

---

# Building the Intelligent Endpoint Protection Platform

---

Security & Risk Management Summit

Peter Firstbrook

June 20-23, 2011

Gaylord National Resort & Convention Center

Washington, DC

Notes accompany this presentation. Please select Notes Page view.  
These materials can be reproduced only with written approval from Gartner.  
Such approvals must be requested via e-mail: [vendor.relations@gartner.com](mailto:vendor.relations@gartner.com).  
Gartner is a registered trademark of Gartner, Inc. or its affiliates.

This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.



## Key Issues

---

1. How has the threat environment changed?
2. What are effective protection methods at each stage of the attack?
3. What trends will have the biggest impact on future endpoint security?


Gartner

## Threat Environment Maturing

Continuous improvement in

- Quality and quantity of attack kits
- Malware encounters
- Industrial espionage
- Social engineering

Stats page Liberty exploit kit

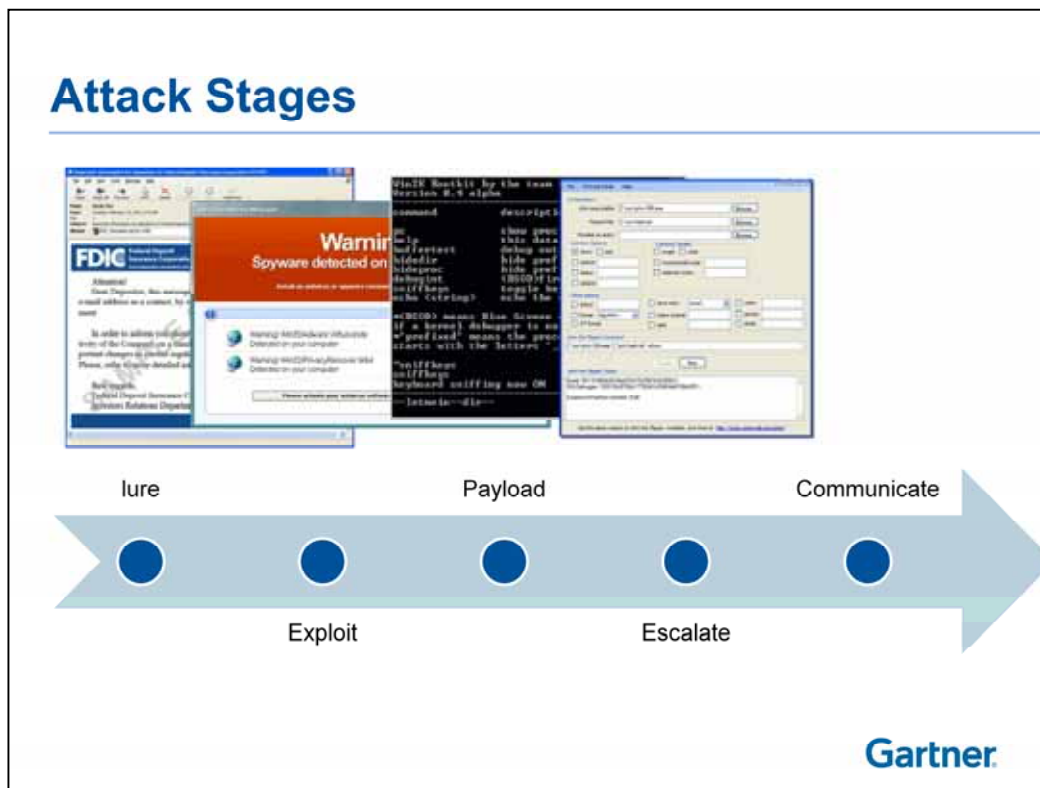


Taken from a live site in early 2010; Credit: Sophos Labs

Gartner estimates that 4% to 8% of corporate PCs are compromised at any given time

