

INSIGHT

The New Symantec: Changing the Goal Post to Enable Secure Availability and Dynamic Resilience

Vivian Tero
Wilvin Chee

Puni Rajah
Kazuyuki Ide

IDC OPINION

IDC evaluates the acquisition of Veritas Software by Symantec Corp., first announced on December 16, 2004. IDC's initial reaction to the announcement is discussed in our event flash document *Symantec Acquires Veritas* (IDC #AP53404L, December 2004). The transaction was finalized on July 2, 2005, following the approval of the merger by both companies' shareholders on July 1, 2005. Key highlights of this analysis are:

- ☒ The merger of Symantec and Veritas was predicated on the ability of the combined entity to leverage existing metadata in the security domain with the storage and availability domain, to simplify and automate security management, and enable information integrity.
- ☒ IDC believes the Symantec-Veritas merger positions the combined entity to go beyond information integrity and be a serious contender in enabling dynamic resilience, specifically secure availability, which includes components of security, storage, system management, application deployment, network management, networking, and system software. Secure availability takes on a more proactive approach to business continuity and enables enterprises to exercise greater control over predictable uncertainties, by proactively engineering security, availability, and resilience into the business process.
- ☒ In Asia/Pacific (excluding Japan) or APEJ, there are minimal overlaps in the combined entities' organizational and channel partner structure. The immediate benefits will come from cost savings arising from the consolidation of its facilities and procurement activities. However, tough challenges lie ahead for the "new" Symantec management.
- ☒ The critical execution issues for Symantec management are to avoid confusion and disagreements with channel partners and customers as the combined entity integrates its organizational and IT infrastructures; retain and recruit critical sales, marketing, and technology personnel; ensure the Veritas brand and identity in the storage software market; grow the Symantec brand in change and configuration and performance management software markets; and stay ahead of the competition, specifically Microsoft, in light of the latter's aggressive forays to expand its addressable markets. In the short term, the vendor needs to convince and convert skeptics to buy into its "information integrity" story. In the long-term, Symantec will need to articulate to the market its strategy for enabling "secure availability."

IN THIS INSIGHT

This IDC Insight evaluates the acquisition of Veritas Software by Symantec Corp., which was first announced on December 16, 2004. IDC's initial reaction to the announcement is discussed in the event flash document *Symantec Acquires Veritas* (IDC #AP53404L, December 2004). The transaction was finalized on July 2, 2005, following the approval of the merger by both companies' shareholders on July 1, 2005. IDC believes the acquisition positions Symantec to be a key player in enabling secure availability. However, the success of the merger is dependent on the "new" Symantec's ability to integrate the Veritas products into its core offerings and avoid confusion and disagreements with channel partners and customers as the combined entity integrates its organizational and IT infrastructures. In the short term, the vendor needs to convince and convert skeptics to buy into its "information integrity" story. Studies have shown that integration execution issues, specifically around the channel management, sales, and marketing, stymie the success of mergers. Additionally, it is critical that the combined entity is able ensure the Veritas brand and identity in the storage software market, grow the Symantec brand in change and configuration and performance management software markets, and stay ahead of the competition, specifically Microsoft, in light of the latter's aggressive forays to expand its addressable markets. This report discusses the implications of the merger to the "new" Symantec's APEJ operations and the potential execution challenges the firm must overcome.

SITUATION OVERVIEW

The Veritas acquisition by Symantec was predicated on the technology capabilities of the combined firm's products to enable information integrity. Symantec is a market leader in security software and its products are designed to protect an enterprise and its information assets from external risks. In APEJ, Symantec security software revenues totaled US\$234.7 million in 2004, which translates into 15.9% of the security software revenue total, while the vendor's revenues in change and configuration management and storage software totaled US\$11.5 million during the same period. Readers should note that secure content management (SCM) software accounted for 53.4% of the APEJ security software revenues and Symantec contributed 27% to the APEJ SCM total.

Veritas built its cachet in the storage software market through its ability to support heterogeneous platforms. Veritas positions itself as an enabler of internal risk management by producing a storage solution that would allow enterprises to ensure its information assets are always usable. In 2004, Veritas storage software revenues totaled US\$155.1 million, which is 16% of the APEJ storage software total. The Precise, Jareva, and Ejasent acquisitions enabled Veritas to shore up its change and configuration management, performance management, and high-availability portfolio (which includes clustering and replication).

