451 Research

MIS Impact Report

Kaspersky sets its sights on single endpoint agent for the enterprise

Analyst: Chris Morales Chris Hazelton 11 Mar, 2013

With the maturation of markets comes the integration of features. The endpoint security space has seen a slew of new technologies introduced and then layered on top of others – all in the name of defense in depth – mostly through the acquisition of smaller startups by larger incumbents. Moving beyond the traditional malware detection that the market has long offered, we have seen the addition of everything from encryption and data-protection tools to the inclusion of system management and compliance/configuration components.

With this growth has come the need for integrated management of these agents on the endpoint along with the need for a single console for event analysis and reporting. As with any integration of disparate technologies developed separately and then acquired, we've seen integration levels accomplished with varying degrees of success.

While it is already an enterprise player, Kaspersky Lab's strength has been in the consumer segment, which has not demanded the same level of depth for its endpoint agents. As it shifts its focus more to the enterprise segment, the company is joining the multifunction agent fray. However, rather than acquire companies, Kaspersky has opted to develop its own technology to complement its current malware platform.

The 451 Take

Considering the company didn't even get started until 1997, Kaspersky knows well how to enter established markets and still make a presence. It has enjoyed tremendous growth, in particular in the consumer market, in its 16 years. Eugene Kaspersky and his team have taken their same methodology of internal development, single agent offering and whitelist protection to build one product to rule them all (endpoints, including smartphones and tablets). The company may well find its niche. While Kaspersky has demonstrated strong application whitelisting capabilities, it will be interesting to see how well it can take on the existing incumbents – including McAfee and Symantec – with the rest of its portfolio.

Context

Eugene Kaspersky founded Kaspersky Lab in 1997 as a new entrant to the endpoint malware space. After considering filing for an IPO, Kaspersky decided to remain a private company, and has seen significant growth over the past 16 years with strong revenue earnings – but it is experiencing the same market challenges as its competitors to continue revenue growth. While its overall revenue growth rate slowed last year from 2011, the security vendor is reporting long-term significant revenue growth as it looks to ramp up its business offerings. The majority of Kaspersky's revenue comes from the consumer side, which saw limited revenue growth last year as the company moved away from retail software sales. In 2012, retail sales fell while online sales rose significantly.

On the B2B side of things, Kaspersky saw overall growth of 7% from a market segment that accounts for almost one-third of its business. Breaking this down even further, SMB sales increased 5%, while enterprise sales ticked up 16%. This highlights the fact that a larger portion of Kaspersky's B2B sales are to the SMB segment, but there is significant upside to penetrating larger organizations, particularly when it comes to mobile.

Technology

Central to Kaspersky's security strategy is the strong investment it has made in whitelisting to complement the rest of its detection technologies. It is now well understood in the industry that blacklisting, the traditional method of identifying known malware primarily based on signatures, can no longer keep up as the growth rate of malicious apps outpaces that of non-malicious apps. From this perspective, it is simpler to build a database of known good apps and provide a method of identifying these apps to allow them to run while denying anything else.

Kaspersky has invested heavily in building an in-house database of known good apps and partners with all of the major software providers, including Microsoft and Adobe, as well as hardware vendors such as HP and Intel in order to keep this list current. The company has enough confidence in its list that it now offers default deny rules in its product as the centerpiece of its application strategy, touting much higher protection rates – with backing from the testing labs – than would be offered by using blacklist detection methods.

As recently seen with Bit9, however, it is possible to sign malware with known good hashes if the database itself is compromised. This is not a compromise of the technology itself but of the methodology used for identifying good apps, and it would require the compromise of the central database within the security vendor. It should be noted that Bit9 is a pure-play whitelisting firm, and Kaspersky maintains that its in-depth defense would have been less susceptible to this type of attack.

Rounding out its security functionality, in addition to whitelisting and blacklisting, Kaspersky has introduced two new technologies. First is automatic exploit prevention, which monitors the execution of malware should it attempt to execute from running programs in memory. Second is a set of technologies Kaspersky is dubbing 'safe money' to be used in banking to provide validation of the banking sites, Web connection and end-user environment. It also provides for cloud-based detection of valid SSL certificates based on reputation to address man-in-the-middle attacks or fake websites.