**Gartner**

There were no major shifts in attack patterns in 2010 and 1H11. However, as the attacking industry matures, it has shown considerable improvement in a few key areas (polymorphism, anti-emulation, Java exploitation and the quality of content). Two-thirds of all Web-based threat activity is attributable to attack kits, according to Symantec (Symantec Internet Security Threat Report, Volume 16, published April 2011). This indicates that there is a growing population of hackers that are able to leverage the work of more-sophisticated programmers to set up their own franchise hacking business. The success of attack kits was a primary reason for a 93% increase in web attacks and a corresponding increase in malware encounters. According to the [Cisco 4Q10 Global Threat Report](#), enterprise users experienced 135 Web malware encounters per month in 2010. In 1H10 there were 60,000 new unique malware samples per day (source: TrendLabs Global Threat Report) taxing the ability of signature-based malware even further. Industrial espionage attacks continue to occur. Some large-scale attacks such as Hydraq/Aurora in January 2010, Stuxnet in June 2010 and Night Dragon in early 2011 have made the news after months or years of stealth reticence in sophisticated organizations such as Google. However, some targeted organizations have reported detecting six to 10 advanced targeted attacks per day. The bottom line is that enterprise organizations are being penetrated by both consumer malware created with kits and highly targeted advanced threats.



While every attack is different and not all attacks follow a linear attack vector, we find it useful to think of the typical attack stages to evaluate defensive strategies.

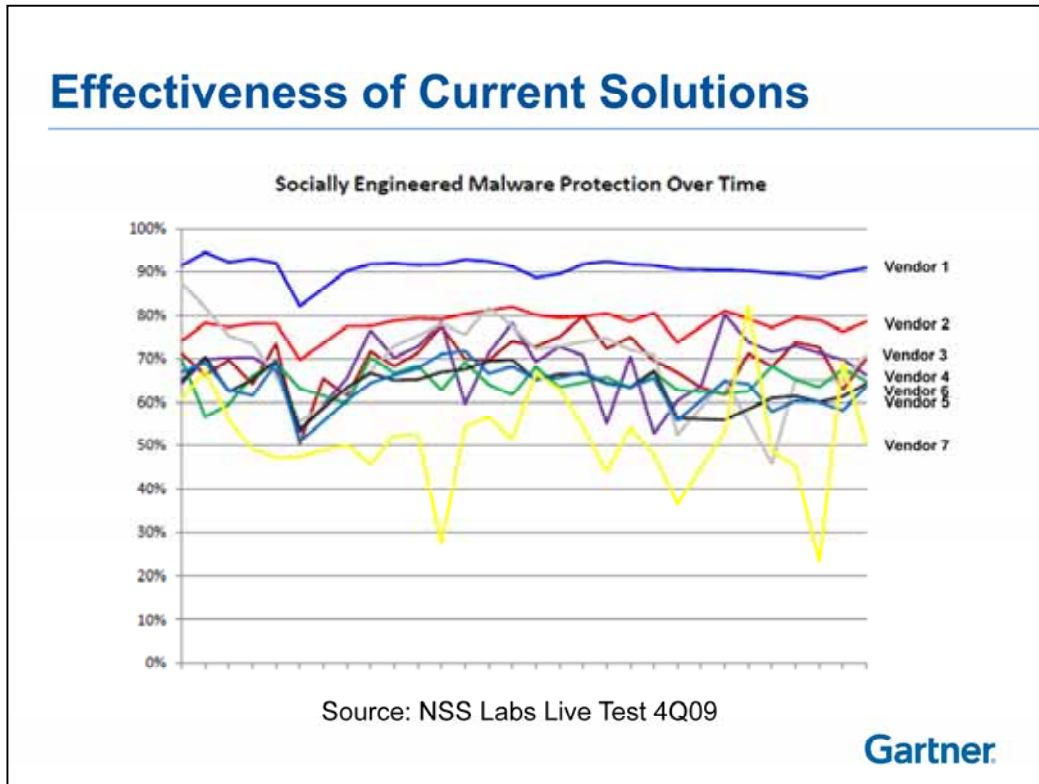
The first stage of an attack is the "lure"; essentially it is a e-mail phish or spam, search engine poisoning, or social engineering attack designed to direct users to attack sites where various attack codes can be used.