Veritas and Symantec have dissimilar but complementary product lines, and the combination positions the vendor to tackle the issue of information integrity. The "new" Symantec defines information integrity as the capability to prevent an attack, quickly recover in the event of a disruption, and make IT systems run more efficiently.

IDC believes the "new" Symantec can go beyond enabling information integrity. The combined firm's portfolio positions Symantec to be a key player in the dynamic IT market for business continuity, which the IDC Asia/Pacific Software and Services Research Special Interest Group (SIG) refers to as "dynamic resilience."

In IDC's executive insight, *Hinge Technologies for the Dynamic Enterprise* (IDC #31371, May 2004), we introduced a framework for developing an IT environment capable of supporting fast-changing business needs, which IDC refers to as "dynamic IT." There are two key areas under dynamic IT:

- ☒ IT operations automation and management will enable end users to realize operational efficiencies through resource sharing of the infrastructure assets. Capabilities include service level management and automation; metering, measuring, and chargeback; security; infrastructure virtualization; infrastructure provisioning; and platform management and monitoring.
- ☒ Business strategy automation and execution will enable end users to quickly adapt to business or technology opportunities, with a layered service-oriented IT environment that better supports the incremental changes in individual parts of a business solution, without impacting the rest of the solution. Capabilities include business monitoring and analytics; business process and application automation; information and data services; integration, event, and deployment services; collaboration and communication services; and access and interface services.

For more information on dynamic IT, please refer to the executive insights *Business Priorities for the Dynamic IT Road Map* (IDC #31672, July 2004) and *An Introduction to the IDC Dynamic Market Map: Worldwide Software Market, 2004* (IDC #33542, June 2005).

Business continuity is often perceived as reactive responses to unpredictable events. Dynamic resilience takes on a more proactive approach to business continuity and addresses the need for the continuous operation of an enterprise's critical business processes, in the context of a distributed environment. Enterprises that have zero business tolerance for downtime will look to achieve a state of "secure availability." Under secure availability, enterprises are able to exercise greater control over predictable uncertainties and are able to proactively engineer security, availability, and resilience into the business process.

From a software perspective, secure availability will include functionalities from the following distinct functional markets in the IDC software taxonomy:

- ☒ Change and configuration management
- ☒ Problem management

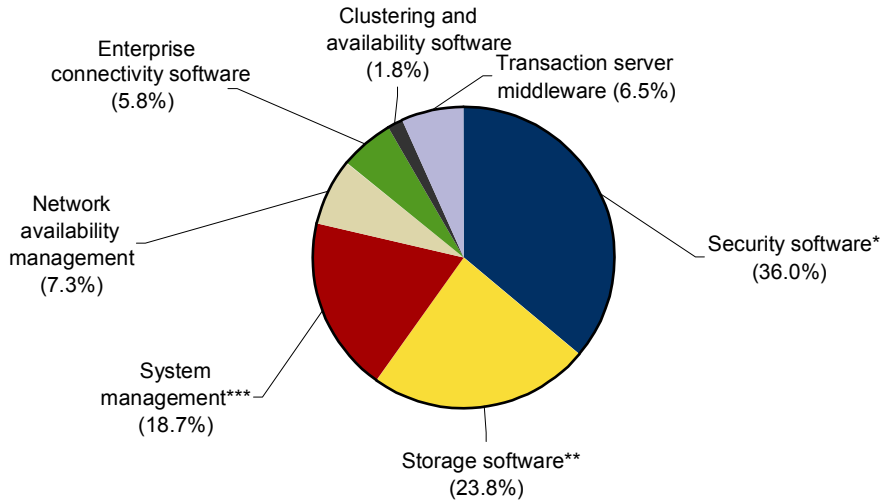
- ☒ Performance management
- ☒ Network availability
- ☒ Clustering and availability
- ☒ Enterprise connectivity
- ☒ Transaction server middleware
- ☒ Backup and archive
- ☒ Storage replication
- ☒ Storage resource management (SRM)
- ☒ File system software (FSS)
- ☒ Other storage software
- ☒ Security and vulnerability management (SVM)
- ☒ SCM
- ☒ Identity and access management (IAM)
- ☒ Threat management (which includes firewall/VPN and intrusion detection system [IDS]/intrusion prevention system [IPS] software)
- ☒ Other security software

In 2004, revenues for secure availability software in APEJ totaled US\$4.1 billion (see Figure 1). The combined entity's portfolio is mainly in storage and security, which totaled US\$2.5 billion. Readers should note Symantec and Veritas have both been shoring up their individual portfolios in change and configuration and in performance management software prior to the merger.

