Analyst Insight

Aberdeen Group
A Harte-Hanks Company

June 2013

Understanding Your Encryption Footprint: Your Reliance on Security and Trust

Encryption has been adopted extensively across the extended enterprise, and has grown by a factor of nearly 2-times over the last five years. Encryption keys and certificates are relied upon not only as the foundation for **security**, but also as the basis for **trust** in critical IT infrastructure. Does your organization have the operational capabilities it needs to sustain security, and the visibility it needs to respond to a compromise in trust?

Business Context: My, How Encryption Has Grown …

Many organizations are surprised at how extensively **encryption** is being used throughout their extended enterprise. From *endpoints* to *networks* to *back-end systems*, encryption provides the very foundation for the most fundamental aspects of information **security**, such as *confidentiality* and *integrity* of data, and *authentication* of users and devices. From another perspective, virtually all enterprises have come to rely on encryption as the very basis for **trust** in their IT infrastructure — e.g., trust in the *devices*, *sites*, *users*, *transactions*, *communications*, and *data* that are used in the day-to-day conducting of business.

Just how extensively has encryption been deployed, and how has it grown over time? In its benchmarking approach to market research, Aberdeen routinely asks companies about their current and planned use of a wide range of IT Security-related technologies; a comparison of findings from a 2007 study with those from a 2012 study with similar demographics provides several valuable insights.

Figure 1 shows the percentage of respondents that indicated current deployments of nearly 30 solution categories related to encryption, for both 2007 (N=152) and 2012 (N=127). Some high-level conclusions:

- The current use of encryption was higher in every category over this five-year period, without exception, by an average factor of 1.9-times
- In absolute terms, the highest adoption of encryption was and remains in the area of **network** security (e.g., *VPN*, *SSL VPN*, and *encrypted Wi-Fi*), followed by encryption of data at rest in **back-end systems** (e.g., *backups*, *file servers*, *storage*, *databases*) and data in use at the **endpoints** (e.g., encryption of *hard drives*, *USB drives*, *mobile devices*, and *removable media*)
- Five-year growth among Aberdeen's respondents in these areas was highest for endpoints (2.1-times), followed by networks (1.8-times) and back-end systems (1.8-times)

