

Fax over Cloud
Secure Fax Showcase

Special Report

Understanding Secure Fax and Document Delivery Solutions for the Enterprise

August 2014

By:
Mark D. Malone

Executive Overview

Organizations today devote significant amounts of their annual budgets to securing their IT networks, the applications that run on them, and the data managed by the applications. One of the most important security considerations IT personnel face is the need to protect sensitive data that comes from healthcare, financial and legal documents among others. Regulations like the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability & Accountability Act (HIPAA) are driving companies to ultimate compliance. In addition, Sarbanes-Oxley (SOX) and a handful of other directives in the financial sector have changed the game of document security forever. The risks associated with violations to these compliance orders include loss of data; security breaches of confidential information and of course -- the penalties, fines and imprisonment possibilities for the most flagrant violations.

One area of concern from a data security standpoint is the protection of fax documents. Faxes are a perfect example of data that needs to be kept secure since they typically contain vital information from a variety of sensitive sources. Because companies today rely on automated fax server systems to manage their faxing needs, a secondary look at these systems from a security standpoint must be made. Many compliance directives are forcing fax system users to re-think their deployments so as to ensure protection of the fax data from endpoint to endpoint. Because faxing systems interconnect with a variety of other business applications that generate the fax documents, a faxing system's architecture and design with respect to security and data protection must be carefully reviewed.

Market data from a variety of sources has provided conclusions that security and compliance concerns rank high among companies' IT initiatives. In addition to security measures, organizations face issues of achieving IT cost reductions through consolidation, the need for higher productivity and seamless redundancy for all their mission critical IT applications. Choosing a fax solution that encompasses all of these critical factors can be a daunting challenge. There are many choices available, but not all of them are the same, especially when it comes to implementing secure faxing and secure document delivery options as part of the complete solution. This paper highlights research that was conducted about an industry leading fax server solution and how it addresses secure faxing and secure document delivery holistically.

Market Overview: Secure and Reliable Faxing Today

The fax market today is growing and undergoing significant change. The use of the fax machine has gone by the wayside in lieu of computer-based fax technologies – now reaching 30+ years on the market. Companies that experience growth will typically migrate from the use of standalone fax machines to fully automated faxing solutions that can be on-premise fax solutions, cloud-based fax services, or a combination/hybrid of both. Cloud-based faxing is growing the most as companies are recognizing the benefits of outsourcing their faxing services to the cloud. The market for automated fax servers and cloud services remains solid and is characterized by Davidson Consulting as follows:

Automated Fax Industry Segment	Market Observation (Davidson) ¹
Fax Services (cloud-based)	The market will increase from \$1.365 billion in 2013 to \$2.795 billion in 2018, a 15.9% compound annual growth rate (CAGR).
Fax Servers (on-premise)	The market will grow from \$385 million in 2012 to \$455 million in 2017, a 3.4% compound annual growth rate (CAGR).
Fax over IP (FoIP) Servers	The market for FoIP servers will grow at 10.2% compound annual growth rate (CAGR) by 2017,

Factors that drive the growth of fax: The numbers above indicate a growing trend in the use of some type of automated fax server or cloud-based service. Many tangible factors are still driving the growth of automated faxing solutions today:

Market Driver	Examples
Cost savings	<ul style="list-style-type: none"> • Significant reduction in costs for fax machines, dedicated phone circuits, and associated fax supplies • Faster fax processing times • Low total cost of ownership (TCO) due to network consolidation
Productivity improvements	<ul style="list-style-type: none"> • Reduced time spent managing faxes, sending long documents, and dealing with paper jams and other physical problems associated with fax machines • Streamlined integrations to other business applications: Email, ERP/CRM, Healthcare and Financial applications, etc. • Process automation and workflow for faxes
Centralized administration	<ul style="list-style-type: none"> • Manage faxes, users and internal fax services, from a single centralized location • Virtualization and redundancy scenarios • Convergence of fax, voice, email technologies (Unified Communications)
Security and compliance	<ul style="list-style-type: none"> • Eliminate risks associated with lost or delayed faxes • Ensure no unauthorized viewing of fax documents • Reduce risk of security breaches • Encrypt fax documents at rest and in transit

The above list of market drivers summarizes the factors that weigh heavily in favor of choosing and implementing an automated fax system that can provide these benefits.

