Analyst Insight

Aberdeen Group
A Harte-Hanks Company

March 2011

Why Don't More Enterprises Adopt Endpoint Encryption?

The business case for endpoint encryption is extremely strong: regulatory compliance, significant risk (e.g., high probability and frequency of occurrence, and high financial impact per incident), and material cost savings and cost avoidance for the top performers. And yet Aberdeen's research shows that current deployments of endpoint encryption are still relatively modest. What is inhibiting enterprise adoption of endpoint encryption?

Business Context: Evidence for Encrypting Endpoints

As detailed in Aberdeen's benchmark study *Laptop Lost or Stolen? Five Questions to Ask and Answer* (February 2010), for every 100 endpoint systems provisioned by enterprises to their end-users, only 85 made it to the end of their natural lifecycle. Eleven are missing and unaccounted for, victim to unidentifiable "inventory drift". Five have been lost or stolen – not really a surprise, given the increasingly mobile nature of the extended enterprise. Of these five lost or stolen, only one is successfully recovered.

At an average total cost of $2,300 per endpoint, this 15% net loss from lost, stolen and missing endpoints translates to a cost leakage of nearly $350 per endpoint in asset value alone, not to mention the inconvenience and opportunity cost for affected end-users and administrators. Higher still is the potential impact of data loss or data exposure due to these lost, stolen or missing endpoints – an average ranging between $500,000 and $640,000 per incident based on Aberdeen's research, figures which are modest in comparison to a number of other third-party studies. By **protecting against data loss or data exposure** – e.g., by encrypting sensitive information, by remotely destroying or "wiping" the data, or by remotely disabling or "killing" the platform – the top performers averted an average of about 350 more potential incidents of data loss or data exposure over the previous 12 months compared to all others, avoiding tens of millions of dollars of cost as well as protecting their reputation and brand.

For so many topics in IT Security, it is typically either the law (i.e., *regulatory compliance*) or the lawless (i.e., *vulnerabilities and threats* derived from malicious intent) that make the business case for current investments. In the case of tracking and encrypting endpoints, however, the evidence in support of investments is extremely strong in terms of both *cost savings* and *cost avoidance* as well.

And yet Aberdeen's research shows that current deployments of endpoint encryption are still relatively modest (Figure 1). With a solid business case –

Analyst Insight

Aberdeen's Insights provide the analyst's perspective of the research as drawn from an aggregated view of benchmark surveys, interviews and data analysis.

Definitions:

For the purposes of this Analyst Insight, the term **endpoint** or **endpoint system** refers generally to end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks, netbooks) and the associated applications, data, and network connectivity on which the end-users depend.

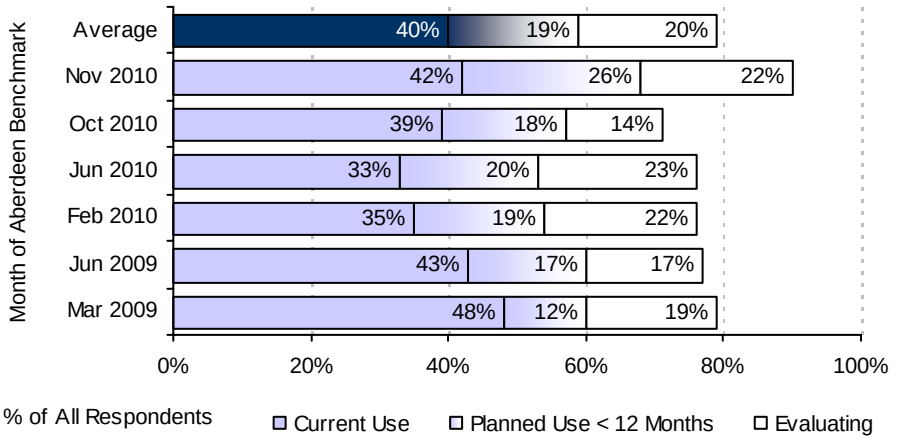
The term **mobile endpoints** or **mobile endpoint devices** refers broadly to smart phones, tablet PCs – which have become end-user computing platforms in their own right, along with associated applications, data and network connectivity – and other IP-connected devices which may or may not be associated with end-users.

and technology that has been around for some time – why is enterprise adoption of endpoint encryption so low?

