Aberdeen Group
A Harte-Hanks Company

September 2013

Seeing Managed File Transfer as Strategic: Business Users Need Full Visibility

Business users are striving to *enable collaboration* and *integrate business processes*, and in our information-driven economy, **managed file transfer** is tied even more closely with the achievement of these critical business objectives. Mechanisms to assure file *delivery* are clearly necessary, but by themselves they are not sufficient — business users also need greater *visibility* into what's happening throughout the file movement process. This correlates not only with fewer errors, but also with reducing the time to deal with exceptions when they do occur — helping organizations to carry out their business processes in the most efficient, uninterrupted manner.

Business Context: Seeing File Transfers as Strategic

In *Best Practices in Managed File Transfer* (April 2013), Aberdeen described how leading organizations have elevated **file transfer** from a tactical problem about transmission protocols and encryption algorithms to a more strategic, holistic set of capabilities in support of their essential business processes.

Unlike the mish-mash of digital do-it-yourself approaches for sharing and transferring files — which typically includes *email attachments*, *FTP servers*, custom *programs and scripts*, and *consumer-oriented "Dropbox" solutions* — enterprise-class managed file transfer solutions are likely to include several more advanced capabilities, such as:

- Support for multiple *modes*, *file types*, and *protocols*
- Integration with multiple enterprise *platforms*, *mobile devices*, *applications*, and *existing IT infrastructure*
- Convenient, reliable, and secure *delivery mechanisms*
- Centralized *policies*, *management*, and *administration*

It's worth remembering that the purpose of managed file transfer solutions has never been merely to transfer files from one point to another. Their purpose is to provide convenient, reliable, and secure means to *enable collaboration* between individuals, and to *integrate business processes* within and between organizations.

In an information-driven economy, managed file transfer is tied even more closely into the achievement of critical business objectives — which means that business users need even greater **visibility** into what's happening throughout the file movement process. These are the people who tend to ask and answer questions such as: Was the file delivered? Who has accessed this information? Were the inventories updated? Were the claims

Definitions

File transfer has multiple *modes*:

√ **Person-to-Person** – an individual sender transfers file(s) to one or more specific receivers

√ **Process-to-Person** – a process or application generates files for specific individuals

√ **Person-to-Process** – an individual submits files into a process or application

√ **Process-to-Process** – file transfers are initiated programmatically by one process and received by another

For each mode, the element of *time* also comes into play:

√ **Ad Hoc / On Demand** – file transfers are initiated as needed, as opposed to at a specific scheduled time

√ **Scheduled / Event-Driven** – file transfers are initiated based on a specific schedule, or triggered by the occurrence of a specific event
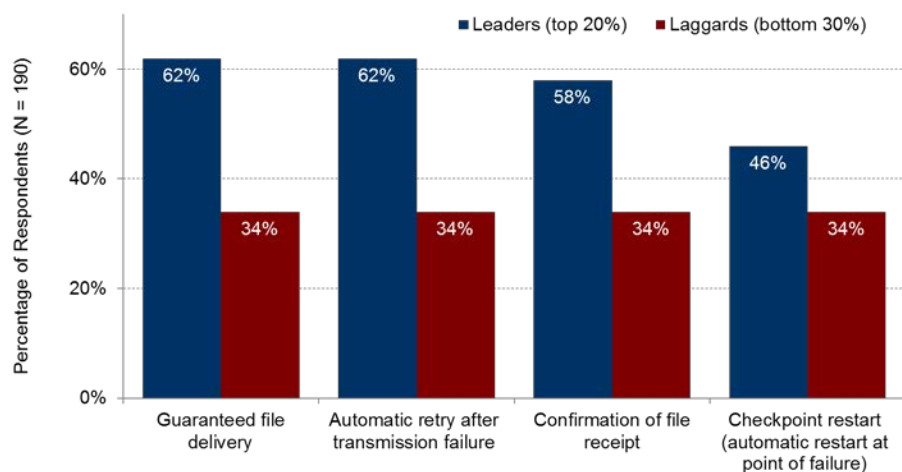
Aberdeen *Group*
A Harte-Hanks Company

submitted? Were the transactions made? Business users need higher-level information than cryptic error messages — or even worse, no information at all. The first time business users know they have a problem with business-critical file transfers should not be when their colleagues or customers call them to complain about it. As Tom Hagen, the *consigliere* to Don Vito Corleone in the movie The Godfather explained to the movie producer Jack Woltz, "Mr. Corleone is a man who insists on hearing bad news immediately."