Most organizations utilize fax systems that are network-based and can either be located in the cloud as a service, on-premise as part of the network enterprise or a hybrid thereof. Not all automated

¹ Source: Davidson Consulting Citing Sources: [<http://davidsonconsultinginc.com/reports.html>]

faxing systems or services are designed the same when it comes to fax data security however. Not all can ensure 100% end-to-end protection of the actual fax and the information it contains. This places them at risk for security breaches and compliance violations. The following section highlights some of the more common security concerns with respect to automated faxing solutions.

Security Challenges and Drawbacks with Unsecure Faxing

Many of today's fax solutions have loopholes where breaches could occur – something no longer acceptable given today's rigid standards like HIPAA, PCI DSS and others. It is often thought faxes are inherently secure by nature. After all, while in transit they travel over physical phone lines or via the internet as secure data packets – both of which embed the fax as a TIFF image via a dedicated connection – processes that are known to be hack-proof and secure from prying eyes. Hacking into a fax while in transit is not something often heard of and is a big reason why today faxes are still considered secure, legal and binding versions of their original documents. Compared to the use of unsecured physical fax machines, network fax servers provide inherently more security because they manage fax documents inside the server's ecosystem which is behind the company firewall or in a secure cloud environment. Not all fax server solutions are the same however, especially when it comes to securing the fax during its entire life cycle, both on the outbound (create and send a fax) and inbound (receive, route and process a fax) side of things.

Security issues may arise at a few points along the life cycle of a fax document. Organizations seeking a total fax solution and are concerned about security issues should consider the following drawbacks or concerns when it comes to fax data security:

- Faxes that are “at rest” on the fax server may not be encrypted
- Faxes sent or received as email attachments may not use secure connections like TLS, e.g.
- Interconnections between the fax server and other processing components may not be secure
- Remote access to the fax system (via web, e.g.) may use unsecured connections
- Alternative delivery options may not be available (secure file transfer, e.g.)

The above list is just a small sample of considerations to make when choosing a secure fax solution. Organizations must first size up their security concerns and determine which solution will best fit their needs. Moreover, it almost goes without saying but despite all the inherent abilities an automated faxing solution brings to the table as far as security, certain human factors could result in confidentially or privacy breaches as well. Organizations must be able to properly configure and deploy the fax solution such that common mistakes are minimized. Below is a list of some of the most common errors made that stem from improper fax system configuration:

- User permissions do not adequately protect unauthorized viewing of confidential fax information
- Incorrect or erroneous routing rules may cause unintentional access to confidential faxes
- Internal routing of faxes may generate multiple copies of the fax document
- Incorrect phone numbers are dialed and faxes are sent to wrong locations
- Captured faxes are sent to printers that are unsecure
- Fax system not synchronized to company directory, causing duplication or errors

Secure Alternatives: FTP/SFTP

File Transfer Protocol is one of the oldest protocols for transferring files over the internet or between two computers over a network connection. Many companies rely on FTP for digital files that exceed mail server limits. But FTP is not the panacea. According to Biscom, “although ease-of-use is a critical requirement, the primary IT concern with FTP is the lack of security and manageability. SFTP is often cited as a secure alternative, but it still requires significant technical knowledge by its users – server or IP addresses, client software installation, and other technical expertise is a must – not to mention that people trying to receive files through SFTP must also be similarly adept at this technical level.” The point is well taken: SFTP is too complex a solution.

Secure Fax and Document Delivery Solutions: Deployment Types and Components

When considering what type of fax solution to implement, careful scrutiny must be first made as to where the system will reside and who will manage it. In addition, there are choices to make about features and capabilities and the system’s ability to maintain faxes and documents securely. That being stated, the following charts will help outline some of the necessary components and deployment types needed to implement a secure and reliable solution.