For more information on dynamic resilience and secure availability, readers should refer to the forthcoming document, *Asia/Pacific Taxonomy for Dynamic Resilience* (September, 2005).

FIGURE 1

Asia/Pacific (Excluding Japan) Secure Availability Software Market, 2004



Notes:

- *Security software includes threat management, SCM, SVM, IAM, and other security software
- **Storage software includes backup and archive, SRM, storage replication, FSS, and other storage software
- ***System management software includes performance management, problem management, change and configuration management only

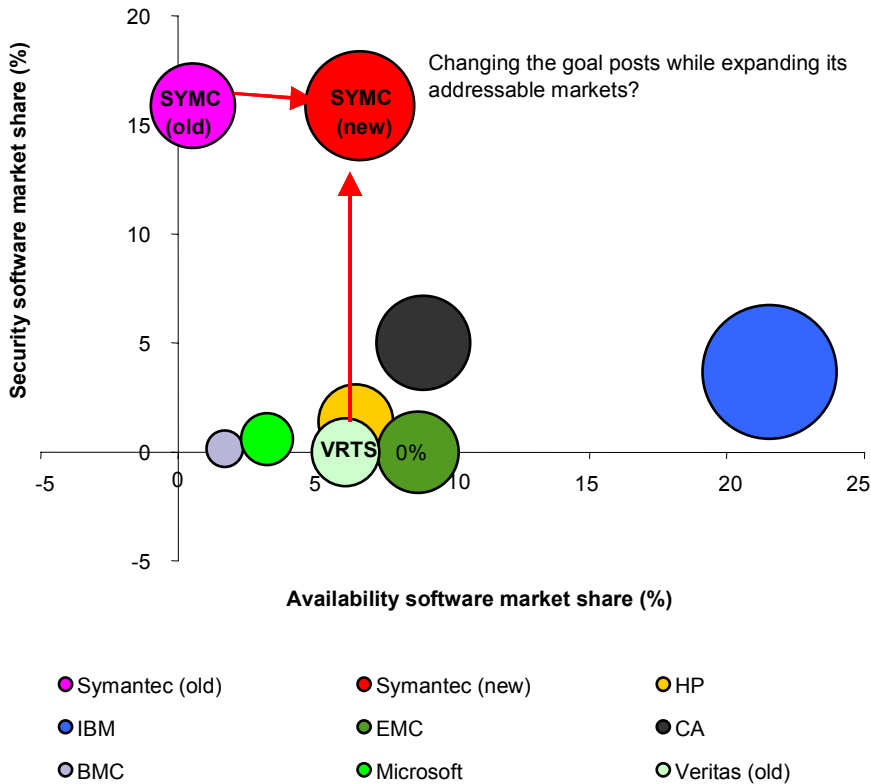
Source: IDC, 1H05

The merger enabled Symantec to enhance its capabilities in information integrity, subsequently changing its goal posts and expanding its addressable markets. Additionally, IDC believes the "new" Symantec has the critical foundations for enabling secure availability and, eventually, dynamic resilience (see Figure 2).

The "new" Symantec segments its capabilities for information integrity along the following solution pillars: Security Infrastructure and Management, Storage Management, Data Management, Application Service Management, and Insight. Insight combines the Symantec DeepSight capabilities with intelligence from storage management and data management, and the provisioning capabilities from application service management to mitigate loss of critical information. IDC views Insight as a competitive differentiator and critical component of secure availability. However, should the "new" Symantec decide to have broader capabilities for secure availability, it will need to add in (through organic growth, acquisitions, or strategic partnerships) the identity and access management, network availability, problem management, and enterprise connectivity components.

