recognize that "999 999 999" is not a valid U.S. Social Security number) or verifying credit card checksums is a more-advanced capability.
- Solutions should have the ability to perform deep inspection within a large number of file types for content matches.
- While stand-alone endpoint DLP capability ("channel DLP") is good and shows technical prowess, progress and potential, most organizations will want the ability to integrate with broader enterprise DLP solutions and/or share policies with other enforcement points, such as

email and Web gateways (see "Guidelines for Selecting Content-Aware DLP Deployment Options: Enterprise, Channel or Lite").

Mobile data protection (encryption solutions) does not need to be tightly integrated with EPP solutions. However, there are administrative and cost savings when they are. When looking at MDM solutions, consider:

- The ability to take advantage of and manage self-encrypting drives seamlessly alongside software-based encryption.
- Multiple different methods for user access recovery on a sliding scale between ease of access and strength of authentication.
- Easy, integrated support for encryption policies involving data written to external devices.
- Proactive auditing and upward reporting of status of system encryption policies, and worst-case scenario countermeasures to lock and then wipe a device that is taken offline (see "Toolkit: Mobile Data Protection RFP Templates").

Mobile device management today is not well-integrated into EPP suites, although several vendors have made investments in solutions with plans to integrate this functionality. Consider the following when looking at MDM functionality (see "Toolkit: Mobile Device Management RFI and RFP Template"):

- Proactive auditing and upward reporting of status of system encryption policies.
- Policy support that takes advantage of all management capabilities in a given platform.
- Proactive detection and countermeasures for jailbreaking, rooting and data leakage prevention.
- Support for three major mobile platforms (Android, Internetwork Operating System [IOS], Windows), realizing that this is not a monolithic challenge.

Service and Support

Service and support are essential concerns for secure endpoint protection suites, as they are for any business-critical technology. Capabilities to consider include:

- Dedicated product engineers' resources or direct access to Level 2 support.
- Global support presence with local language support engineers in necessary geographies.
- Evidence of extended tenure of support staff.
- Vendor willingness to agree to high service-level agreements (SLAs) for callback responses.
- Support resources, including user forums, best-practice guidance and white papers.
- Installation assistance and training.
- Clear and consistent escalation policies.

Note 1 Critical Tasks

Common tasks might include:

1. Review home page dashboard, paying particular attention to the placement of indicators that illustrate negative changes in the security posture of endpoints. Look for direct links to more information, recommendations and action steps to resolve events.
2. Tour the report center, create a custom report, and schedule it for delivery to an email box or Web server/portal.
3. Show alert configuration capability, and integrate an alert with an external subscriber identity module (SIM).
4. Show real-time data that lists clients on a network that do not have an EPP agent installed.
5. Create or edit the policy elements that can be delegated (or restricted) to end users.
6. Create or edit the policy configuration for client update distribution and step-through policy creation.
7. Create or edit the policy to automatically push the EPP client to an endpoint that does not have it installed.
8. Configure scheduled scans for endpoints. Focus on the ability to limit CPU utilization, and delegate the ability for end users to delay scan execution.
9. Create or edit the port (i.e., USB, CDs, infrared) control configuration. Pay particular attention to the granularity of the restrictions and the linkage to file types and encryption, if any.
10. Create or edit VPN policy (i.e., deny split tunneling) for a specific Active Directory group.
11. Create or edit location-based policy, and pay attention to the level of automation in selecting when a policy should be invoked.
12. Create or edit a Wi-Fi-specific policy.
13. Create or edit a whitelisting and/or lockdown configuration for a certain group of PCs. Add a new executable program to the whitelist. Autogenerate a whitelist from the installed applications on a PC. Authorize a software distribution method and directory as a whitelisted source of applications.
14. Show a single-page summary of client configuration information, and print it for review.
15. Review HIPS policy configuration and step through the false-positive-handling process, including deactivating a specific HIPS rule for a specific application.
16. Edit role-based administration and hierarchical administration to add a new role.

Note 2 Evaluating a Task-Based System

A task-based system can be evaluated by creating a list of common tasks and comparing the number of steps required to complete each task.

Note 3 Choosing an Enterprise's Policy Interface

An enterprise's policy interface — like its policies — should be chosen fundamentally to address the needs of the business. Excessively complex and technical policy interfaces and reporting will force IT to interpret and implement business policy, increasing both workload and the potential for errors and miscommunication. A policy interface should be intuitive and usable by nontechnical business personnel — for example, HR and legal staff. A good way to test the usability of an interface is to give such personnel an opportunity to test it.

Note 4 Reusable Policy Objects

Reusable policy objects are critical to the creation of a scalable policy environment. Objects such as dictionaries should be separate referenced databases, files or subroutines, so that they can be reused in multiple policies but updated centrally. Policies that use hard-coded objects require administrators to update multiple policies to make a simple change.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Atago Green Hills MORI Tower 5F
2-5-1 Atago, Minato-ku
Tokyo 105-6205
JAPAN
+ 81 3 6430 1800

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600