Fax deployment type	Description/Considerations
On-Premise Fax Server	Software, server hardware and telephony interfaces are purchased and operated internally in an organization. The telephony interfaces can be hardware-based or via FoIP software. Users have full control over the entire system and can access connectors and APIs to integrate the faxing system with a variety of other business applications. Choose a solution that offers secure connection options, and can encrypt faxes while at rest.
Cloud-based (SaaS) Fax Service “email to fax” solution	This is Software as a Service (SaaS) model via the cloud. All software, hardware and telephony interfaces are hosted by a service provider. Also known as an email to fax solution, faxes are sent and received usually via an email interface. Must have secure sending ability (like transport layer security TLS for example) over SMTP.
Cloud-based (SaaS) Fax Service with Enterprise Features	Another SaaS deployment model, only with additional advanced enterprise fax features and capabilities including integration possibilities such as those typically seen in an on-premise solution including application integrations and synchronization of users via Active Directory for example.
Hybrid Fax Solution	An organization can choose to deploy both an on-premise fax solution that is tied to a hosted fax service. This combination can support business continuity as well as peak load when the internal fax servers are over-utilized.

Secure Fax and Document Delivery Component	What to look for
Fax Server	The core of the automated fax application system is the fax server. Manages the sending and receiving of faxes. The server should have options to be deployed on-premise, or as a hosted solution. Secure connection to the server should include support for secure socket layer (SSL).
Fax Server Integration Tools	Every fax server application should come with the tools and architecture to reliably support integrations with other platforms, various fax clients, devices, etc.
SQL Database	Seek a solution that uses a database like Microsoft SQL Server. One use of the database is it can store the fax metadata for every fax that is sent or received.
Client Interfaces	The fax server must have the ability to support various client interfaces like MS Outlook, SharePoint, Web, MFPs, APIs etc. Look for solutions that support transport layer security (TLS) over SMTP.
Secure Document Delivery Options	No fax solution is complete unless there are other secure delivery options that augment fax delivery. This can include secure file transfer options among others.
Secure File Synchronization Options	Allows organizations to share corporate files and fax documents easily while giving IT control and management of users, devices, and access. Choose a solution that works with the existing security and authentication infrastructure.

Biscom: A Secure Fax and Document Delivery Solution

Many solutions are available that address the issues and items brought forth in this briefing. One solution of note comes from Biscom, Inc. a company founded in 1986 and makers of FAXCOM® and FAXCOM Anywhere. Biscom pioneered the world's first computer-based fax server that offered true, secure document delivery and today they have thousands of servers installed representing millions of pages faxed per day . They evolved their fax server technology over the years to face the ever-growing demands for more and more security features that were driven by the ever-changing marketplace. Biscom serves all market segments, but is particularly strong in financial, healthcare, legal and government verticals. To complete the overall security picture, Biscom also offers Secure File Transfer (SFT) and enterprise file synchronization and sharing (Verosync) products to handle secure file delivery, remote file access, and collaboration.

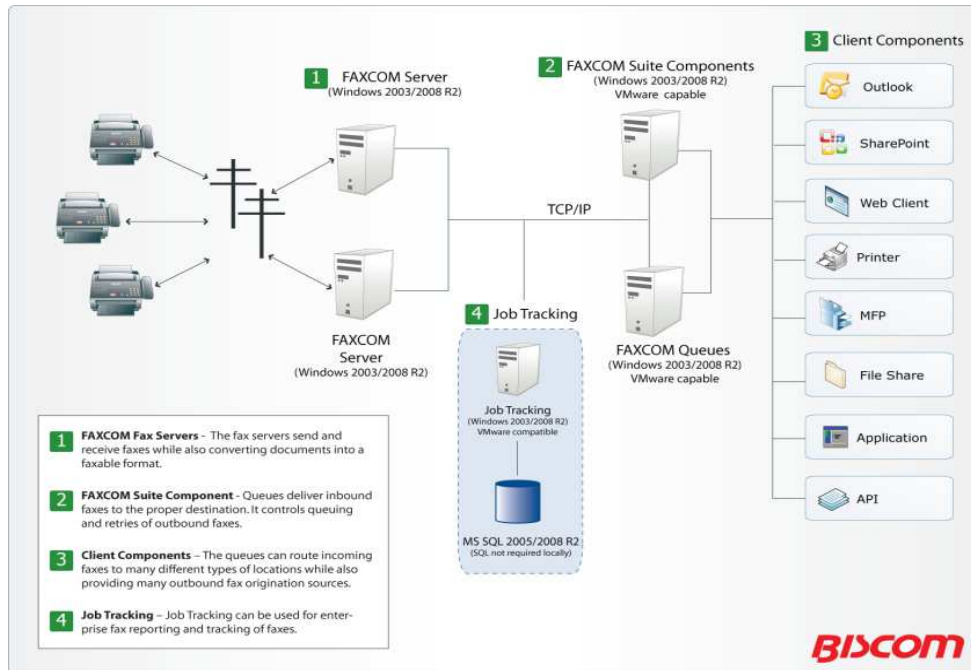


Figure 1: The Biscom Secure Document Solution Overview.

