



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

Why Free Endpoint Encryption Is Not Good Enough

November 2012

Adapted from *Worldwide Data Loss Prevention 2011–2015 Forecast and 2010 Vendor Shares: DLP Gets More Embedded into Enterprise Infrastructure* by Phil Hochmuth, IDC #231367, and *Worldwide Endpoint Security 2012–2016 Forecast and 2011 Vendor Shares* by Charles Kolodgy, IDC #235930

Sponsored by Symantec

The traditional enterprise perimeter is becoming more open and extended as the number of mobile and remote employees increases and enterprises connect to more trusted external partners and contractors. The use of consumer mobile devices — such as smartphones and tablets — is changing the nature of enterprise connectivity as well.

As enterprise perimeters crumble or become more diffused, enterprises are pushing security closer to the endpoint — or where the data actually resides. As a result, encryption is a growing trend, particularly among larger organizations that have dispersed workforces. This paper examines the drivers for endpoint encryption, where the technology is gaining momentum, and the challenges of managing enterprisewide endpoint encryption at scale. It also looks at the role of Symantec in this strategically important market.

Introduction

The complexity and management challenges for endpoint security grow as firms' employee bases become larger and more dispersed. The nature of larger organizations introduces more complexities and variables, which can lead to security gaps and, ultimately, to the exposure of confidential data.

In reaction to this, larger firms are choosing the strategy of moving security controls closer to the endpoint (where the data lives) as a way to gain tighter control and more efficient security management. This practice is in contrast to smaller firms, which rely on perimeter defenses to protect smaller, physically concentrated pools of workers and machines. As a result, encryption — in particular, full disk encryption — is an attractive solution to enterprises because it provides a reliable and measurable level of data protection while addressing requirements for security compliance audits.

Some organizations view the use of encryption tools built into modern PC operating systems (OSs) as a viable strategy for achieving fast, cheap endpoint-centric data protection. The thinking for some enterprises is that full disk encryption software is already on the PCs they have purchased — it just needs to be turned on and put into use. However, at the enterprise level, leaving the task of encryption up to free tools built into operating system components is incongruous with the effort to control end-user security more closely and efficiently. In this area, third-party products continue to incorporate advanced features that are worth the investment.

Definitions

According to IDC, the endpoint encryption market is composed of products that perform data-at-rest encryption for endpoint storage. This category includes various types of encryption, such as full disk encryption, file/folder encryption, and removable storage media (such as USB flash drives) encryption.

There are many standalone products in the endpoint encryption category; in addition, endpoint encryption is being included within other products, specifically endpoint security suites, data loss prevention (DLP), proactive endpoint risk management, and mobile devices.