Aberdeen's Research Findings: Leaders Raise the Bar on the Visibility of File Transfer Activities

Aberdeen's research shows that, beyond basic "tracking and tracing" capabilities — analogous to the on-demand lookups provided by physical package delivery services — the leading performers have a consistent, unified view of the activities and events related to file transfer. This correlates not only with fewer errors, but also with reducing the time to deal with exceptions when they do occur — helping organizations to carry out their business processes in the most efficient, uninterrupted manner.

Reliable delivery of file transfers is obviously important; Leaders are much more likely than Laggards to have deployed solutions with capabilities such as *guaranteed file delivery*, *automatic retry* after a transmission failure, and *confirmation of receipt* (Figure 1). For enterprise-class managed file transfer solutions, basic tracking and tracing capabilities to make ad hoc inquiries on the status of file transfers have become table stakes.

Figure 1: Obviously, Assurance of File Delivery is Important
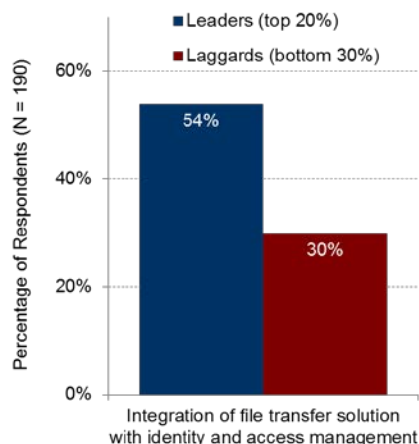

Source: Aberdeen Group, September 2013

Integration with an organization's existing IT infrastructure is also an important consideration for enterprise-class managed file transfer solutions. For example, integration with the existing *identity and access management* infrastructure (Figure 2) can allow organizations to customize what

Aberdeen *Group*
A Harte-Hanks Company

information a given end-user can access and transfer based on their job function (*role*) or on other business *rules*. In addition, such integration can enable administrators to leverage the organization's existing policies and processes for control of the access and flow of information, such as *attestation* and *separation of duties*.

Figure 2: Integration with Existing Infrastructure is also Important

Source: Aberdeen Group, September 2013

For business users, the value of visibility is in seeing the file movements that are relevant to themselves, and in reducing the time it takes to deal with errors and exceptions when they do occur. How quickly can problems be identified? How quickly can problems be remediated?

Figure 3: Visibility into the File Movements that are Relevant
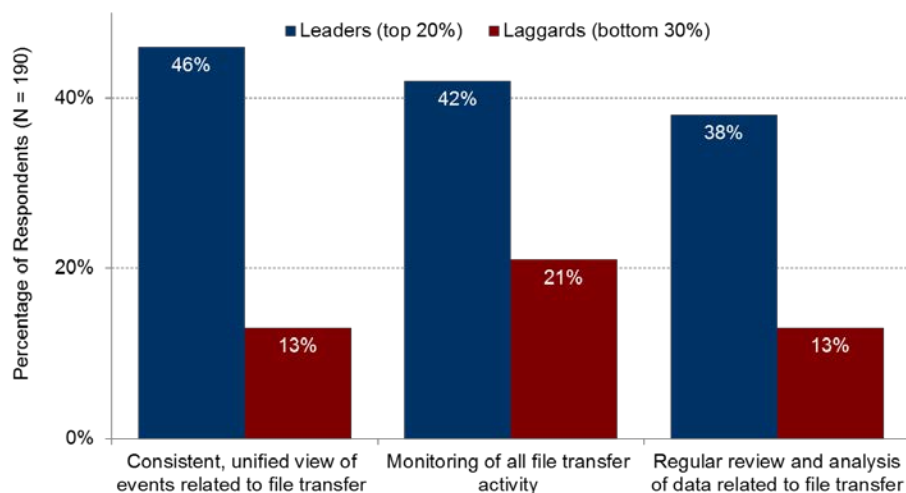
Source: Aberdeen Group, September 2013

Definitions

√ **Identity and Access Management (IAM)** refers to managing end-user identities and access privileges over their lifecycle – from initial provisioning, to real-time daily operations, to ongoing end-user support, to eventual de-provisioning and revocation

√ **Separation of duties** (or **segregation of duties**) refers to dividing tasks and associated privileges for certain business processes among more than one individual, to help prevent potential abuse or fraud