Secure Fax and Secure Document Delivery are not Biscom brands. They are however inherent capabilities of the Biscom FAXCOM Server, FAXCOM Suite, FAXCOM Anywhere, Secure File Transfer (SFT) and Verosync file synchronization products. As mentioned previously, the foundation of any solution that needs to secure business documents while in transit and at rest lies within the overall design and architecture of the faxing solution itself. Biscom offers a multi-tiered, scalable and hierarchical design that has proven itself over the last 28+ years in the marketplace. As a result, they provide true, end-to-end document protection capable of meeting the most rigid security standards of today. The following table outlines the scope of Biscom secure fax solutions:

Biscom Secure Fax and Document Delivery	
Biscom Component	Description
FAXCOM Server	The FAXCOM Server plays an important role in the overall secure fax solution. The server can be on-premise or hosted, or operate as a hybrid server/cloud solution. It handles document conversion and translation natively so it is a high-performance, scalable system. In addition, FAXCOM Servers perform the transmission and reception of faxes by connecting to the public switched telephone network or a voice over IP service
FAXCOM Suite	This is Biscom's key management tool that provides the user and administrative capabilities within the fax server system. Its architecture is scalable as well as secure. The FAXCOM Suite manages the connection of the client components via Queues (see below).
FAXCOM Suite: Client Components	While Biscom provides customizable desktop and Web clients, users can also send and receive faxes and attachments from virtually anywhere through a variety of interfaces, including Microsoft Outlook, Simple Mail Transfer Protocol (SMTP) mail clients,

	Microsoft SharePoint, multi-function printers (MFPs), business applications and programming interfaces (APIs).
FAXCOM Queues	This is the FAXCOM service that integrates fax users and network resources with FAXCOM Servers. While the FAXCOM Servers perform the transmission, reception and translation of faxes, FAXCOM Suite deploys Queues that perform the integration to the client components. Suite is installed as a Microsoft Management Console (MMC) snap-in, and Queues are distributed to remote server locations. Queues can be described as lightweight software gateways.
Mailbox Server	As part of an improvement to the FAXCOM solution overall architecture, Biscom created Mailbox Server. Mailbox Server is the interface between the FAXCOM clients and the rest of the FAXCOM system. According to Biscom, <i>“Mailbox Server accesses a Microsoft SQL Server which stores the fax metadata for every fax that is sent or received. Mailbox Server provides significantly more control over faxes, more complex workflows, and better security.”</i>
FAXCOM Job Tracker Server	This is a component that monitors the progress of both received and transmitted faxes in the FAXCOM system. The service tracks and indexes FAXCOM jobs, records monitored events in a database, and generates alarms when jobs do not complete in a timely manner.

FAXCOM Anywhere – Cloud Based Secure Faxing

To meet the market demand for cloud services, Biscom offers their FAXCOM Anywhere solution. FAXCOM Anywhere comes in two versions to meet a wide range of needs: Office Edition and Enterprise Edition. The Office Edition offers a competitive email-to-fax solution that rivals eFax, ConcordFax, OpenText, Retarus and others. Office Edition targets the small-to-medium market segment and has robust functionality including SMTP integrations, optional installed printer drivers (print-to-fax) and custom cover pages - ideal for companies with large numbers of individual email users that need desktop fax support. From a security standpoint Office Edition offers the ability to use Transport Layer Security (TLS) over SMTP.

Enterprise Edition is a fully featured cloud faxing solution that meets the needs of not only desktop email users, but across all applications among an enterprise. This includes:

- Email systems: Microsoft Exchange, Office 365, Domino, and SMTP
- Fax clients: Web, Mobile and Desktop
- Software applications: SharePoint, ERP, SAP, Oracle, , iSeries
- Healthcare applications: EMR, GE Centricity, Epic, Siemens, McKesson, etc.
- Enterprise content management: Hyland OnBase, FileNet, Documentum
- Programming interfaces: Web Services API, C++, Python, Java, .NET

Biscom Datacenters: FAXCOM Anywhere utilizes datacenters that are completely redundant and secure. According to them, the datacenters are SSAE 16 Type 2 compliant. Enterprise systems are supported via Secure Socket Layer (SSL) and store the faxes on the customer side, not in the cloud and include an encryption at rest option – a feature vital for security and compliance mandates.