Analyst Insight

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

Definitions

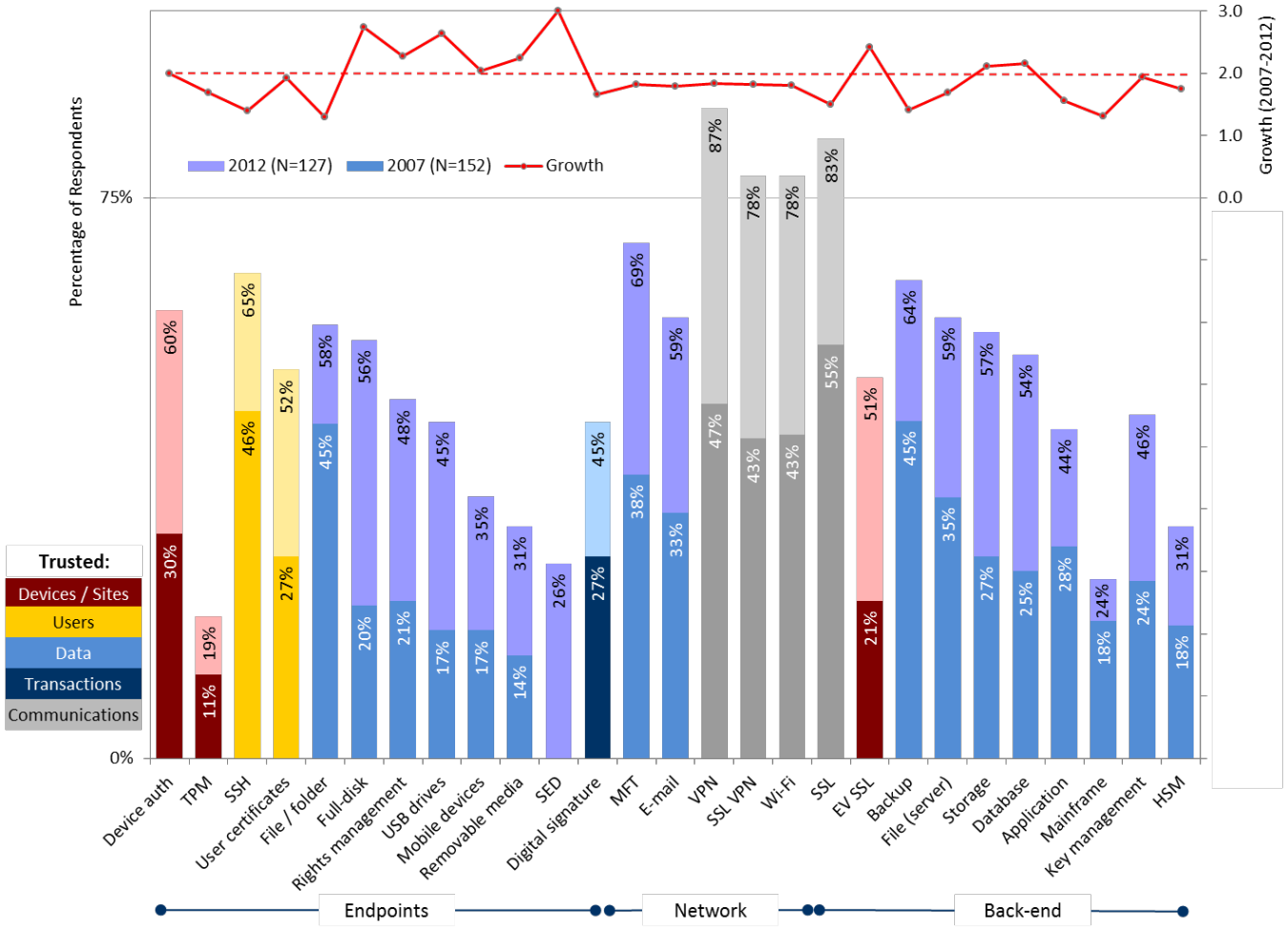
√ **Encryption** refers to the process of transforming human-readable information (*plaintext*) into a form that appears random and unreadable (*ciphertext*) without the possession of special knowledge, referred to as a *key*.

√ **Enterprise key management** refers to a common, heterogeneous solution for managing encryption keys across multiple encryption platforms and applications (i.e., as opposed to the native capabilities of a point encryption solution).

√ **Digital certificates** are credentials which have been issued by a trusted authority (a *certificate authority*, or CA); they establish a relationship between a specific end-user and a specific cryptographic key.

- From the perspective of trust, the highest adoption of encryption in absolute terms is in support of trusted **communications** (e.g., *remote access* over VPN, SSL VPN, or Wi-FI), followed closely by trusted **users** (e.g., *remote administration* using SSH) and trusted **data** (including at data at rest, data in motion, and data in use)
- Five-year growth among Aberdeen's respondents in these areas was highest for trust in devices / sites and data (2.0-times), followed by trust in users, communications, and transactions (1.7-times)

Figure 1: Current Enterprise Deployments Related to Encryption (2007, 2012) and 5-Year Growth



Source: Aberdeen Group, June 2013

Encryption and Your Enterprise Reliance on Security

As Aberdeen has noted many times before (see the *Related Research* table at the end of this report), the widespread adoption and rapid growth of encryption-enabled solutions such as those highlighted in Figure 1 also translates to a proliferation of encryption **keys** and digital **certificates**, which in turn creates a new security management problem. The typical

enterprise may have thousands of keys, and all keys have a *lifecycle* — which includes generation, distribution, storage, use, archiving, backup and retrieval, replacement, revocation, and eventual expiration and termination.