√ **Attestation** refers to the periodic validation that enterprise end-users have appropriate access rights, i.e., as part of providing assurance that the right end-users have the right access to the right resources at the right times

√ A **role** is typically a job function within the context of a specific organization; all end-users assigned to a particular role are provided with equivalent *entitlements* and access *privileges*

√ A **rule** is a logical expression of *policy* regarding access to protected resources that can be evaluated and combined by a *Policy Decision Point*

In addition to status, business users also want to see trends and historical comparisons: Are *Service Level Agreements* being met? Are *key performance indicators* tracking according to plan? Is *business partner behavior* being tracked, scored, and managed? In Aberdeen's research, the leading performers are found to be 2- to 4-times more likely than Laggards to capture, monitor, and review such information and events related to their enterprise file transfer activities (Figure 3).

In Figure 4, we see that Leaders are 2-times more likely than Laggards to have real-time notifications of exceptions, events, or policy violations related to file transfers — as well as 2-times more likely to seek out and eliminate the root causes, to prevent such issues from occurring again. Strategically, this is a theme that Aberdeen has recently noted as emerging in many other aspects of traditional IT Security: the recognition that **prevention** cannot be successful one hundred percent of the time, and so it is being *augmented* with an increased focus on rapid **detection** and **response**.

Figure 4: Having Visibility is Good; Taking Action is Even Better
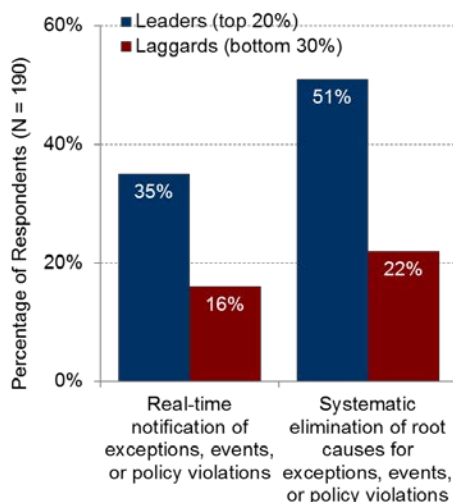
Source: Aberdeen Group, September 2013

## *Visibility is the Strongest Differentiator of Top Performance*

The traditional bar chart format of Figure 1, Figure 2, Figure 3, and Figure 4 can make it difficult to see that capabilities related to **visibility** for business users are in fact the *strongest* differentiators of top performance in managed file transfer. In Figure 5, the same research findings are presented in a different way:

- The x-axis shows the *absolute* degree of adoption by the leading performers in Aberdeen's study, on a scale of 0% (none of the leading performers indicated having a given capability) to 100% (all of the leading performers indicated having that capability)

- The y-axis shows the degree of adoption by the leading performers *relative* to that of the lagging performers; i.e., an equal percentage of

Aberdeen Group
A Harte-Hanks Company

Leaders and Laggards having a given capability would be a ratio of 1.0, while a ratio of 3.0 means that Leaders were 3-times more likely than Laggards to indicate having that capability

- Color is used to distinguish selected groupings of capabilities; e.g., yellow shows capabilities related to assurance of file delivery, and blue shows capabilities related to increased visibility of file movements for business users

Figure 5: Visibility is the Strongest Differentiator of Best-in-Class
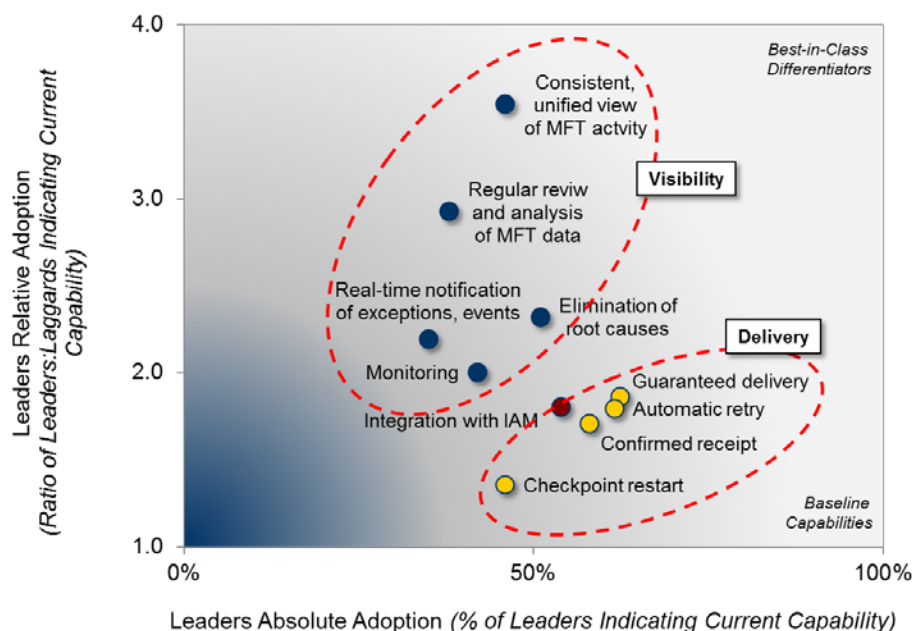
Source: Aberdeen Group, September 2013

