OVUM

ComputerWeekly

Ovum research

Extracted from the report 2011 Trends to Watch: Security

For more information about this report please email enquiries@ovum.com

www.ovum.com

SUMMARY

Catalyst

Security needs are growing fast. Businesses are facing a large-scale and well-resourced criminal network intent on defrauding them and their customers. On top of this there is the growing threat of cyber espionage, and the need to meet ever more stringent compliance benchmarks. At the same time, businesses are becoming more inherently vulnerable through greater use of automated collaborative processes, more customer self-service online, and more flexible and mobile workforces. The adoption of cloud services is just one aspect of this new business model. All of this needs a new approach to security that is based on protecting assets rather than defending perimeters.

Ovum view

Among the many changes in the business environment, we have identified compliance, the protection of intellectual property, cost reduction, and defense against online fraud and cyber espionage as the most pressing needs. Although the "big bang" of compliance initiatives that followed from scandals such as Enron are now in place, businesses are facing refinement and extension of the framework, such as with the introduction of the Solvency II regulations in the European insurance sector and the extensions to European data-protection legislation. The need to be more agile and reduce costs is driving interest in the use of cloud services. While many businesses are unsure about committing to the public cloud, they are pressing ahead with deployment of "private clouds" within the organization, and with other technologies such as virtualization that can save money in the data center by sharing resources. Online fraud is an arms race against an adversary with an increasing capability and determination. Fraud-detection technologies are advancing both within the data center and with the end user. Banks, for example, have given away various security products to protect their online customers. Cyber espionage, whether committed by business competitors, states, or criminals, is now being recognized as a major problem.

Key messages

- Compliance requirements place additional burdens on security
- Cloud services bring new security challenges that are only slowly being understood
- Virtualization brings both opportunities and challenges for improving security
- Enterprises, such as banks, are providing security to users outside of their organization
- The holistic view offers hope for improved security
- The range of threats continues to grow
- Demand for security on embedded devices is growing

RECOMMENDATIONS

Recommendations for enterprises

Enterprises should adopt a proactive and agile approach to security based on a business-focused risk-management activity. Risk management provides a vehicle for prioritizing security provision and response. It also enables changing business processes and changes in the external environment to drive modifications in security policy.

Within the security field there needs to be a move away from signature-based defenses to more holistic approaches. Many branches of the IT security industry are advancing with significantly enhanced products and services, including information protection and identity and access management. Several useful aspects of security can now be acquired in the form of managed services, including cloud services, such as infrastructure scanning, penetration testing, secure information transfer, mobile device management, and identity-management services. Most malware products are now delivered through a hybrid service/on-premise architecture.

New technology architectures, notably cloud services and virtualization, provide a range of security opportunities and challenges. While the issues are still emerging, enterprises that are adopting either approach need to be aware of the implications for their risk profile and provide an appropriate response.

Enterprises should examine the opportunities for providing more efficient and cost-effective security by working in collaboration with their customers or business partners. Eliminating threats at source is usually easier than limiting their consequences down the line. In some cases these joint initiatives can be presented as a competitive advantage by showing concern for the well-being of the wider community.

Recommendations for vendors

Vendors must work to address the changing priorities of businesses, including protecting them from the growing range of threats and addressing the needs of new architectures and services. Organizations are looking to vendors to provide advice and leadership, as well as products and services, and they expect vendors to remain relevant.

Organizations are becoming more open to buying security in the form of a service, and vendors should whenever possible provide their technology in three form factors:

- As a managed service/cloud service
- As a traditional software product or appliance
- As a virtual machine for use on virtualized servers or endpoints.

There are significant new opportunities in securing mobile devices of all types, along with the range of emerging data and content services that are being delivered across IP networks to devices other than computers.

Ovum (Europe)
119 Farringdon Road
London, EC1R 3DA
United Kingdom
t: +44 (0)20 7551 9000
f: +44 (0)20 7551 9090/1
e: info@ovum.com

Ovum Australia
Level 5, 459 Little Collins Street
Melbourne 3000
Australia
t: +61 (0)3 9601 6700
f: +61 (0)3 9670 8300
e: info@ovum.com

Ovum New York
245 Fifth Avenue, 4th Floor
New York, NY 10016
United States
t: +1 212 652 5302
f: +1 212 202 4684
e: info@ovum.com