Market Trends: Aberdeen's Benchmark Findings

During 2009 and 2010, Aberdeen has conducted seven benchmark studies that measure the adoption of endpoint encryption. For all respondents, the range for *current adoption* was as low as 33% and as high as 48% (Figure 1); across all studies, the average current use by all respondents was a relatively modest 40%. A healthy level of market interest is evidenced by a nearly equal number of all respondents indicating *planned adoption* in the next 12 months (19%) or *current evaluations* (20%).

Figure 1: Benchmark Findings on the Adoption of Disk Encryption



Source: Aberdeen Group, March 2011

Analysis of the Leading Inhibitors to Endpoint Encryption

Aberdeen consistently asks enterprises about the *pressures* and *strategies* that are driving their current investments in IT Security, findings which are regularly reported and analyzed in its research publications. But what about the leading *inhibitors* to current investments?

Across the same seven benchmark studies conducted over the course of 2009 and 2010, Aberdeen's findings regarding the leading inhibitors to current investments in endpoint encryption were quite consistent – as shown by the rankings in Table 1. **Complexity of the enterprise endpoint computing environment** – including the changing volume and mix of *end-users*, *platforms*, *networks*, *applications* and *data* – was the number one inhibitor to increased adoption of endpoint encryption. It's worth noting that the top six inhibitors are equally dispersed among the traditional triad of *people*, *process* and *technology*:

- *People* – Staff lack necessary bandwidth; responsibility and ownership are dispersed among different groups

- *Process* – Complexity of the endpoint environment; lack of consistent policies for data protection
- *Technology* – Complexity of currently available solutions; functionality of solutions viewed as not sufficient

Table 1: Leading Inhibitors to Current Investments in Disk Encryption (Excluding Cost-Related)

Top Inhibitors to Investments in Encryption, by Date of Aberdeen Benchmark Study	Mar 2009	Jun 2009	Sep 2009	Feb 2010	Jun 2010	Oct 2010	Nov 2010	Avg. Rank
Complexity of our endpoint environment	1	4	1	1	1	2	1	1
Staff lack necessary bandwidth	3	3	5	5	3	1	2	2
Responsibility and ownership are dispersed among different groups	4	1	4	3	2	3	5	2
Complexity of currently available solutions	2	5	3	2	5		3	3
Lack of consistent policies for data protection		2	2		4	5		4
Functionality of solutions viewed as not sufficient	5			4		4	4	5

Source: Aberdeen Group, March 2011

Selected findings from Aberdeen's benchmark research help to illustrate the growing complexities of the endpoint computing environment.

Endpoint Complexity: Changing End-User Populations

In *The Zen of Network Access* (December 2010), the total number of end-users currently supported on the enterprise network averaged about 32,000, broken down across all respondents as follows:

- Employees (32%)
- Temporary employees and contractors (10%)
- Business partners (10%)
- Customers (44%)
- Guests (4%)

Estimated growth for these segments ranged between 2% and 7% year-over-year. Note in particular that across all respondents there are more "external" end-users (business partners, customers and guests) than "internal" end-users (employees, temporary employees and business partners), by a factor of 1.4-times – leading to greater diversity and complexity, and creating significant challenges to maintaining visibility and control.

"Network endpoints are increasing at a pace never seen before."

~ IT Staff,
>$1B insurance company

Endpoint Complexity: Changing Endpoint Devices

Also from *The Zen of Network Access* (December 2010), the total number of devices currently supported on the enterprise network averaged around 19,000, broken down across all respondents as follows:

- Enterprise-managed endpoints (49%)
- End-user managed endpoints (36%)
- Other IP-enabled devices, i.e., devices not associated with end-users (15%)