Secure File Transfer (SFT)

Biscom's secure faxing is augmented by a product called Biscom Secure File Transfer (SFT), which enables organizations to securely send and receive sensitive files of all sizes and types. According to Biscom, SFT is a "Web-based secure file transfer solution that lets end users send large or confidential files easily, without IT intervention." Secure deliveries are created, managed, sent and tracked, including proof of receipt notifications back to the sender, and is often used to assist organizations that need to meet strict compliance standards. FAXCOM integrates SFT into its clients directly, so faxes have an additional layer of security using 256-bit AES encryption that is FIPS 140-2 certified. SFT supports any file type or size, including files over 100GB, and recipients simply need to have an email address to receive the files. Secure workspaces are also included for group collaboration, and granular reports help with visibility into the system for administrators.

As far as integration capabilities: in addition to Microsoft Outlook and SharePoint connectivity, Biscom SFT has a comprehensive RESTful API layer that supports Web services, .NET, Java, and SMTP, as well as scripting languages such as Ruby and Python. AutoPost and AutoFetch are two add-ons that help with automating processes of sending or receiving secure deliveries.

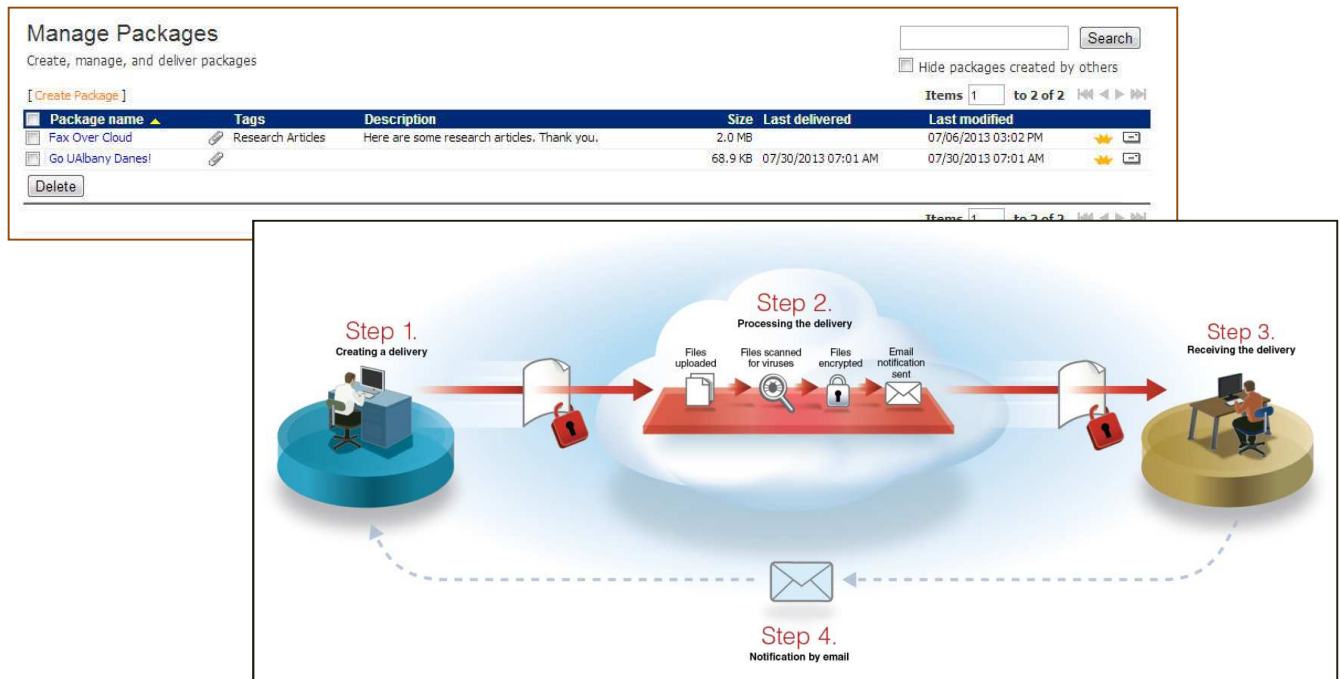


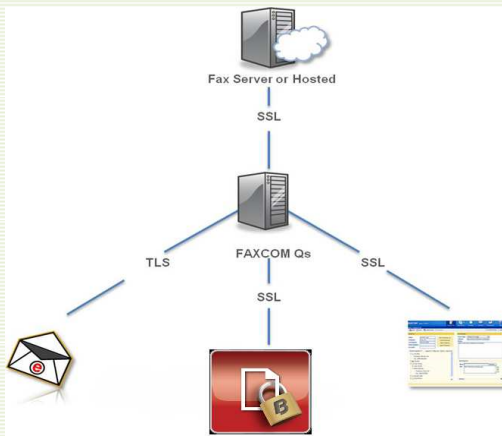
Figure 2: Biscom's Secure File Transfer. Above is the SFT inbox showing received packages that contain secure files. Below shows the overview of how SFT works.

Verosync Enterprise File Synchronization and Sharing (EFSS)

Biscom Verosync is described as an enterprise file synchronization and sharing solution (EFSS). It serves the needs of both IT professionals who wish to maintain control over data in their networks, and end users who need simple easy-to-use secure collaboration solutions. Data is under the full

How it works - security throughout the document life cycle:

- Faxes are received into a FAXCOM (on-premise) or FAXCOM Anywhere (cloud) server. Connections to the Queue use SSL.
- Faxes on the FAXCOM server may be configured to encrypt the data at rest until a FAXCOM Queue can pick up the fax, adding security.
- Once the FAXCOM Queue has the fax, it can send the image in a variety of ways:
 - Via email using SMTP over TLS.
 - Using the Biscom Secure File Transfer solution which also uses AES and SSL encryption.
 - Through a web client via an SSL connection.
- If using FAXCOM's Mailbox Server, all faxes are encrypted at rest in the server's data store.