In this format, it's easy to see why capabilities related to assurance that files will eventually be delivered can be considered *baseline* — they are highly present in leading organizations and they have relatively high presence in lagging organizations as well. On the other hand, capabilities related to visibility are much more strongly correlated with top performance: they reflect moderate to high absolute adoption by the Leaders, and high adoption by Leaders relative to that of Laggards.

This brings us back to the fundamental point. Business users are primarily concerned not about protocols and file formats but about *enabling collaboration* and *integrating business processes*, and in our information-driven economy, managed file transfer is tied even more closely to the achievement of such critical business objectives. Mechanisms to assure file **delivery** are clearly necessary, but alone they are not sufficient — business users also need greater **visibility** into what's happening throughout the file movement process.

Aberdeen Group
A Harte-Hanks Company

Quantifying the Benefits of Top Performance

Better visibility over file movements should ultimately be reflected in tangible business benefits such as fewer errors (*cost avoidance*) and more efficient processes (*cost savings*, *faster time-to-revenue*), both of which can be seen in Aberdeen's research.

For example, Table 1 summarizes the significant advantage of Leaders over Laggards in terms of *data loss or data exposure*, *audit deficiencies*, and *unauthorized access to enterprise resources* related to managed file transfer. The total cost per incident can vary widely (in Aberdeen's studies, the average is in the hundreds of thousands of dollars per incident). Readers are encouraged to do their own back-of-the-envelope calculations regarding the benefits to leaders from such cost avoidance (see sidebar at right).

Back of the Envelope Example

Incidents experienced in the last 12 months

√ Laggards: 11.2

√ Leaders: 0.7

√ Difference: 10.5

Average cost per incident

√ $640K (use your own figure)

Leaders cost avoided

√ 10.5 x $640K = $6.7M / year

Table 1: Selected Performance Metrics for Managed File Transfer

Average for All Respondents (last 12 months)	Leaders (top 20%)	Laggards (bottom 30%)	Leader Δ
Incidents of data loss or exposure related to file transfer	0.7	11.2	*16.7-times*
% of respondents indicating NO incidents due to:			
Data loss or data exposure related to file transfer	94%	10%	*9.4-times*
Audit deficiencies related to file transfer	83%	2%	*41.5-times*
Unauthorized access to enterprise resources	89%	15%	*5.9-times*

Source: Aberdeen Group, September 2013

Aberdeen's research on *B2B Collaboration: The Impact and Advantages of Managed File Transfer* (June 2012) found that managed file transfer was strongly correlated (by a factor of 10-times) with companies being able to onboard new business partners within days — a business benefit which should be straightforward for readers to quantify as *faster time-to-revenue*.

The impact of better visibility on the flow and efficiency of critical business processes is perhaps the strongest and most sustainable business benefit for Leaders in managed file transfer, particularly given the high cost of process *downtime*. For example, for every $10M in annual revenue generated by a given process or application, the direct cost of downtime is $1,140 per hour (assuming that revenue is continuous, and that all revenue lost to downtime goes unrecovered). Again, readers are encouraged to do their own back-of-the-envelope calculations for the impact of faster or more reliable business processes, based on the parameters that best describe their own business environment.

Solutions Landscape (illustrative)

Aberdeen's research indicates that, for most companies, much of the current file transfer activity takes place below the radar. As a prelude to any evaluation process for managed file transfer solutions, companies should

Aberdeen Group
A Harte-Hanks Company

inventory existing file sharing activities to establish a baseline for modes, volumes, frequency, methods, applications, end-users, and systems.

Solution providers for managed file transfer can range from smaller specialists to global, multi-billion firms; Table 2 provides an illustrative list.