Managing this lifecycle is an essential operational aspect of maintaining effective information security; key management is not a set-it-and-forget-it business process. And yet in Aberdeen's experience, less than one out of five enterprises feel that they have an accurate inventory of their organization's keys and certificates.

As described in *KMIP, KMIP, Hooray! The Value of Standards for Enterprise Encryption Key Management* (July 2012), for the respondents in Aberdeen's 2012 study nearly half (47%) of all encryption initiatives are still managed independently — i.e., in the "silos" or "stovepipes" that result from the very natural tendency of organizations to identify a problem and deploy a solution to address it, then move on to deal with the next one. Over time, as encryption initiatives expand organically across the enterprise in this way, this can obviously lead to greater complexity and a higher total cost of ongoing operations and management.

About one-third (36%) of all respondents are addressing this complexity and cost either by *standardizing on one primary encryption solution*, or by *adopting complementary solutions such as enterprise key management* to support encryption at higher scale and lower total cost.

Encryption and Your Enterprise Reliance on Trust

The widespread adoption and rapid growth of encryption throughout the extended enterprise also creates another management concern — one which is presently under-recognized by most companies, in Aberdeen's experience — which is the organization's reliance on the **trust** in their IT infrastructure that is established by these solutions.

In Figure 2, an alternate view of the same information used to create Figure 1 is presented in a "*treemap*" format: the percentage of respondents indicating current deployments in 2012 is proportional to the *size* of each respective box (*greater adoption is larger*), and the five-year growth in adoption is represented by the *color* of the box (*higher growth is darker*).

As previously mentioned, encryption helps to establish trust in the *devices*, *sites*, *users*, *transactions*, *communications*, and *data* that are used in the day-to-day conducting of business … but if the trust in this essential IT infrastructure should become compromised, the organization needs to be in a position to react and respond quickly.

Some examples of the heavy reliance organizations are placing on trust in encryption, keys, and certificates can be readily seen by a simple visual inspection of Figure 2, including the following:

- **Endpoint encryption.** The high growth in the use of encryption at the endpoints (e.g., *full-disk encryption*, *self-encrypting drives*, *encryption of USB drives*) reflects the need to support greater enterprise

Key Management Approaches

The most common approaches to managing encryption keys involved one of the following four scenarios:

√ **Local** – localized management by the end-user; native for a single encryption application; limited key lifecycle (example: initializing encryption on a USB drive, based on establishing a password)

√ **Native** – centralized management by an administrator; native for a single encryption application; expanded key lifecycle (example: deploying a full-disk encryption solution which has its own native key management console)

√ **Independent** – silos / stovepipes of multiple native solutions for multiple encryption applications; managed independently (example: a company that deploys full-disk encryption, backup encryption, and email encryption typically ends up with three native key management systems, each independently managed)

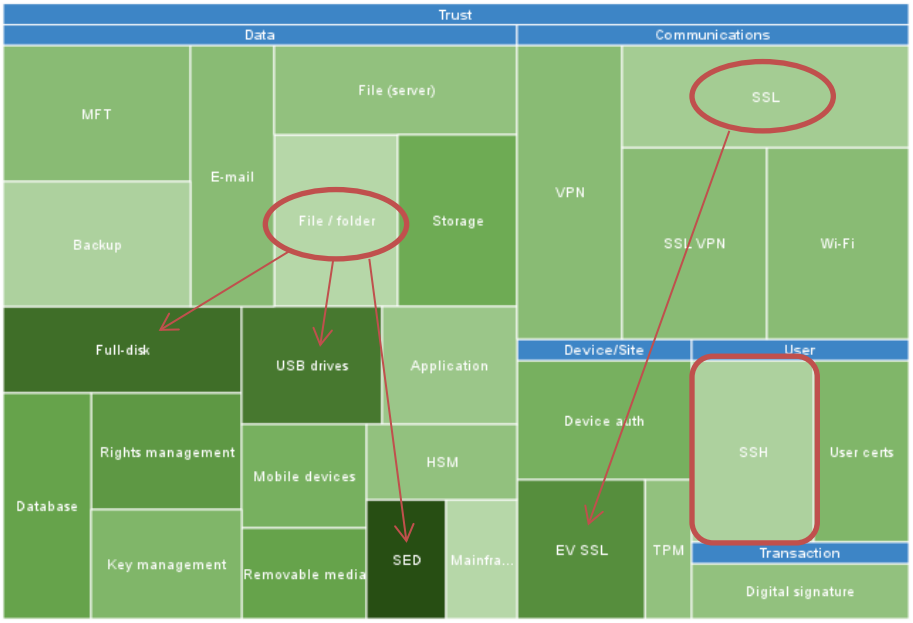
√ **Enterprise** – centralized management by an administrator; non-native for multiple encryption applications; full key lifecycle

