IDC
Analyze the Future

I D C T E C H N O L O G Y S P O T L I G H T

Delivering Endpoint Integration and Control

January 2013

Adapted from *Western Europe Security Software Forecast, 2012-2016,* by Kevin Bailey, IDC # IS01U, and *SMB Security Competitive Best Practices Key Performance Attributes,* by Charles Kolodgy and Raymond Boggs; IDC # 233439

Sponsored by Kaspersky Lab

This Technology Spotlight explores the benefits that integrated endpoint security platforms with centralised management control offer organisations. This paper also examines the role that Kaspersky Endpoint Security for Business has in meeting IT needs related to ease of use, effectiveness and return-on-investment in the strategically important market for endpoint security.

Introduction

Organisations are struggling to keep pace with a constantly evolving threat landscape, while also keeping a firm grip on an ever-expanding array of devices, software, applications, hardware and user profiles.

As many observers have pointed out, information is the new oil; it has significant business value but, to a certain extent, we take it for granted. Organisations of all sizes have become familiar with storing terabytes and petabytes of data — whether in structured data marts and warehouses or whether unstructured content such as journals, video, Web pages and other documents. Whatever forms the data is in, end users increasingly expect to be able to access information in real time. And just like oil, information that isn't kept under control gets out of hand very quickly. One small leak can cause a lot of damage.

IDC continues to challenge vendors to deliver authentic, integrated, intuitive and centrally managed endpoint platforms. These platforms not only help organisations keep pace with an evolving IT landscape, but they protect commercial availability, intellectual property, client personal identifiable information (PII), brand reputation and customer loyalty.

The Complexity of Attacks

Endpoint security protection began life in the 1980s, when attacks like the Vienna virus were first launched against computers. These early viruses focused mainly on self-reproduction and seldom contained malicious code designed to destroy systems or steal information. As malware and viruses developed more sinister capabilities, however, prominent coders and developers began forming alliances and discussion groups aimed at improving detection and reducing threats. Among the earliest of these was a mailing list called VIRUS L, of which Eugene Kaspersky was a founding member.

Yesterday's virus creator has long since evolved into today's 'hacktivist' or cyber criminal, unleashing highly targeted malware designed to expose vulnerabilities in business networks and the applications running on them. Today's cyber criminals take full advantage of our increased connectivity and the increased availability of information that follows in its wake.

Today's threats are constantly evolving, transitioning towards ever-greater payoffs for criminals and causing greater damage to affected businesses (see table 1). Consider the following examples:

- **Phishing→Spear-phishing:** Specific individuals are targeted rather than canvassing an entire organisation with malware.
- **Trojans→ Ransomware:** Criminals threaten to activate malicious code embedded in Trojans, or use 'scareware' to extort payment from end users or businesses.
- **PC Malware→ Mobile Malware:** The explosive growth in smart devices has fuelled new breeds of malware designed to exploit flaws in mobile operating systems and applications. Increased use of smartphones in the workplace — and their ability to access business networks and sensitive information — has presented criminals with an opportunity to diversify into new revenue streams and new opportunities for disruption.

Table 1

Cyber Attack Dynamics Across All Market Segments

Viruses, Worms, Trojans	Malware	Botnets	Web-Based Attacks	Stolen Devices	Malicious Insiders	Phishing & Social Engineering	Denial of Service (DDoS)
100% of markets have and will continue to experience real-time, zero day and advanced persistent threat (APT) attacks	Android attacks have tripled in the first 6 months of 2012. The impenetrable Mac (Apple) was hit in early in 2012 affecting hundreds of thousands of Mac computers	9 million PCs infected with ZeroAccess botnet, primarily but not restricted to the United States	Drive-by downloads are bypassing firewalls to infect Web users, hiding malware for future attacks	Device IDs, postcodes, phone numbers, addresses, user names, device types are examples of data regularly extracted for criminal activities	Links to organised and/or Internal criminal enterprises, for data extraction, modification, fake credentials. Over 71% of attacks happen during normal working hours.	Increased merging of business and social network exploitation: Li nkedIn, Facebook, Chatter, Yammer, etc. are conduits for driving up these attacks due to the lack of security controls	No one is safe: HSBC Web sites down in October 2012; Wikileaks Web site down August 2012; morphing into TDoS for telco attacks. Plus blackmail and extortion variants to pre-empt a planned attack.

Source: IDC, BGR, Wired, Computer Economics, Carnegie Mellon, InfoSecurity

The diversity of threats experienced illustrates the dwindling effectiveness of point security. Today's threats that combine multiple attack vectors require blended solutions capable of addressing device, Web and email vulnerabilities. Many security managers attempt to tackle the situation by applying several point solutions, which places a greater strain on resources, requiring more maintenance and monitoring. This response encourages a fire-fighting approach to security and increases the time spent on developing and implementing individual policies for each different solution. This time could be better spent optimising the customer experience, working on other more commercially rewarding projects and developing a more proactive security stance.