The "exploit" stage — Once a user is directed to an attack site, the machine is fingerprinted (using legitimate or other means) to detect what type of machine is connecting. At this point, the attack code will look for the best method to silently compromise a machine, typically by exploit Internet-facing application vulnerabilities, but it could also involve social engineering.

Once the machine is compromised, the attack will launch one or more binary payloads to solidify a permanent presence and to hide.

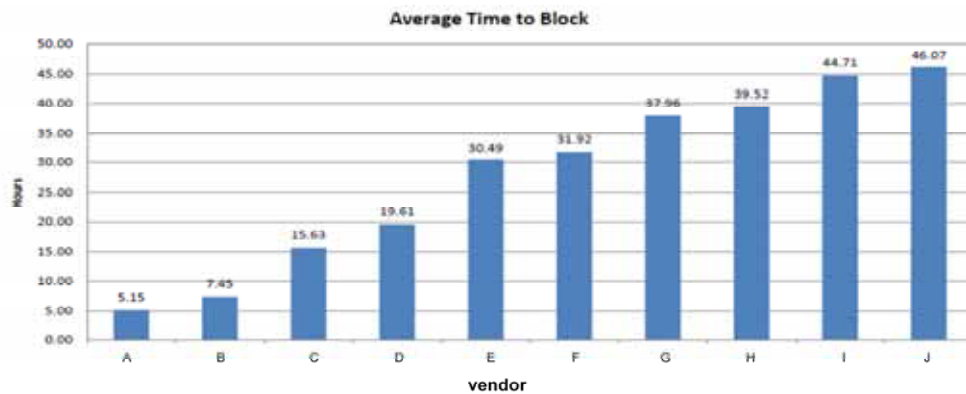
After that, the permanent presence may be used to escalate and expand their presence by elevating their privilege, mapping network resources, attacking other machines, or simply spreading infection internally.

In most cases, for the attacker to get value out of the infection, the attacker has to control their infection and export whatever information they deem valuable. This communication phase lasts throughout the infection life cycle. Because almost all modern malware exploits ubiquitous Internet access, detecting communications streams can represent a good opportunity to detect resident malware.



NSS Labs conducted a test of 10 consumer endpoint protection solutions, taking test PCs to 17,000 suspicious sites every eight hours over 17 days to see if the PC was infected, accumulating a total of 231,351 test results with a reported margin of error of 1.58% ,with a confidence interval of 95%. For details of the test, please contact NSS Labs. Our purpose in exposing this data is to show, yet again, how ineffective malware detection systems have become, even for consumer mass-produced malware. We expect significantly more dismal results in detecting targeted malware that is not mass-produced.

## Effectiveness of Current Solutions



Source: NSS Labs Live Test 4Q09

Gartner

---

NSS Labs conducted a test of 10 consumer endpoint protection solutions, taking test PCs to 17,000 suspicious sites every eight hours over 17 days to see if the PC was infected, accumulating a total of 231,351 test results with a reported margin of error of 1.58% ,with a confidence interval of 95%. For details of the test, please contact NSS Labs. Our purpose in exposing this data is to show, yet again, how ineffective malware detection systems have become, even for consumer mass-produced malware. We expect significantly more dismal results in detecting targeted malware that is not mass-produced.