Market Trends

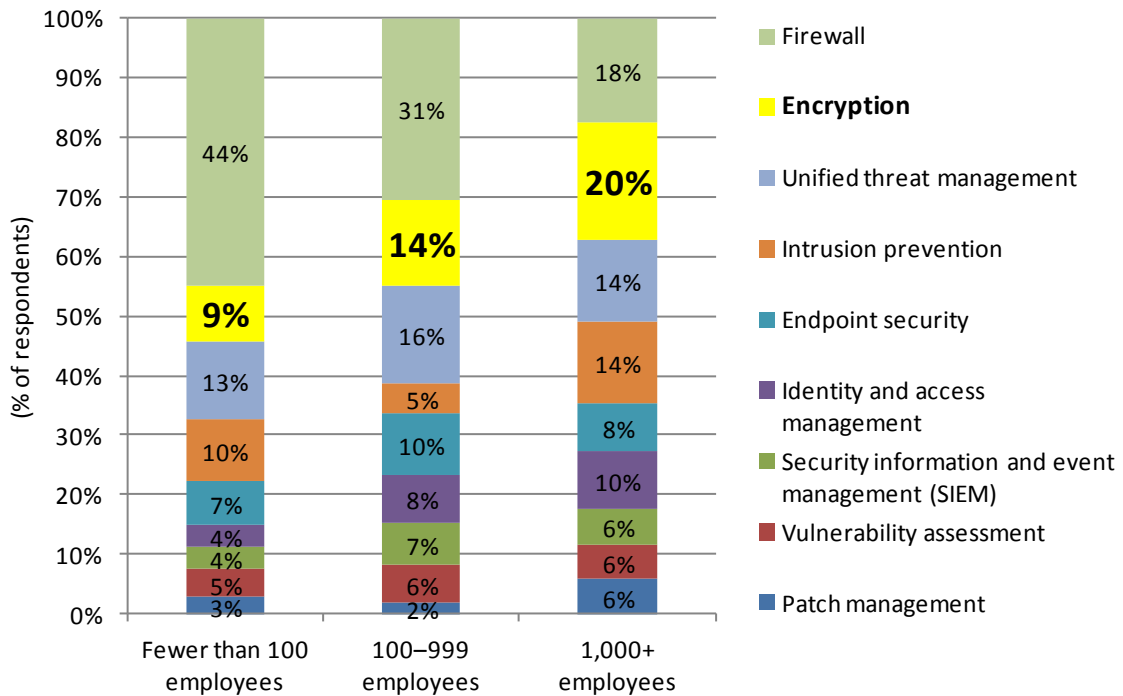
Traditional network-based security — firewalls to protect office workers, VPN for remote/mobile employees — is not enough in enterprises with large numbers of employees who are mobile or work remotely. Security must move closer to the endpoint and, more importantly, to the data because static security constructs don't work. Security that keeps corporate assets "behind" a firewall or requires users to log in to be protected and secured becomes difficult for enterprises to maintain.

As organizations move security controls closer to the endpoint in order to better protect data, security vendors are providing deeper integration of technologies such as full disk encryption, file/folder encryption, and DLP into IT infrastructure. IDC is seeing significant interest in encryption and DLP products in association with storage management systems, which indicates enterprises are connecting the dots between management and data security.

Interest in encryption technologies in general rises sharply as the size of the company increases. According to IDC's 2011 Security Survey, among companies with fewer than 100 employees, encryption ranked as the fourth most valuable technology for protecting against security risks; only 9% of small companies cited encryption, ranking it behind firewall, unified threat management (UTM), and intrusion prevention systems (IPS). Among companies in the 100–999 employee range, 14% cited encryption as a top technology (ranking third behind firewall and UTM). Among enterprises (1,000+ employees), 20% cited encryption as the top tool, more than any other security product category. This data illustrates the trend that as small organizations get larger, secure perimeter technologies such as firewall and UTM become less important as end users become more mobile, more dispersed, and harder to contain (see Figure 1).