In addition to traditional attack vectors such as Web and email, cyber criminals now scan organisations for vulnerabilities in operating systems, inadequately patched applications, hardware and software topologies and guest connectivity to business networks.

As cyber threats have increased from one per day to one per second, IDC believes that — without the intelligent merging of security and systems management functionality — organisations will be vulnerable to concealed attacks that may remain dormant or be used by opportunistic or coordinated attackers.

The Diversity of Security Protection Offerings

The scope and intensity of attacks has widened the market opportunity for vendors to provide security offerings that can reactively mitigate external and internal malware exploitation and data removal breaches. Table 2 identifies the breadth of advanced security categories that vendors need to address in order to help an organisation advance its security posture. This scenario is further complicated by the introduction of virtualisation, SaaS, cloud and on-premise delivery models for business-critical operations as well as budget optimisation strategies.

Table 2

Sub-Functional Security Categories

Anti-Malware	Network	Web	Data Loss Prevention	Encryption	Firewall
Device Control	Application Management	Patch Management	Mobile Device Management	Vulnerability Management	Collaboration
Storage	Virtualisation	Security Management	Email	Policy Management	System Provisioning

Although each of the sub-functional security categories shown in table 2 strengthens an organisation's security posture, as individual products they increase the resources and demands placed on security administrators. When implemented individually, the products entail the following:

- Multiple initial deployments
- Multiple update deployments
- Multiple skill sets
- Multiple management systems
- Multiple policy engines
- Multiple scanning
- Multiple profile mapping

Complexity is not only the enemy of security; complexity also inhibits any organisation's ability to implement a more agile, proactive security posture capable of supporting a hyper mobile workforce while continuing to protect assets (devices, data and people) from attack or exposure to financial or reputational damage.

Security administrators are not infallible and must keep increasing their operational skill sets to simplify the management of multiple operating systems with subtle differences, policy constructs that use different prioritisation tables, inadequate time to patch multiple vulnerabilities, and do so while they maintain a manageable architecture topology.

Endpoint: From Solutions and Suites to Platforms

According to IDC, endpoint security has always been the final line of defence against malware and other threats. Now as employees become increasingly mobile, endpoint security solutions are now a primary line of defence.

Organisations must combine effective products, people and processes to resolve the complex security issues they are encountering. When presented with products they must apply more scrutiny to determine if it is an authentic platform, rather than a packaged together or so-called integrated offering banded under the terminology 'solution' or 'suite'.

- A **'solution'** in IT terminology has always been sceptically seen as a way to combine multiple or resource intensive products and consulting services to resolve an organisation's known issue. The concern at the heart of any solution is that third party consultants are engaged to resolve the problem and then leave at the end of the project, only to be bought back when subsequent (often related) issues arise, due to the lack of education imparted on the existing organisational technical/security specialists.
- A **'suite'** traditionally combines a number of products bundled under a single SKU to address a specific category of issues such as security management, endpoint protection, and mobile security, among others. Suites are marketed as a way to ease procurement and provide a complete offering for the particular category in question. The inherent inadequacy of a suite is that it is normally just a combination of products without centralised control; a suite does not have fully integrated chatter or intelligent architecture among the offered products.

Fully integrated, platform-based solutions optimise each functional component while minimising resource intensity. Platform architectures ensure that communication, policy enforcement and product longevity can be delivered.

IDC believes that security vendors should be actively developing an endpoint security platform as a way to differentiate themselves from traditional solution or suite terminologies, encouraging organisations to realise the benefits of:

- Single code architecture reducing emulation, translation or bridging between code sets
- Single policy management defined across all platform functions
- Single management control of endpoint security coverage across all current (and future) devices
- Single unified console to execute, monitor and remediate the desired security posture

Deployment, manageability and a unified architecture are essential factors to consider when implementing complex systems, whether these are integrated or by association. As such, vendors should consider including options such as:

- Automated wizards: These create an out-of-the-box experience for end users, enabling immediate return on investment benefits
- Enhanced customisation and configuration options capable of reacting and adapting to the unique internal needs of users as well as external challenges

IDC believes that the combined value of an endpoint security platform and fast implementation will allow smaller organisations to realise the high levels of security normally associated with enterprise-sized budgets and resources.

Benefits of an Endpoint Platform Architecture

An endpoint platform architecture unifies security with the trend of centralising systems management functions. This approach provides a framework capable of responding to evolving threats as well as internal fluctuations in people, commercialisation and technology. Any platform should provide organisations with common programmatic coding, but also encourage the use of APIs to connect to or from collaborative security and non-security architectures. Specifically focused on advanced persistent threats (APTs) and technology enhancements, endpoint platform architecture should also provide the following benefits:

- **Malware detection.** Cyber criminals are developing increasingly complex malware to attack devices, applications and Web sites. Among other methods, criminals use self-modifying polymorphic/paramorphic code that compiles target information before overwriting boot files to prevent a system from re-booting. A single platform architecture could identify the flow and residency of code across device, business or relevant countries, using common heuristics, behavioral, whitelisting and reputational detection techniques to limit exploitation.
- **Device management.** As BYOD initiatives increase across organisations of all sizes, a single platform architecture will ensure the application of common security standards across business and user-owned devices.
- **Asset tracking.** Organisational data is a valuable asset and an attractive target for criminals. The ability to track data in use, in motion and at rest allows organisations to maintain complete control over their data, including where, when and how it is used.