## Blocking the Lure

- User education
- Filter e-mail for spam and phishing attacks
- Block websites with suspect reputation
- Block polluted channels (i.e., P2P)
- Standardize communications policy

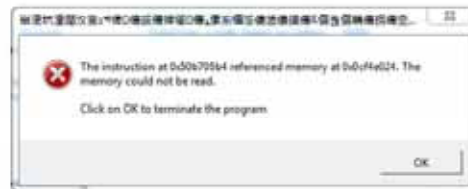


Gartner

Blocking the lure keeps users away from potential attack sites. The increasing glut of personal information on social networking and other sites is making the attackers' job easier by enabling them to personalize their message. User education is necessary to inform users about the potential dangers of attacks. While most solutions strive to minimize the impact on end users, we see more solutions that are attempting to inform users about potentially dangerous activity, including Windows 7. Phishing attacks are some of the most common lures and, consequently, e-mail solutions play an important role in blocking the lure. Most lures attempt to redirect users to a website, so URL filtering for both known bad sites and suspect sites is important (sometimes called URL reputation filtering). Secure Web gateway and endpoint protection platforms are both useful in this regard. We see more vendors, such as Sophos and Trend Micro, implementing URL filtering in the EPP solution. Some consumer grade applications such as P2P are hotbeds of malicious content and so should be blocked with both client-based application control solutions and network controls wherever possible. Since many attacks attempt to mimic internal corporate communications or communications to business partners and customers, it is important to develop a standard communications policy that clearly states how organizations will communicate and what they will ask for or request via e-mail.

### Blocking the Exploit

- Vulnerability shielding
- Vulnerability detection
- Patch management
  
- Real-Time Web page analysis
  - Code analysis
  - Sandboxing or emulation



Gartner

---

The primary attack vector in the "exploit" stage is compromising a known or unknown vulnerability — typically, Web-facing vulnerability. We have been stressing for years that patching is the most significant security mechanism available. Ninety percent of modern exploit code uses vulnerabilities as a primary method of compromise. Before patching is possible, however, organizations must understand what application they have in use (application inventory) and which ones are vulnerable (vulnerability analysis). Not all vulnerabilities can be patched. On the day of vulnerability disclosure, roughly 50% have patches. For the remainder, it can be 30 to 90 days before a patch is available. Vulnerability shields attempt to identify exploits by the characteristic of the code that would be required to take advantage of the vulnerability rather than attempting to classify each specific exploit (aka signature). Vulnerability shields protect unpatched systems until a patch is available; however, they do not protect against unknown vulnerabilities. For unknown vulnerabilities, real-time analysis can identify exploits by analyzing the Web code (static analysis) for common exploit "tells" or by running suspect code in a sandbox environment to monitor its behavior or to protect the endpoint from changes. The graphic from Secunia's yearly report 2010 compares how vulnerabilities reported by Secunia can be exploited. It clearly illustrates how important vulnerabilities are as an attack vector when at least 84% of vulnerabilities can be exploited externally.


---




### Blocking the Payload and Escalation

- Signature detection
- Application control
- Real-time database
- Behavior monitoring

Apple App Store  
65,000 + apps



Bad → Unknown → Good



Gartner

---

While signature-based detection is still the most effective way to detect the payloads for known mass-propagation threats, it is not effective against rapidly morphing threats, targeted threats and new threats. Signature solutions will increasingly incorporate both known threats and known good applications. Due to the rate of change, application knowledge must be delivered in real time from cloud-based data centers or local relays. The known good list allows solutions to spend less time evaluating well-known applications, freeing up resources to look more critically at the unknown applications, perhaps disallowing these applications as a policy until they are evaluated or running these applications in a sandbox environment. Numerous security-conscious organizations are adopting a more-managed application environment, which enforces policy that allows only well-known applications or applications that have been preapproved to run on corporate devices. Apple's "app store" is example of a scalable application management environment. At the same time, effective solutions will monitor application behavior to ensure they do not break out of known boundaries.