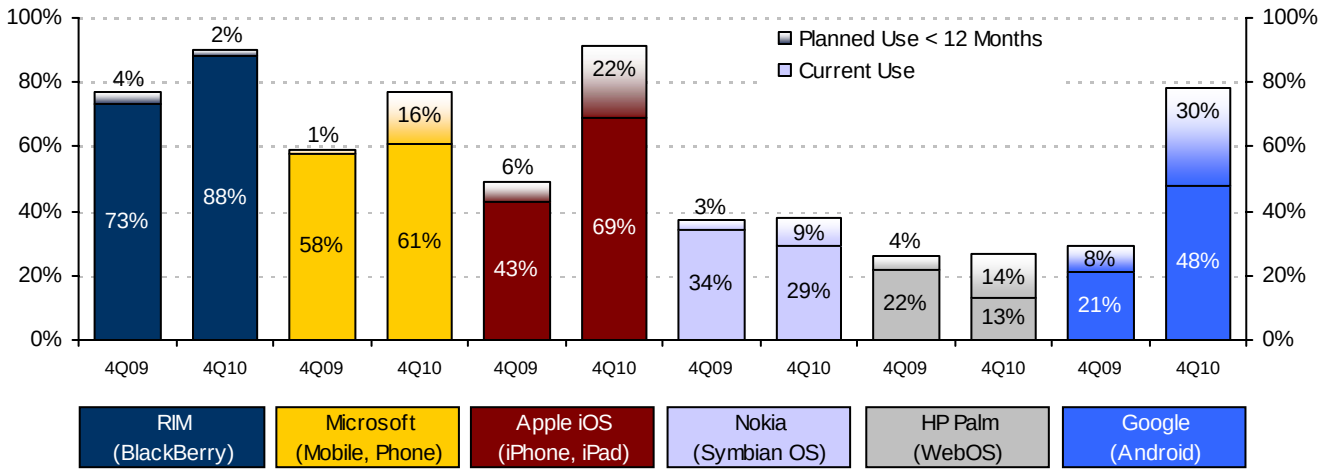
Estimated growth for these segments ranged between 4% and 6% year-over-year. Note in particular the growing population of endpoints that are *not* managed by the enterprise; for the participants in this study, the ratio of enterprise-managed endpoints to end-user managed endpoints was about 1.4. Again, this speaks to the building momentum behind diversity and complexity, and the corresponding challenges to maintaining visibility and control.

In total, there were 40% more enterprise *endpoints* than there were internal enterprise *end-users* – the excess would include, for example, "headless" IP-enabled devices (so called because they are not associated with end-users), and end-users who have more than one endpoint device (such as both a laptop PC and a network-enabled smart phone or tablet).

Endpoint Complexity: The Rapid Rise of Mobility

Rapid changes in the mobile device platforms currently deployed in the enterprise also underscores the recurring theme of diversity and complexity at the endpoints. In comparing Aberdeen benchmark data from the fourth quarter of 2009 with benchmark data from the fourth quarter of 2010 (Figure 2), the strongest incumbents in the enterprise are seen to be RIM (*BlackBerry*) and Microsoft (*Windows Mobile*, *Windows Phone*). The strongest growth in the last 12 months, however, is clearly Apple (*iPhone*, *iPad*) and Google (*Android*). Taking the survey responses for planned use in the next 12 months as a reasonable proxy for market interest and near-term growth, the momentum is currently behind Android, iOS and Windows Phone. But market share for these mobile device platforms, with their consumer-driven lifecycles, can easily shift again just as quickly.

Figure 2: What a Difference a Year Makes – Enterprise Use of Mobile Platforms (all respondents)