Social engineering, user naivety, device theft or loss, and information exchange are just some of the risks to company data. Only an integrated platform architecture can support a single control management system capable of delivering the fundamental security processes including policy enforcement, encryption (automated/on demand) and the separation of mobile personal and business data.

Considering Kaspersky Endpoint Security for Business

Kaspersky Endpoint Security for Business allows administrators to see, control and protect IT environments through the use of tools and technologies across a non-disruptive tiered architecture. Kaspersky Endpoint Security for Business relies on a common codebase across on-premise and cloud-enabled delivery models.

Key features Include:

- Progressive protection across endpoints, the web, file servers, mobiles, virtual devices and applications, managing both IT architecture changes and commercial diversity.
- Full-disk and file level encryption (FDE and FLE), organically integrated into Kaspersky's anti-malware technologies using AES 256.
- Security for mobile devices that extends beyond basic mobile device management (MDM) functionality to offer data and application containerisation, over-the-air provisioning and remote device lock out.
- Security for mail and Web gateways, protection of Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim and automatic removal of malicious/hostile programs in HTTP(S), FTP, SMTP and POP3 traffic.
- Vulnerability management, via the integration of systems management functionality to manage common OS levels, infrastructure scanning and patch management.

A key differentiator organically developed within Kaspersky's codebase is the ability to implement integration and control across a single platform:

- Kaspersky Security Center gives security administrators a single pane-of-glass view of their network, users and devices, allowing them to execute and refine Kaspersky features for virtual, physical and mobile devices from one central location. Integrated policy enforcement and status reporting capabilities further support a stable security environment.

- Endpoint Control tools are enhanced by Kaspersky's anti-malware technology, delivering a multi-layered security posture, including:
  - **Application control with dynamic whitelisting:** Allow, block or regulate the applications that run on the network or user devices
  - **Web controls:** Restrict, deny or enforce granular controls (for example, time limits) on Web access from the endpoint
  - **Device control:** Enforce policies based on device type, device serial number, user/function and connection bus (not only USB/CD). Align controls to Active Directory for company-wide policy enforcement.

Challenges for Endpoint Integration and Control Platforms

The implementation of fully integrated, centrally-controlled endpoint security architectures requires the alignment of existing but often disparate policies and procedures. Deploying integration is not the kind of change that simply happens overnight; if it is not based on an intuitive, simple console and transparent endpoint agents it could require security administrators to learn new skills, educate end users and adjust existing architectures. As such, near-term success is subject to the limitations of organisational skill sets and cross-functional business bureaucracy.

Kaspersky's offering needs to prove ease of single policy management for organisations operating in multiple jurisdictions. Data protection legislation and standards can vary greatly across geographies and industry verticals, making ease of policy management a vital success factor for administrators operating in these conditions.

Kaspersky claim to be first to market with this platform architecture, although there are a number of other security vendors using similar terminology across a smaller product offering. Kaspersky argue that their unified platform approach adds value to all size organisations; from very small businesses to large enterprises. In particular small and medium organisations may benefit as Kaspersky helps them embrace complex security technologies that have formerly only been the territory of large enterprise organisations. Enterprise organisations will benefit from the use of familiar security technologies, but with a significantly easier user experience and a harmonised platform.

The Security Information & Event Management (SIEM) category is growing in importance to provide a security framework of all architectures. Kaspersky's lack of offering in this space needs to be supplemented in Kaspersky Endpoint Security for Business by integrating with competitors or SIEM vendors like IB'Q1 or HP's ArcSight.

Conclusion

For the past two-to-three years, organisations have been subject to an increased number of attacks which can be mitigated by an integrated security platform. Vendors have responded by providing workable but often disjointed or difficult to manage offerings via solutions and suites, which provide coverage across the threat landscape but do not answer the need for intelligent integration and centralised controls.

The evolution of platform-based secure content and threat management offerings allow organisations to proactively manage focused, phishing and advanced attacks. Budget's should not be a

constraining factor, but instead increased around an endpoint security platform implementation that meets organisations needs.

The consumerisation of IT, Web 2.0 and the hyper mobile workforce compliments existing business practices; consequently security administrators will need to review their current infrastructure and plan for migration to a platform architecture in order to embrace and adopt these compelling security technologies and maintain a high level security posture.

IDC believes that the need to protect all endpoints and threat vectors (physical, virtual, mobile and cloud-enabled) from a common platform and presented on a single pane-of-glass is essential in mitigating attacks. Kaspersky Endpoint Security for Business provides the integration and centralised-controls and positions Kaspersky Lab for success in the marketplace today.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com