**Strategic Planning Assumption: By 2015, more that 50% of organizations will have instituted a "default deny" application management policy that will restrict the applications that users can install.**

### Strategic Planning Assumption

**By 2015, more that 50% of organizations will have instituted a "default deny" application management policy that will restrict the applications that users can install.**

<b>Analysis Supporting the SPA:</b>	<b>Analyzing the Alternate Position:</b>
<ul style="list-style-type: none"><li>• 15%-20% already have policy.</li><li>• Flexible large-scale deployment experience.</li><li>• Symantec's File Insight will have ~22% market share.</li><li>• Windows 7 app locker.</li></ul>	<ul style="list-style-type: none"><li>• Not complete protection.</li><li>• Good applications "universe" is large.</li><li>• Inflexible systems may stall growth.</li><li>• Users may balk at excessive restrictions.</li></ul>

**Gartner**

---

### **Analysis Supporting the SPA:**

15%-20% already have policy that blocks application change.

App management vendors are gaining experience in flexible large scale deployments.

Symantec's File Insight is effectively a default deny system and will have ~22% market share.

Windows 7 app locker windows will accelerate the adoption and decrease the price of whitelisting.

The Apple iPad app store is socializing users to accept a constrained choice of apps in return for reliability.

### **Analyzing the Alternate Position:**

Does not eliminate the need for other security controls in dynamic environments.


The rate of change of good applications is considerable.

Inflexible systems that do not allow for sources of change may stall growth.

Users may balk at excessive restrictions.

### Blocking Communications and Remediation

- Secure Web Gateways
- IPS
- Data Loss Prevention
- Change Monitoring
- Remediation
  - Forensic analysis
  - System restore/reimage