Table 2: Solutions Landscape for Enterprise Managed File Transfer (illustrative)

Company	Web Site	Solution(s)
IBM	www.ibm.com	IBM Managed File Transfer suite (includes IBM Sterling Connect:Direct, File Gateway, File Transfer Service, Control Center, Business Monitor, Secure Proxy, QuickFile)
Attachmate	www.attachmate.com	File Express, Reflection for Secure IT
Seeburger	www.seeburger.com	Seeburger Business Integration Suite (BIS)
GlobalSCAPE	www.globalscape.com	Enhanced File Transfer, Managed Information Xchange (MIX) SaaS
Biscom	www.biscomdeliveryserver.com	Biscom Delivery Server (BDS)
Axway	www.axway.com	Axway SecureTransport, File Transfer Direct
PKWARE	www.pkware.com	SecureZIP, SecureZIP PartnerLink
TIBCO	www.tibco.com	TIBCO Managed File Transfer, TIBCO Slingshot
Ipswitch	www.ipswitch.com	MOVEit, MessageWay
Attunity	www.attunity.com	Attunity Managed File Transfer (formerly Repliweb)
OpenText	www.opentext.com	OpenText Managed File Transfer
Liaison	www.liaison.com	Liaison Exchange
Cleo	www.cleo.com	VL Trader, LexiCom, Harmony

Source: Aberdeen Group, September 2013

Summary and Key Takeaways

Leading organizations have elevated **file transfer** from a tactical problem about transmission protocols and encryption algorithms to a more strategic, holistic set of capabilities in support of their essential business processes.

For most companies, much of the current file transfer activity takes place below the radar. Many have a mish-mash of digital do-it-yourself approaches for sharing and transferring files— which typically includes *email attachments*, *FTP servers*, custom *programs and scripts*, and *consumer-oriented "Dropbox" solutions*.

In contrast, enterprise-class managed file transfer solutions are likely to include several more advanced capabilities, such as support for multiple *modes*, *file types*, and *protocols*; integration with multiple enterprise *platforms*, *mobile devices*, *applications*, and *existing IT infrastructure*; convenient, reliable, and secure *delivery mechanisms*; and centralized *policies*, *management*, and *administration*.

Business users are primarily concerned not about low-level protocols and file formats but about *enabling collaboration* and *integrating business processes*, and in an information-driven economy, managed file transfer is tied even

Aberdeen Group
A Harte-Hanks Company

more closely into the achievement of critical business objectives. Mechanisms to assure file **delivery** are clearly necessary, but alone they are not sufficient — business users also need greater **visibility** into what's happening throughout the file movement process.

Aberdeen's research confirms that better visibility over file movements is ultimately reflected in tangible business benefits such as fewer errors (*cost avoidance*) and more efficient processes (*cost savings*, *faster time-to-revenue*). For example, Leaders were on average 10-times more likely than Laggards to experience *no* incidents of data loss, audit deficiencies, or unauthorized access related to file transfer in the last 12 months, and experienced an average of 16.7-times fewer actual incidents.

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

Related Research
Incident Response: Detecting and Containing Earlier in the Attack Lifecycle; July 2013 *SharePoint Collaboration: Secure and Mobile*; June 2013 *Best Practices in Managed File Transfer*; April 2013 *Protecting Your Intellectual Property: It Starts with a Single Click*; April 2013 *Three Steps to Successful Data Classification*; February 2013 *Tokenization Gets Traction*; July 2012 *B2B Collaboration: The Impact and Advantages of Managed File Transfer*; June 2012 *Secure File Sharing in the UK*; 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	*Email and Web Security, Differentiated: Protecting Content is King*; Nov. 2011 *DLP, the Ideal Referee: Let the Game Go On!*; November 2011 *Secure / Managed File Transfer: Why You Should Be Looking More Closely Right Now*; August 2011 *Why Don't More Enterprises Adopt Endpoint Encryption?*; March 2011 *Putting the P in DLP*; July 2010 *Content-Aware: The 2010 Data Loss Prevention Report*; June 2010 *The Case for Enterprise Key Management: Higher Complexity and Scale at Lower Cost*; June 2010 *Enterprise Rights Management: Persistence Pays Off*; August 2009 *Microsoft SharePoint: The Comedy (and Tragedy) of the Commons*; July 2009 *The Cost-Based Business Case for DLP*; June 2009
Author: Derek E. Brink, CISSP, Vice President and Research Fellow for IT Security and IT GRC (Derek.Brink@aberdeen.com)