control of IT with the ability to restrict users, devices, and IP addresses that can sync files. The product uses FIPS 140-2 certified 256-bit AES encryption and deploys a three-tier architecture which is hardened against common penetration and vulnerability attacks. EFSS supports LDAP/AD integration, policies, quotas and permissions. Verosync works seamlessly with the FAXCOM and FAXCOM Anywhere solutions.

Summary

Biscom's leadership position as the premier secure fax and document delivery solution provider is based on several factors: They have led the marketplace with product vision since their inception in 1986 and continue to be visionaries; their leadership is stable and the founders are still running the company today; and as demands for more secure document communication solutions have evolved, so have they. The FAXCOM solution from an architectural standpoint was designed as a true enterprise solution that offers security, redundancy and very high reliability. The FAXCOM solution incorporates multiple, interoperable components that gives end customers the ability to scale seamlessly and securely. Moreover, they have options for both on-premise and cloud-based solutions – or a hybrid thereof.

Yesterday's fax server is not necessarily today's secure fax solution and very few vendors can claim that they have been able effectively address the problem, especially in light of the evolving compliance directives that companies face today (HIPAA, PCI DSS, state and federal data privacy laws, etc.) Security is a way of life at Biscom, and is evident in their products: FAXCOM, FAXCOM Anywhere, Secure File Transfer and Verosync. Inside, it's the FAXCOM Queue that provides the "glue" that ties all of the products together in a secure, redundant and highly available scenario. No other independent software vendor can claim this level of secure capabilities from a single platform.

About Mark D. Malone

Mark D. Malone, a long time participant and contributor in the Fax and Electronic Document Delivery industry segments, created the Fax over Cloud industry web site. His overall experiences embody a 25+ year period of dedication in the software application industry, with the last 14 years specifically dedicated to computer-based fax solutions. During his career he has made contributions to many published works in journals of science, engineering, as well as numerous product articles, white papers and research reports. Learn more at www.FaxOverCloud.com.

About Biscom

Every day millions of users and thousands of enterprises rely on Biscom for secure and reliable document delivery solutions. Founded in 1986, Biscom pioneered the fax server marketplace with FAXCOM® and its award-winning fax management solutions. Since then, Biscom has developed expertise and solutions around secure file transfer, synchronization, file translation, cloud solutions, and mobile devices for the world's largest organizations. Learn more at www.biscom.com.