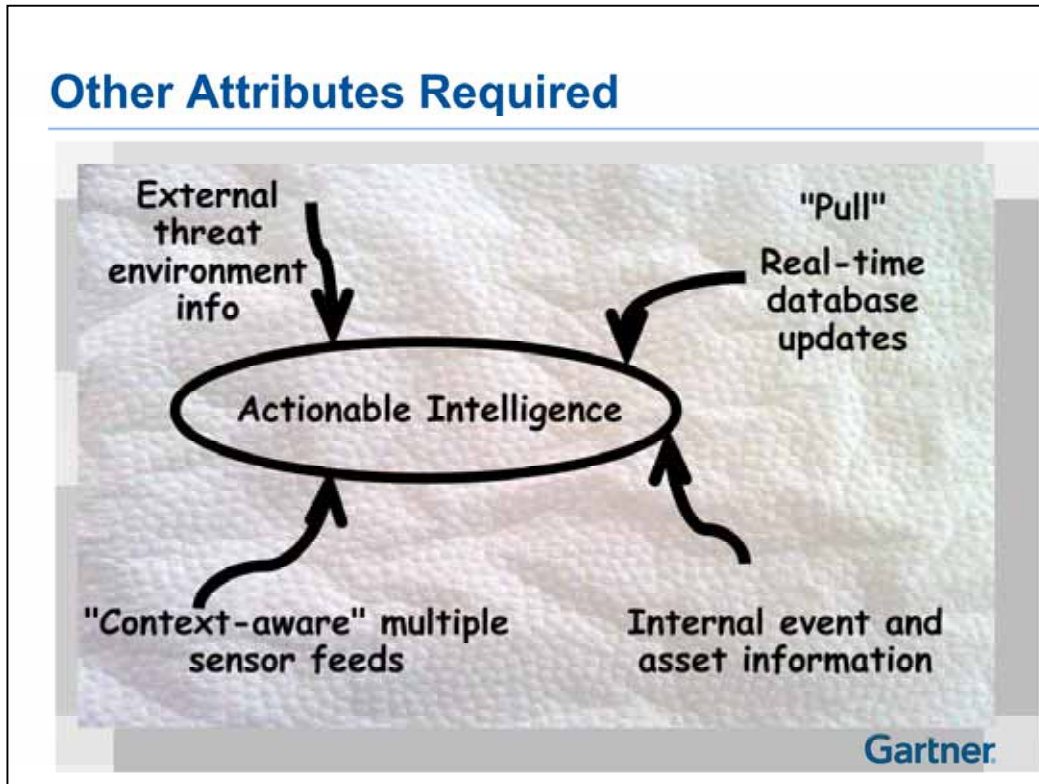


Network and endpoint monitoring must converge

Gartner

All client-based endpoint protection solutions are fallible. Good security requires a layered approach; however, most solutions rely exclusively on client-based protection mechanisms. Growing device proliferation and consumerization will reduce the ability of IT to deploy heavy client-based protection mechanism. Network components, particularly secure Web gateway (SWG), will play an increasing role in protection schemes. Independent gateways can monitor application and rogue traffic looking for indicators of infection such a command-and-control traffic, block this traffic, and notify desktop administrators or end users. Eventually, these gateways can also use data loss prevention techniques to detect potentially malicious exportation of critical data. The utility of SWGs for this purpose will be dependent on their effectiveness at detecting evasive traffic, the quality of the information about the infection, and the location of the solution in path of devices. SaaS SWG solutions are optimal for roaming users and SOHO installations; however, these solutions often have limited ability to inspect evasive traffic. As infections become more evasive and tenacious remediation is increasingly difficult, organizations that experience targeted threats will need to develop a core competency in forensic evaluation and evidence preservation. Ultimately, system restore and reimaging are the only truly effective methods of restoring compromised devices.

See also "A Buyer's Guide to Secure Web Gateways" (G00174650).



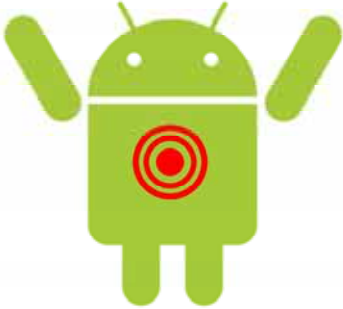
The final piece of the protection puzzle is the accumulation of information that leads to intelligence that can result in action. The key attribute of this type of information is that it is contextualized and correlated to make it relevant to the enterprise. Modern endpoint protection vendors are accumulating a massive amount of data on real-time threats from their network of customer and honeypots across a large spectrum of devices. They are gradually learning how to sort this data and correlate it to provide them with intelligence about the global threatscape. As they get better at this, they will combine this information with local data to provide a more actionable management interface. Think of network operations consoles or security incident management consoles just for the endpoint environment. For example, think of an external event, the disclosure of a vulnerability, combined with local information on which assets are affected by this vulnerability, combined with the threat environment. Several threats are circulating that exploit this vulnerability, combined with suspicious events across several sensors and several pull-based lookups for signature hashes of unknown code. None of this information by itself is sufficient for action; however, all of it together provides a much more complete picture. Next-generation EPP solutions will provide a much richer information management capability.

### Consumerization — Dual Security Priorities

---

#### Protect the Data

- Web application
- Password protection
- Encryption /VPN
- Containment
- Remote wipe



Enterprise e-mail synchronization is the carrot that will enable some level of support and control

**Gartner**

---

The increase in a diverse array of employee-owned devices resulting from the declining price (concurrent trends that are captured by the "consumerization" short form) has two distinct implications for security organizations. (1) How do we protect data on devices that we do not own or manage? (2) How can we protect our infrastructure such as networks and applications from these devices? The bad news is that there are no simple solutions to solve these problems. The good news is that a combination of existing technologies and processes can go quite far to minimize these risks. The best method of protecting corporate data is to use Web-based applications that do not store data locally. However, most business cases require local data, in which case, protecting the data involves turning on incumbent device encryption and password protection solutions and monitoring these settings to comply with a corporate policy. NAC and SSL VPNs can do basic detection of settings on devices such as iPhone, iPad and some Android devices. Several devices also support remote wipe in the event devices are lost. Longer-term, we expect to see data containment solutions that allow for remote wipe of corporate data only. Protecting the infrastructure will exploit the same policy and procedure that is used for guest access to networks. For most users, e-mail is the primary carrot for compliance with policy. Best practice is to offer active synch in return for policy compliance and monitoring, and perhaps a light client presence.