Aberdeen's analysis of companies using enterprise key management found a total cost advantage of nearly $100 per end-user per year over those that did not, in addition to the operational efficiency of supporting encryption in greater diversity and at higher scale.

mobility, and is one tool being used to address the risks involved with "bring your own device" (BYOD) initiatives. For additional insights in this area, see Aberdeen's *Right to Choose vs. Right to Wipe: The Division Triggered by BYOD?* (August 2012).

- **Server certificates.** The large footprint of *SSL Server Certificates* and *Extended Validation (EV) SSL Server Certificates* is being targeted by attackers, who are successfully exploiting known vulnerabilities such as untrusted self-signed certificates, certificates configured for weak encryption, and unwieldy certificate revocation mechanisms. In addition, attackers have successfully pulled off more sophisticated exploits such as fraudulently issuing certificates from trusted third-party authorities, and forging certificates that are relied upon for code-signing. Most enterprises are not proactively managing the risks associated with these attacks, and are unprepared to respond quickly to a compromise — as discussed in greater detail in Aberdeen's *Is Your Enterprise Managing Its Certificates?* (July 2012).
- **SSH.** The large footprint of *Secure Shell (SSH)*, which traditionally has been used for remote administration of mission-critical enterprise systems, is increasingly being used to give enterprises low-level access and some degree of "control" over cloud-based services. In our current era of *advanced persistent threats*, it's important to keep in mind that these sophisticated **attack lifecycles** are targeting highly privileged, loosely-managed infrastructure — such as SSH — to implement and execute exploits.

Figure 2: Enterprise Trust Footprint for Encryption (2012)



Higher adoption in 2012 is larger; higher growth since 2007 is darker
Source: Aberdeen Group, June 2013

Definitions

Attack lifecycle:

√ Identify vulnerabilities (i.e., reconnaissance of IT networks and systems)

√ Implement exploits

√ Execute exploits

√ Automate exploits (i.e., run at scale)

√ Modify exploits (e.g., adapt as vulnerabilities are identified and eliminated)

The most sophisticated attacks are being designed with imperceptibility in mind, and may be carried out over a period of weeks, months, or even years.

Case-in-Point: Attacks on SSL

Recent attacks have exposed operational vulnerabilities in the ubiquitous SSL Server Certificate infrastructure that can be exploited, including:

√ Untrusted self-signed certificates

√ Certificates configured for weak encryption

√ Unwieldy certificate revocation mechanisms

In addition, attackers have successfully pulled off more sophisticated exploits that undermine the very basis for trust, such as:

√ Fraudulently issuing certificates from trusted third-party authorities

√ Forging certificates that are relied upon for code-signing

Solutions Landscape (illustrative)

Solution providers for enterprise-wide management encryption keys and certificates range from smaller specialists to multi-billion dollar firms; the following is an illustrative list:

- *Cryptsoft* (KMIP SDKs, servers and adaptors)
- *IBM* (Tivoli Key Lifecycle Manager)
- *RSA, The Security Division of EMC* (RSA Data Protection Manager)
- *SafeNet* (SafeNet KeySecure)
- *Hewlett-Packard* (HP Enterprise Secure Key Manager)
- *Thales e-Security* (Thales keyAuthority)
- *QuintessenceLabs* (Quantum Security Product Family)
- *NetApp* (NetApp Lifetime Key Management)
- *Venafi* (Certificate Manager, Key Manager, Assessor)
- *Symantec* (PGP Key Management Server)
- *Oracle* (Oracle Key Manager)
- *Liaison Technologies (nuBridges)* (Liaison Protect)
- *Voltage Security* (Voltage Key Management Server)
- *Vormetric* (Vormetric Data Security Manager)
- *CA* (CA Encryption Key Manager)
- *Cryptomathic* (Key Management System)
- *Zertificon* (Z1 CertServer)

Summary and Key Takeaways

- Encryption is deployed extensively throughout the extended enterprise.
- Encryption provides the very foundation for the most fundamental aspects of information **security**, such as *confidentiality* and *integrity* of data, and *authentication* of users and devices.
- Enterprises also rely on encryption as the very basis for **trust** in their IT infrastructure — e.g., trust in the *devices*, *sites*, *users*, *transactions*, *communications*, and *data* that are used in the day-to-day conducting of business.
- A comparison of findings from a 2007 study with those from a 2012 study with similar demographics shows that current use of encryption was higher in every one of nearly 30 solution categories over this five-year period.
- The corresponding proliferation of encryption **keys** and digital **certificates** in turn creates a new security management problem. Managing the key and certificate lifecycle is an essential operational aspect of maintaining effective information security.
- Another management concern is the organization's reliance on the **trust** in their IT infrastructure that is established by these solutions. If the trust in essential IT infrastructure should become compromised, the organization needs to be in a position to react and respond quickly.
- Examples of the heavy reliance organizations are placing on trust in encryption, keys, and certificates include **endpoint encryption**, **server certificates**, and **SSH**.
- If your enterprise is one of many that manages its keys and certificates manually — e.g., in a log book, or with a spreadsheet — or in disparate solution "stovepipes," then it likely lacks essential

operational capabilities required to sustain an effective information security program. In addition, it likely doesn't have full and accurate visibility to make a risk-based response — based on how many keys and certificates there are, where they are, what kind, and what systems are potentially at risk — in the event that trust in critical IT infrastructure is compromised.

- Companies should take immediate steps to understand their encryption footprint, by taking an inventory of existing encryption activities and establishing a baseline of use cases, data, applications, end-users, and regulatory requirements.
- Companies should evaluate enterprise key management and certificate management solutions for their potential to support greater complexity and reduce the total cost of ongoing security operations and management, and for their ability to support rapid response in the event of a compromise in trust.

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

Related Research

Protecting Your Intellectual Property: It Starts with a Single Click; May 2013
Best Practices in Managed File Transfer; April 2013
Three Steps to Successful Data Classification; February 2013
Right to Choose vs. Right to Wipe: The Division Triggered by BYOD?; August 2012
KMIP, KMIP, Hooray! The Value of Standards for Enterprise Encryption Key Management; July 2012
Is Your Enterprise Managing Its Certificates? Three Reasons It Should Be; July 2012
Endpoint Security: Hardware Roots of Trust; June 2012
The Role of Data Classification in Protecting Your Intellectual Property; May 2012
Encryption Without Tears; March 2012
Does Your Enterprise Classify Its Data?; January 2012
Left to Their Own Devices: Does Your Enterprise Have a "Dropbox Problem"?; January 2012
Too Trusted to Fail: Attacks on SSL Server Certificate Infrastructure in 2011; October 2011
Why Don't More Enterprises Adopt Endpoint Encryption?; March 2011
The CIO's View of Data Protection: Seven Symptoms to Self-Diagnose Your Data Protection Initiative; August 2010
The Case for Enterprise Key Management: Higher Complexity and Scale at Lower Cost; June 2010

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