Axway Secure Collaboration

Unified "safe-for-work" solutions to protect your enterprise

Enterprises need unified controls over email, file sharing, and mobile device access in order to increase user productivity while managing data security risks.

Are your employees unintentionally putting your organization at risk by using unsecured file sharing tools?

Are they increasingly using their own mobile devices to access work-related email and files?

Can you afford to use email as a mission-critical communication channel without making sure it is protected from every possible angle?

Do you wish you had unified controls over email, file sharing, ECM content and mobile device access in order to increase user productivity while managing data security risks?

A recent survey* of 621 IT executives concluded that:

- 89% of organizations are unlikely to know if sensitive or confidential data was lost or stolen due to a data breach in the public cloud.
- 80% are concerned about the negative consequences of public cloud tools due the potential loss of intellectual property.
- 69% are not likely to know whether employees are using unapproved and risky file sharing tools.
- 66% rank file sharing a high or very high risk to their organization.
- Nearly 50% believe popular cloud-sharing services are not suitable for business use.

* "Achieving Security in Workplace File Sharing", Ponemon Institute, February, 2014

axway
business. in motion.

Axway Secure Collaboration solutions fully protect your enterprise — from sanitizing inbound email streams, to filtering and encrypting outbound messages, to securing and managing shared files, to making mobile data access safe for work. Microsoft SharePoint content is also protected and safe on the Secure Collaboration platform. Designed to be easy to use, easy to manage, and seamless to deploy within your existing architecture, Axway Secure Collaboration solutions are flexible and modular, enabling a "start anywhere" approach that can adapt to meet changing business demands. Axway provides IT management with the collaboration solutions they need to control, secure, and manage multiple user channels, and to empower employees with safe-for-work, enterprise-managed tools that let them do their job without putting the company at risk.

The increased adoption of public cloud tools raises serious questions about their enterprise-class security credentials. Today's employees rely on email, collaborative file sharing, and mobile device access to do their jobs; so IT must control and manage this data as it moves in and out of the organization in order to mitigate risk, meet regulatory and compliance mandates, and protect high value business information assets.

In order to fuel adoption of secure collaboration policies and keep workers productive, however, stringent security must be balanced with employee preference and usability concerns.

Securing the human element is critical to protecting your organization from:

- Network breaches and data losses that can expose confidential operational, employee or customer data, bringing the regulatory hammer down on your business.
- Accidental leaks of sensitive information that can occur when just one well-intentioned employee sends an unsecured message or shares a file with the wrong recipient.

The fallout from these kinds of email and file sharing security failures can be devastating in terms of lost data, business disruption, damage to brand, and litigation and regulatory fines. The only way to fully protect your business is to analyze and appropriately handle every message and file that enters or exits your network, every single time.

Secure and control collaborative file sharing

With an enterprise class alternative to public cloud file sharing services

Axway Secure Collaboration enables you to fully control file sharing, including ECM content such as SharePoint, which many collaboration solutions don't even address. Our Outlook Integration provides a familiar and popular user interface and experience, so users do not have to change the way they work. Axway eliminates the infrastructure, cost and security concerns that surround sharing large confidential files via unsecured means, such as email, FTP, public-cloud based file sharing services or physical media.

Prepare your organization to support the increasing adoption of BYOD (Bring Your Own Device) and empower employees to get their jobs done by accessing data via different devices, without the risk of having sensitive data being placed in a public cloud or shared in an uncontrolled fashion.

Secure email

Inbound and outbound, from start to finish

Email security is not a one-way street. While preventing potentially malicious messages and intruders from sneaking in is essential, it's also crucial to prevent proprietary enterprise data, intellectual property, and sensitive customer, client, patient, constituent, and partner information from leaking out.

Axway MailGate SC provides complete email protection that leaves no gaps in inbound defenses or outbound security. Combining network protection, policy-based content filtering, automated encryption, and file attachment management in a single solution, Axway can help your organization reduce administrative headaches, infrastructure costs, and the liabilities associated with unprotected and unmanaged email and file sharing communications.

You can easily and incrementally add these multiple layers of security to your email network — without making changes to your enterprise systems, applications, protocols, or end-user workflows.

And MailGate SC is the only solution of its kind that can decrypt and inspect any S/ MIME encrypted email sent and received by your organization to ensure it complies with the policies you have defined.

Protect data and improve governance

With outbound message security

Axway Secure Collaboration provides centralized data loss prevention (DLP) capabilities, including proactive content filtering, policy enforcement, and automatic gateway-to-gateway encryption, to protect against accidental data leakage, corporate policy infractions, unintentional blunders and regulatory violations. For example, you can:

- Define and manage security policies to enforce rules based on content, users, recipients and/or attachments. Apply a wide range of protective actions, from blocking to re-routing to encryption.
- Filter the content of all outbound messages and files to identify and prevent sensitive and regulated information from leaving your network. A simple user interface lets you choose filters to identify confidential information such as PIN, credit card, Social Security and CUSIP numbers.