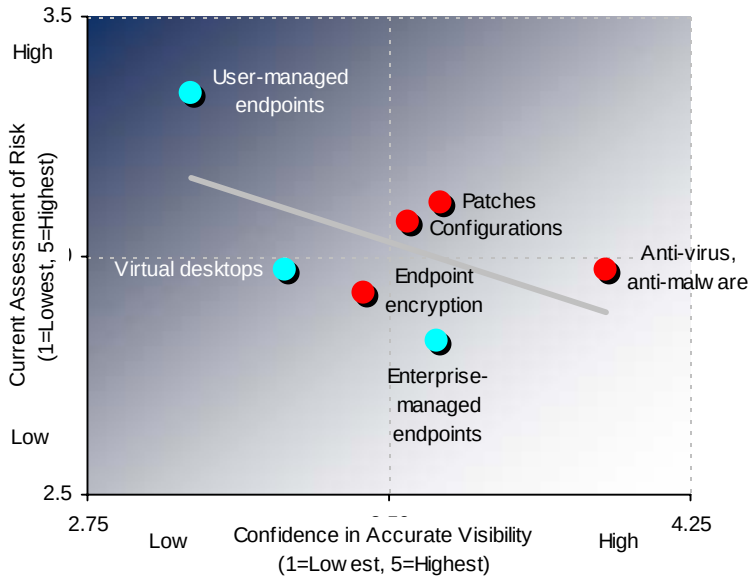


Source: Aberdeen Group, March 2011

Endpoint Complexity: Visibility versus Perceived Risk

Aberdeen's research shows that higher confidence in **accurate visibility at the endpoints** generally correlates with **lower perception of current risk** (Figure 3). That is, having the visibility that agents and software for *anti-virus / anti-malware*, *patch management*, *configuration and change management* and *endpoint encryption* solutions are installed, running and up-to-date on the endpoints that are connecting to the enterprise network generally corresponds to a lower assessment of current risk.

Figure 3: Confidence in Accurate Visibility vs. Perceived Risk



Source: Aberdeen Group, March 2011

Of these four commonly deployed endpoint security technologies, however, note that endpoint encryption is somewhat of an anomaly – i.e., it is ranked the lowest in terms of current assessment of risk, in spite of ranking the lowest in terms of confidence in accurate visibility. Given the considerable evidence to the contrary, this speaks to an ongoing need for education and awareness regarding the risks and costs of lost, stolen and missing endpoints and the associated loss or exposure of sensitive data. Since there are just four possible actions that can be taken with respect to IT Security risk – *accept* it, *ignore* it (which is the same as accepting it), *assign* it to someone else, or *mitigate* it using appropriate IT Security controls – the primary obligation of the security practitioner, in Aberdeen's view, is to be sure that the business leader who owns the risk is accepting it by deliberate decision, rather than by ignorance and inaction.

"We have actually seen the presence of both personal data and corporate data on end-user laptops to be a benefit, in terms of raising individual awareness of the value of a lost or stolen device. The people who realize that 'my life is on that laptop' are the ones who tend to value and protect their systems more, and lose them less."

~ IT Staff,
leading global semiconductor manufacturer

Endpoint Complexity: Blended Personal / Professional Use

Note also from Figure 3 that the viral growth in *user-managed* endpoints that many organizations are currently experiencing only intensifies the problems of visibility and risk, especially in comparison to traditional *enterprise-managed* endpoints. For example:

- In *Going Mobile: Securing and Managing Smart Phones and Other Mobile Endpoint Devices* (January 2010), Aberdeen noted that growing familiarity with and dependence on mobile endpoint devices in an everyday blend of both personal and professional activities introduces new categories of risk to end-users themselves that should be taken into consideration, such as personal information stored on the device that could be leveraged for identity theft (including passwords and PINs, details of credit cards and bank accounts, social security numbers, names of family members and pets, birthdays and anniversaries).
- In *Content-Aware: The 2010 Data Loss Prevention Report* (June 2010), a senior security architect for one of the largest departments in the United States government described the problem in the context of their data loss prevention initiatives. "We found early on that a huge number of data loss prevention issues were actually related to the personal information of our employees, who are using their employer-issued PCs for personal activities," he noted. "We discovered everything from online banking information to mortgage applications, tax returns, and health-related forms."