---



### Virtualization — Two Key Issues

---

#### Reducing the impact of security controls

- Offload common functions to a single VM
- Reduce resource contention
- Minimize resource utilization

#### Exploiting virtualization for improved security

- Container for suspect applications
- Create and isolate work/play workspaces

Gartner

---

Virtualization offers both security challenges and potential solutions. For VDI, the issue is reducing the impact of security controls on VDI density. Resource contention and massive duplication of content and functions effects the TCO of VDI. VDI implementations that do not allow persistent change are often run without traditional endpoint protection. While this protects thin clients from persistent threats, it does not provide memory protection. However, strict application and network controls can mitigate risk to an acceptable level. Solutions that cannot use these controls should have more-active endpoint protection. Solutions that can randomize scheduled scans and exploit vShield to centralize functions will have the least impact on VDI density. VMware vShield is a vSphere-level feature that when activated enables real-time, on-access anti-malware scanning to be offloaded to a security VM without requiring agents in each VM being protected. It requires third-party anti-malware vendors to support vShield Endpoint APIs.

Virtualization can potentially play a role in improving consumerization and other security issues by providing a drop-down virtual managed environment that is isolated from the native OS. This allows for containers to run suspect code before being accepted into the core OS. Alternatively, it can be used to create a managed enterprise container for enterprise use on employee-owned consumer devices. This solution is not without challenges such as performance, and compatibility issues.

---

### Integration Cloud and Host Protection

---

#### Cloud assist

- Real-time threat info
- Synchronization of policy
- Cloud-based management
- Lighter clients

#### Cloud protection

- Network-based monitoring and filtering
- Minimal client
- Augments host protection
- Protects SaaS and Web applications

Gartner

---

Cloud-based resources will play an increasing role in real-time protection for endpoints. Traditional solutions have always exploited centralized cloud databases for signature updates. However, in the past this was a pull-based system that occurred at frequent intervals. New pull-based systems can have a lighter database of only the most prevalent threats, but will check with the cloud resource to get updated information on new threats. The quantity of information exchange between client and the cloud will also increase to include good file attributes, a Web reputation data and policy updates. Cloud-based management consoles are already popular with small business; however, their appeal is growing with enterprises that must support global fleets.

Manny future devices will not be good candidates for fat-client solutions, and even those that do could benefit from another layer of network-based protection; basically, clean pipes network capability to filter network traffic and apply policy and logging.

### Key Findings

---

- Full protection will require a cocktail approach for all stages of the attack cycle.
- Effective solutions must:
  - Provide protection for web attacks
  - Analyze both good and bad applications
  - Provide more-precise application management and control
  - Correlate information to provide contextual protection
  - Update in real time
- Unmanaged machines have to focus on protecting the data

**Gartner**



### Recommendations

---

- Acknowledge that existing systems are flawed
- Applications must be patched
- Look for vendors and solutions that offer:
  - Application management (default deny)
  - Vulnerability shielding
  - Web protection
  - Containment mechanisms
- Consider the integration of network and client controls
- Controlling unmanaged devices will require a mix of exiting solutions

Gartner

### Related Gartner Research

---

- **Making Sense of Intel's Acquisition of McAfee**  
Peter Firstbrook, Neil MacDonald (G00206852)
- **Emerging Vendors in Malware Control, 2010**  
Rob McMillan, Peter Firstbrook (G00209586)
- **Magic Quadrant for Endpoint Protection Platforms**  
Peter Firstbrook, John Girard, Neil MacDonald (G00208912)
- **A Buyer's Guide to Endpoint Protection Platforms**  
Peter Firstbrook, John Girard (G00209491)
- **Toolkit: Endpoint Protection Platform RFP Template**  
Peter Firstbrook (G00209494)

For more information, stop by Gartner Solution Central or e-mail us at [solutioncentral@gartner.com](mailto:solutioncentral@gartner.com).