Axway Secure Collaboration solutions help organizations comply with laws governing the security and privacy of information that is electronically stored, maintained, or transmitted. Examples include:

- U.S. state-specific encryption laws such as California's SB 1386 and Massachusetts' 201 CMR 17.00 (businesses may be subject to these laws even if they are not based in either state)
- Gramm-Leach-Bliley Act (GLBA) – U.S.
- Health Insurance Portability and Accountability Act (HIPAA) – U.S.
- Health Information Technology for Economic and Clinical Health (HITECH) Act – U.S.
- U.S. Patriot Act
- Sarbanes Oxley Act (SOX) – U.S.
- European Union Data Protection Directive (Directive 95/46/EC)
- Personal Data Protection Law – Japan
- Law on the Promotion of Utilization of Information and Communication Networks and the Protection of Data – South Korea
- Privacy Amendment (Private Sector) Act – Australia

axway
business. in motion.

Other comprehensive enterprise software solutions from Axway include:

- **Managed File Transfer (MFT)** for secure, auditable, and easy-to-manage B2B, Application-to-Application (A2A), and ad-hoc information exchange within existing infrastructures.
- **Business-to Business (B2B)** for automating and integrating supply or value chain activities — such as order processing, delivery, invoicing, and payments — that involve multiple business partners and customers.
- **Integration** for orchestrating end-to- end enterprise application integration and data exchanges, both within your organization and with your trading community of external partners, suppliers, and customers.
- **Identity Security** for real-time validation of digital certificates within PKI environments, ensuring the validity and integrity of highly valued and trusted transactions for security-intensive financial services, healthcare, and defense organizations.

Analyze, manage, protect and report on email traffic

With a powerful encryption platform

Axway Secure Collaboration includes a state-of-the-art SMTP relay and powerful policy-based content filtering capabilities that monitor all messages at the internet gateway. To improve governance and compliance, you can:

- Encrypt and authenticate inbound and outbound email streams based on centralized policies and automated message routing, whether the channel is gateway-to-gateway, gateway-to-desktop or web-based message delivery.
- Deploy secure email capabilities to any employee, customer, or partner with a browser and email client — without requiring them to install or learn new software.
- Automate and track message delivery all the way to recipient desktops to create a documented “paper trail” for email compliance and auditing purposes.

Boost employee productivity and reduce network risks

With robust inbound threat protection

Working in concert with your existing network security measures and email firewalls to protect against inbound threats, Axway MailGate SC can:

- Detect and eliminate viruses, worms, Trojan horses, spyware, and other forms of malicious — even criminal — activity that can cripple your network, bring everyday operations to a halt and potentially cost you millions of dollars. Axway Secure Collaboration stands guard at the Internet gateway, preventing potentially damaging messages and attachments from ever entering your network.
- Block unwanted email that’s not only annoying, but also creates legal liabilities, hurts productivity, and strains network and IT resources. Layered anti-spam filtering technologies effectively block more than 99 percent of all inbound spam, with virtually no false positives.
- Prevent unauthorized network access that poses a grave risk to valuable corporate assets, including sensitive customer and partner information, financial data, and intellectual capital. Intelligent Edge Defense capabilities effectively eliminate up to 90 percent of unwanted email traffic before it enters your network.

Your solution, your way

With a flexible architecture and deployment options

Every enterprise has unique communication needs. That's why the Axway Secure Collaboration platform is based on a flexible architecture that lets you select the specific levels of inbound and outbound protection you need now, while making it easy and straightforward to add new capabilities in the future.

This one-platform, one-box solution was designed with input from customers around the world and is available on premise, in a VM environment, hosted in the cloud, or a combination of all three. And Axway Secure Collaboration solutions give you the option of single or multiple administrators.

Delivery Options

Axway/Dell Appliance

Virtual VMware Appliance

Private Cloud

Mobile Clients

Android

iOS

Axway MailGate SC™ Secure Collaboration Platform

Secure file sharing anywhere	
DropZone™	Delivers enterprise-class secure file sharing and collaboration capabilities to familiar email interfaces and web-based clients, eliminating the problems associated with sharing large or confidential files using unsecured file sharing platforms. SharePoint Integration allows for SharePoint content to be mounted inside DropZone, enabling and applying DropZone security policies to SharePoint data. Empowers users to securely share files and interact with other internal and external collaborators from their desktop, tablet, or smart phone – all with enterprise-class policy controls, virus protection and encryption. Outlook Integration enables users to access their DropZone files via Outlook. DropZone Desktop Agent lets users synch local folders to DropZone folders.
Policy-based email content management & encryption	
Secure MailBox™	A comprehensive platform that inspects all email at the network gateway, identifies email content that is in violation of enterprise-defined security policies, and automatically redirects suspect messages to a secure, encrypted email channel for further action, such as deletion, quarantine, encrypted delivery, or end-user notification of policy violation.
Comprehensive email hygiene and network protection	
MailGate SC™	Reduce network congestion and enhance employee productivity with virus protection, anti-spam filtering, and defense against dark traffic.
Single, extensible platform	
Secure Collaboration gateway	An IPv6-enabled Secure Collaboration gateway appliance that provides multiple tiers of security and policy-based content management. Enterprise multi-tenancy allows for deployment within complex environments where multiple business units in a large enterprise, or multiple customers being supported by a single managed service provider, can be independently managed. A rich, RESTful API enables customers and solution providers to integrate the MailGate SC platform into enterprise portals, applications, and mobile device deployments.

Learn more today

To learn more about how Axway Secure Collaboration solutions can defend your organization against external and internal threats that jeopardize security and regulatory compliance, email us at collaboration@axway.com or visit us at www.axwaysecurity.com.

For more information, visit www.axway.com

axway
business. in motion.