Vendor	Website	Full-Disk Encryption
Check Point Software Technologies	▪ www.checkpoint.com	▪ Pointsec Mobile Security ▪ Check Point Full Disk Encryption
CREDANT Technologies	▪ www.credant.com	▪ CREDANT Full Disk Encryption, ▪ CREDANT FDE DriveManager
Intel **- McAfee**	▪ www.intel.com ▪ www.mcafee.com	▪ Intel AES, AES-NI Hard Drives, Anti-Theft Technology ▪ McAfee Endpoint Encryption; Total Protection for Data
Microsoft	▪ www.microsoft.com	▪ BitLocker Drive Encryption
Sophos	▪ www.sophos.com	▪ SafeGuard Enterprise; SafeGuard Disk Encryption / Mac
Symantec **- PGP** **- Guardian Edge**	▪ www.symantec.com ▪ www.pgp.com ▪ www.guardianedge.com	▪ Symantec Endpoint Encryption ▪ PGP Whole Disk Encryption ▪ Guardian Edge Hard Disk Encryption
Trend Micro **- Mobile Armor**	▪ www.trendmicro.com ▪ www.mobilearmor.com	▪ DataArmor, DriveArmor
Trusted Computing Group Storage Security Subsystem	▪ www.trustedcomputinggroup.org	▪ OPAL-compatible, hardware-based self-encrypting drives are currently available from companies such as Dell, Fujitsu, Hitachi, Samsung, Seagate, Toshiba
Trustwave	▪ www.trustwave.com	▪ Trustwave Encryption; Managed Encryption
WinMagic	▪ www.winmagic.com	▪ SecureDoc Full-Disk Encryption

Source: Aberdeen Group, March 2011

As always, successful implementations are a function of *people* and *process* in addition to *technologies*. "We tested the key vendor claims for full-disk encryption in-house against a list of critical requirements, and chose our final solution based on that," noted the managing director of a mid-sized financial services firm based in South Africa. "We found holes in several vendor claims, as well as several important issues with integration that needed to be addressed." Well-defined requirements, explicit testing of critical capabilities and critical points of integration, and direct experience with vendor support are important lessons learned that will increase the probability of your own successful deployment.

Summary and Recommendations

Complexity of the enterprise endpoint computing environment – including the changing volume and mix of end-users, platforms, networks, applications and data – is the number one inhibitor to increased adoption of endpoint encryption, in spite of the extremely strong evidence in support of making such investments. Even in the face of these challenges, Aberdeen's research has shown that best practice is to:

- **Proactively protect against data loss or data exposure**, by encrypting sensitive information on the endpoints, by remotely destroying or wiping endpoint data, and by remotely disabling or killing the endpoint platform.
- **Minimize disruption and opportunity cost to end-users and administrators**, by communicating consistent polices and best practices, by regularly backing up endpoint systems and data, and by implementing endpoint protection solutions with minimal impact on the end-user experience.
- **Reduce the number of endpoints that go lost, stolen or unaccounted for**, by maintaining accurate information about the company's platforms, software licenses and data, by the ability to track and recover endpoints when possible, and by taking proactive steps to deter future occurrences.
- **Integrate solutions with existing business processes** (e.g., backups, password resets, provisioning of access to supported applications, help desk support) to support the changing volume and mix of enterprise end-users, devices, networks, applications and data; and to integrate endpoints with existing capabilities for audit, reporting, e-discovery and forensics.

In addition, words of wisdom from successful deployments suggest that **well-defined requirements**, **explicit testing** of critical capabilities and critical points of integration, and **direct experience with vendor support** are key success factors for your own successful endpoint encryption initiative.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
The Zen of Network Access; December 2010	*Laptop Lost or Stolen? Five Questions to Ask and Answer*; February 2010
Managing Vulnerabilities and Threats: No, Anti-Virus is Not Enough; December 2010	*Endpoint Encryption Head-to-Head: File / Folder vs. Full-Disk*; January 2010
The State of IT (In)Security; November 2010	*Going Mobile: Securing and Managing Mobile Endpoints*; January 2010
Five Key Capabilities for Gaining Visibility and Control over Your Network Devices, Endpoints and End-Users; September 2010	*Full-Disk Encryption On the Rise*; September 2009
What's Protecting Your Endpoints?; September 2010	*Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect*; June 2009
Putting the P in DLP; July 2010	*The Cost-Based Business Case for Data Protection*; June 2009
Content-Aware: The 2010 Data Loss Prevention Report; June 2010	*Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence*; March 2009
The Case for Enterprise Key Management: Higher Complexity and Scale at Lower Cost; June 2010	*Managing Encryption: The Keys to Your Success*; October 2008

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)