FIGURE 1

Security Technologies Most Critical to Threat Prevention by Company Size



Source: IDC

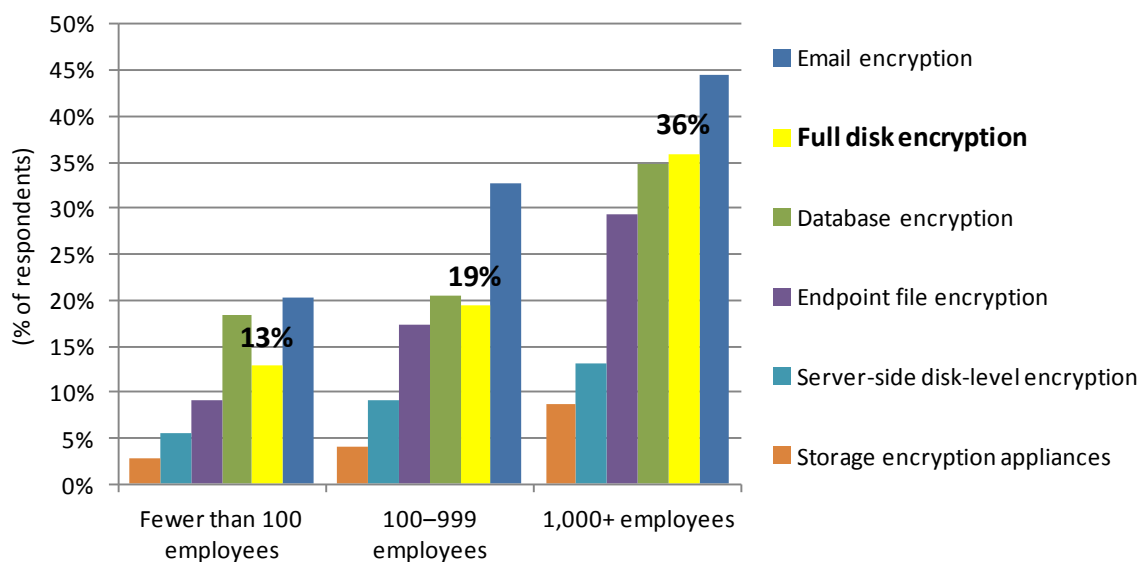
According to IDC's 2011 Security Survey, use of full disk encryption also increases depending on the size of the organization. While email encryption is the dominant form of encryption deployed among companies of all sizes, use of full disk encryption is prevalent in larger firms. Among the types of encryption being used by organizations, only 13% of organizations with fewer than 100 employees said focused encryption was being used or considered. This percentage jumps to 19% for midsize companies (100–999 employees). For enterprises, 40% said they were using or planning to deploy folder encryption. File encryption also is more prevalent in bigger firms; nearly twice the percentage of enterprises said they were using or planning to use this technology compared with midsize and small firms.

Large companies are more interested in encryption than smaller companies, which reflects the nature of threats (both perceived and experienced) in enterprise organizations. In IDC's 2011 Security Survey, 40% of small companies cited "inadvertent exposure of confidential data" as a top security concern, ranking it behind trojans and spyware as top threats. Among enterprises, 60% cited this as a top concern, ranking it number two, still behind trojans and spyware. Again, this follows the logic that bigger and more dispersed companies face increased risks, such as data being lost on a laptop or mobile device left in a taxi cab or at an airport security checkpoint.

To deal with changes in the perimeter, enterprises are pushing security closer to the endpoint, but they are not ratcheting up security capabilities on the endpoints themselves. Instead of building up walls of protection around endpoints and valuable data to ensure data security, organizations are using encryption as the key tool. Full disk encryption is taking hold in a significant minority of enterprises (see Figure 2). However, when it comes to encryption, keeping data safe on a few hundred PCs can be difficult; many commonly available tools, such as commodity encrypted USB media or tools built directly into PC operating systems, can help lock down this type of environment. In many cases, securing such endpoints might be as easy as turning on full disk encryption features built into a laptop's operating system. However, as businesses grow in size and become more organizationally complex, the ability to manage and control what individuals do on endpoint machines decreases, while potential costs and risks rise with regard to data security and protection on endpoints.

FIGURE 2

Types of Encryption Deployed and Planned by Company Size



Source: IDC

Benefits of Centralized Endpoint Encryption

Centralization of management and control over applications by a corporate IT department provides more reliable support and performance for most types of business applications; in most large enterprises, it is not realistic for end users to set up their own email accounts, configure their network credentials and domain associations, or install and configure core business applications. However, most of these capabilities are possible via built-in or free tools provided on PC operating systems. Given the default and built-in tools provided by the latest PC operating systems, it is technically feasible for end users to self-configure many core functions for business computing. However, anyone who has worked a day on an IT help desk knows the impracticality of such an approach.