FIGURE 2

On the Road to Dynamic Resilience: From Information Integrity to Secure Availability



Note: Availability software includes: storage software, performance management, problem management, change and configuration management, enterprise connectivity, transaction middleware, clustering and availability software, and network availability software

Source: IDC, 1H05

FUTURE OUTLOOK

Symantec puts in place a three-phase plan for product integration:

- ☑ Phase 1 will focus on addressing the interoperability of Symantec and Veritas products, leveraging Symantec DeepSight to trigger alerts in the Veritas backup products. The vendor plans to offer joint solutions for business continuity, email management, and regulatory compliance.

- ☒ Phase 2 will focus on product-to-product integration (including common user interface, licensing, installation, and live update integration) and on enabling an integrated support infrastructure.
- ☒ Phase 3 will focus on developing new information integrity management, and compliance and performance optimization solutions based on a shared technology and architecture.

Phase 1 of the product integration plan was originally scheduled to take place within six months after the completion of the merger, and phases 2 and 3 are scheduled to happen within the next 6 to 12 months and over 12 months thereafter. However, Symantec and Veritas have done a significant amount of comprehensive interoperability testing on key products prior to the merger transaction closing date and appear to be ahead of schedule. IDC expects an acceleration of the "new" Symantec's product integration plans and believes the key challenge will lie in the organizational and IT integration. In the run up to the closing date of the merger, Symantec and Veritas have also spent a considerable amount of time communicating with and addressing their channels and customers key concerns, and held a 10-city road show. The "new" Symantec is aware that not all customers and channels are buying into the information integrity vision and continues to communicate with the market. Highlights are as follows:

- ☒ The new Symantec will focus on supporting heterogeneous platforms and will continue ongoing research and development (R&D) investments in its expanded product lines.
- ☒ In the short term, buying contracts and programs of the individual entities will continue to operate separately.
- ☒ The company has put in place technical and organizational integration strategies and the Symantec's senior executives' performance are gauged on the success of the integration execution.
- ☒ Veritas initiated a review of its software licensing strategy prior to the merger and this remains an ongoing project. The intent is to minimize disruption to the business, reduce the complexity in the software licensing, and make the process easier for partners and customers.
- ☒ Channels will remain critical to the new Symantec's business model and the vendor has a plan in place to eventually enable qualified partners the capabilities to sell and deliver both Symantec and Veritas products. One of Symantec's immediate post-merger goal is to avoid unsettling changes to its existing partner programs. Symantec announced the Symantec and Veritas channel programs will continue to operate independently in the short term, but will be eventually merged toward the end of 2005.
- ☒ Symantec has traditionally been very strong at the two extremes: large enterprises and the consumer market; while Veritas has a large presence in the enterprise markets. In 2004, the small and medium-sized business (SMB) segment contributed 30.4% to Symantec's software revenues and 17.6% to

Veritas' software revenues. The new Symantec plans to expand its traction within the SMB segment by offering SMB-tailored product offerings and expanding its presence in the reseller markets.

☒ Capitalize on system engineers to enhance product integration, create new bundled offerings, and eventually offer solutions the functionalities of which encompass both storage and security.

☒ Leverage cross-selling opportunities, as there are minimal overlaps in the individual companies' existing installed base.

In APEJ, there are minimal overlaps in the combined entities' organizational and channel partner structure. The immediate benefits will come from cost savings arising from the consolidation of its facilities and procurement activities. Symantec has indicated that it is on an expansion mode and it will continue to beef up its domain expertise in compliance and information integrity solutions.

The "new" Symantec will exert immense pressure on security and infrastructure vendors alike. However, tough challenges lie ahead for the management, as we have not seen many successful cases of a merger of (almost) equals. Symantec has articulated its product integration plans, channel management integration plans, and software pricing and licensing initiatives. It is critical for Symantec to avoid missteps in the execution of its integration strategy. IDC believes Symantec will face execution challenges in the following areas:

☒ Internal organization and market execution issues

☐ Maintaining staff morale and customer focus and in retaining critical sales, marketing, and technical executives as the company works out its headcount redundancies. In APEJ, IDC sees very little overlap and expects the impact to be minimal. Symantec has also taken great pains to emphasize that there will be no redundancies in the region and will be in a hiring mode in the coming months.

☐ Experienced IT architects who are well-versed in the conceptualization, design, and implementation of secure architectures are rare in the region. This shortfall of qualified personnel could potentially stymie Symantec's opportunities to grow its business.