Beyond its standard malware detection and security aspects, Kaspersky is looking to round out its endpoint offering even further by including system management, mobile device management (MDM) and encryption features. Initial system management tools available today include hardware inventory, network access control, software management, patch management, license management and remote control. Encryption features include file-level and full-disk encryption. Future plans are to introduce content-aware data-loss prevention features.

The company has taken an agentless approach to virtualization, being one of the first players to employ VMware vCloud Networking and Security, the latest in a line of hypervisor-based technologies that VMware has introduced for analyzing data on virtual hosts. Beyond VMware, Kaspersky also supports Citrix Ready and Microsoft Hyper-V to round out the major hypervisor platforms. As with its standard endpoint offering, management is from the same unified console for reporting and command and control.

Kaspersky has offered mobile security for several years, and is expanding its portfolio to include MDM and the management of mobile apps – which could see further capabilities as the company's whitelisting strategy encompasses mobile as well. While the mobile management space is crowded, Kaspersky sets itself apart from other players with its focus on SMBs and its ability to provide a single console to manage and secure mobile, virtual and desktop. As Kaspersky bumps up against other security providers targeting enterprise mobility, it takes pride in the fact that it has developed its mobile tools in-house, instead of via M&A. In this way, its mobile management tools are built from the ground up to run alongside its other security offerings.

The company will also rely on partnerships with device OEMs like Samsung, Nokia and HTC to leverage firmware APIs to closely monitor and secure these devices. Another partner is Qualcomm, which Kaspersky will work with to provide a hardware-based mobile security offering to provide secure data storage within Qualcomm's SecureMSM chipset. This is based on ARM Ltd's TrustZone, and could provide a tamper-resistant data storage product for apps and services that cannot be removed or changed by the users.

Strategy

As comprehensive as its technology list seems, Kaspersky has wrapped everything up into a single offering, including the mobile and virtualization pieces. The latest version of this product is Kaspersky Endpoint Security for Business 10. It is here where the company looks to differentiate with a simpler pricing model, simplified operation business process, single console and single agent. This integrated offering has all of the functionality of competitor product suites, with a single console in a single agent as well as attractive pricing and usability, and it should be appealing, especially for SMBs. Kaspersky will focus on key partners for growth in the enterprise segment along with improved corporate brand awareness. It will also ramp up its online presence for purchases in the consumer space.

In the past couple of years, Kaspersky has transformed its marketing and channel strategies – including the first global campaign level for its endpoint security business starting in 2012. As the company looks to expand into new lines of security and management to revitalize its revenue growth, such as enterprise mobility, it will need to also increase its brand awareness within the B2B space.

Competition

Endpoint protection is perhaps the largest and most competitive security segment. From a competitive standpoint, we see Symantec, McAfee, Trend Micro, Lumension and Sophos as vendors offering products encompassing the functionality that Kaspersky is looking to integrate into a single product. McAfee in particular has grown through acquisitions, folding each target into its ePolicy Orchestrator central management console for a unified management story. While the various agents do share a single pane of glass for management, it is still a multi-agent approach for the host, and not all of the management areas are consistent since each introduces its own set of technologies pieced together.

Symantec has yet to provide an integrated console beyond its traditional endpoint offering and still treats data protection and encryption as separate products. Trend Micro is particularly strong in virtual environments and will perhaps be the largest rival for Kaspersky on VMware. Trend Micro is using the previous hypervisor integration technology, vShield, with impressive success as it partners with VMware on deals. Sophos has introduced new licensing models for its product to be user-based instead of device-based, which will greatly reduce licensing costs and should appeal to SMBs. This means that virtual agents, mobile or traditional endpoints to a single user count as a single license. Competition also comes from AVG Technologies and AVAST Software for malware protection, while Bit9 and Triumfant offer application whitelisting.

SWOT Analysis

Strengths

In-house development allows Kaspersky to provide tight integration for all of its functions – avoiding the challenges of integrating acquired technologies and staff that competitors face.

Weaknesses

The company is late to the game and still lacks some key features for encryption, MDM and system management – but this may allow Kaspersky to focus on what's important without worrying about legacy product lines.

Opportunities

The cost of the endpoint has diminished and virtual environments are growing. A product delivered at the right price could quickly gain traction.

Threats

Competitors are already installed in large enterprises. Most of what Kaspersky will be faced with is conquest sales. Trying to integrate everything at once could lead to not-as-strong features.