Similarly, manageability and scale are the main challenges when relying on free or default OS-based tools for endpoint encryption. Free programs or tools built into operating systems or added onto storage or PC hardware from OEM manufacturers are targeted at individual users' needs around data security and protection. These tools do not offer support for large-scale deployment of policies across multiple devices or groups of end users categorized by department, function, or role. Such tools are also not able to be centrally managed by an IT department; tasks such as encryption key/password generation and management and recovery must be done on a machine-by-machine basis. If end users lose their keys or forget passphrases, there is a risk that data encrypted via such tools could be unrecoverable.

The consumerization of IT presents another wrinkle to the challenge of endpoint encryption management. In enterprises where end users bring in personal laptops, the machines can come from a variety of manufacturers and providers, each of which offers a different set of full disk encryption tools for the hard drive or add-ons to the operating system for providing disk or file-based encryption services. Even in a scenario where an enterprise tries to manage endpoint encryption from the ground up, relying on building tools on the endpoint, this can quickly get out of control in the consumer environment.

Loss of control over what is being encrypted is another challenge when relying on free endpoint encryption tools, particularly for file-based encryption scenarios. End users may not know what levels of sensitivity should be applied to different types of data, and therefore encryption may be applied too heavily or too lightly. Relying on end users to make decisions about what to encrypt is the result of leaving encryption technology decision making up to the end-user community.

Managing endpoint encryption from a centralized platform alleviates the management and troubleshooting burdens of supporting endpoint data encryption on a large scale and at the same time reduces the risk of loss of critical data due to end-user error. Centralized encryption platforms also allow enterprises to centrally manage policies around encryption, with regard to full disk and file-level encryption.

Product Profile

Symantec is a global provider of security, storage, and systems management solutions that are designed to help consumers and organizations secure and manage their information assets. The company's software and services are designed to protect against multiple risks at multiple points. Headquartered in Mountain View, California, Symantec has operations in 40 countries.

Symantec offers Symantec Drive Encryption, full disk encryption for laptops, desktops, and servers. Symantec Drive Encryption is designed to provide organizations with comprehensive, multiplatform, and high-performance full disk encryption for all data, including user files, swap files, system files, and hidden files. The encrypted data is protected from unauthorized access, providing strong security.

According to the company, Symantec Drive Encryption is easy to use and provides the following benefits:

- **Reduces risk of sensitive data exposure from loss or theft:** High-performance full disk encryption
- **Ensures compliance accountability:** Single, extensible console to define, manage, and automatically enforce encryption security policy with event monitoring and reporting
- **Simplifies day-to-day operations:** Minimizes help desk, administration, and maintenance costs

Challenges

Symantec faces challenges, however, because — as the old saying goes — it's hard to beat free when it comes to price. Many organizations will see built-in full disk encryption features on PCs as good enough for many of their endpoint protection needs, especially in smaller organizations where larger encryption management infrastructures might be seen as too pricey or complex. At the same time, Symantec's competitors in the traditional endpoint security software market have acquired encryption technology and are integrating features such as full disk encryption and enterprise encryption key management into broader solutions. Meanwhile, many end users in the enterprise are moving from traditional endpoints to "post-PC" computing deployments, where endpoints such as smartphones and tablets store little to no data and access information from cloud-based data resources or virtual environments.

Conclusion

IDC believes that endpoint encryption security will remain a critical component of an in-depth security strategy, especially for enterprises with large, geographically dispersed locations and remote/mobile workforces. IDC expects the endpoint market to be dominated by integrated endpoint security suites that contain antivirus, antispyware, firewall, intrusion prevention, white listing, advanced heuristics, and encryption components. A single agent is easier to install and manage while able to match the capabilities of individual standalone products.

Like all security technologies, endpoint security has to respond to an ever-changing and increasingly aggressive threat environment. IDC believes that because of the need to respond to these threats, endpoint security solutions will not become a commodity that can be swapped in and out. Instead, organizations will need to continuously assess which products meet their existing and future security needs.

IDC believes the market for endpoint encryption products will continue to be important. To the extent that Symantec can address the challenges described in this paper, the company has a significant opportunity for success.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

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