☐ Maintaining Veritas strong brand and presence in the storage software market. Symantec needs to articulate if it will choose a multiple brand strategy.

☐ Symantec Insight is a competitive differentiator. At the moment, the vendor views Insight as a product category. There are opportunities to offer Insight as a managed service product. If it does, Symantec will need to clarify its execution plans and the role of its channel partners. Will Symantec be expanding its services organization to include the delivery and fulfillment of Symantec Insight and its associated services? Or will Symantec leverage its existing channel structure, thus creating new revenue opportunities for partners? IDC believes Symantec's strategy for Symantec LiveState Suite, where qualified and trained channel partners will conduct the delivery and fulfillment of Symantec Livestate Delivery 6.0 Enterprise Manager and Symantec LiveState Recovery, gives an indication of the vendor's strategy.

The latter course will go a long way to increasing Symantec's partner preference rate, at the same time, help Symantec minimize any potential channel conflict.

- ❑ Change and configuration management and performance management software are relatively new markets for Symantec, and the vendor does not have the cachet that it does in the security and storage software markets. These functional markets are also dominated by large infrastructure management software vendors (CA, IBM, HP, BMC), the products of which offer relatively more advanced functionalities and much wider portfolios, and are more tightly integrated with the rest of the individual vendors' system and network management products. In APEJ's cost constrained markets, it may be wise to position these products as critical components to a modular approach to secure availability.

☒ Channel management

- ❑ Symantec and Veritas drive more than 90% of their business through partners. It is critical for the new Symantec to execute on integrating its channel strategy, enabling the qualified partners to sell and fulfill both product lines and increase the partner preference rates.
- ❑ Symantec's major competition in its expanded addressable market now includes major infrastructure software vendors like CA, IBM, and HP. HP and IBM both derive a significant portion of their respective revenues from their services practice. All three vendors currently face channel management challenges, especially in the SMB segment, and have posted spiky performance across APEJ in 2004. Symantec will need to plan and execute on an SMB-focused strategy that would not alienate its existing channel partners.
- ❑ Minimizing confusion among customers and channels as the vendor integrates its billing, CRM, and customer support systems. For existing customers that have both Symantec and Veritas contracts, the new Symantec will need to articulate its plans for consolidating these contracts into a single agreement. Symantec's existing strategy for contracts that are up for renewal is to evaluate the merits on a case-by-case basis. This approach could potentially create pricing transparency issues (with both the customer and channels).

☒ Competition

- ❑ The convergence of system management, network management, storage, and security continues driven by end-user demands to reduce complexity, instill more intelligence into the exiting IT infrastructure, and manage the costs of IT operations. At the same time, vendors are looking to expand their addressable markets and seek out new competitive differentiators. Microsoft has recently announced its intention to acquire FrontBridge and expand Exchange into a managed email security. Microsoft Windows' dominance in the x86 server and desktop OSs market underpins the pull-through demand

for Microsoft Windows Operations Manager, Windows System Management Server, and System Center Reporting Manager. Microsoft is building out its portfolio in storage software with its System Center Data Protection Manager and Storage Server, and in security with its Sybari and Giant acquisitions. FrontBridge's DiscoverNet and HEAT products will augment the Microsoft Server System's existing network management, problem management, patch management, and event management capabilities. These developments combined with Microsoft's plans to expand Exchange into managed email security positions Microsoft to be a serious player in secure availability. Symantec products are strongly aligned with the Microsoft Windows platform. IDC believes Veritas' platform agnostic approach is a critical differentiator that Symantec should leverage to its expanded portfolio.

- The planned expansion of MS Exchange into managed email security also raises the bar for Symantec in terms of its strategy for building out a comprehensive email security strategy. Phase 1 of Symantec's product integration plans includes a plan for going to market with joint solution offerings for email management and regulatory compliance. IDC believes the Microsoft Exchange announcement serves as a catalyst to hasten the product integration and underscores the urgency of coming out with new information integrity management solutions. These developments will also spur Symantec to identify and develop new secure and compliant email archiving and storage solutions. Solutions around unstructured content, unified messaging (UM), and instant messaging (IM) are only some of the possibilities in this area.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2005 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: Asia/Pacific Semiannual Security Software Tracker; Asia/Pacific Security and Business Continuity Services; Asia/Pacific Infrastructure Software