DATA SHEET

CA Email Supervision

CA Email Supervision mitigates the risk of insider threats by controlling the flow and distribution of sensitive information within and outside the organization.

Benefits

With CA Email Supervision organizations realize the following benefits:

- Control of internally and externally destined email via client, Web and mobile email usage
- Precise control over email that also enables business processes through the usage of identity
- Cost effective packaged solution that delivers fast time-to-value and continual improvement over the life of the deployment

Overview

Even as corporate social media sites and collaboration applications proliferate, enterprise email continues to remain one of the most used communications in the workplace. High volume email communication puts organizations at significant risk of either accidentally or intentionally distributing sensitive information inside or outside the company. Forrester Research Inc. estimates that 43% of reported security breaches were committed by insiders (malicious or unintentional)[1]. CA Email Supervision reduces the risk of communicating sensitive information that could do harm to the company while enabling necessary communication flow to continue.

Controlling Insider Threats

CA Email Supervision protects the organization from insider threats through the control of sensitive information via one of the most used workplace communication modes, email.

Insider communication threats

Insider threats that expose the organization to brand and financial impact via email are often broken into three groups:

- Accidental communication threats
- Negligent communication threats
- Malicious communication threats

Accidental communication threats

The multi-tasking of executives and employees can often result in unintentional information distribution. Fat-fingering keys, entering the wrong email address or "replying to all" are common forms of accidental communication. The result is sensitive information getting intothe wrong hands directly impacting brand image or shareholder value.

Negligent communication threats

Employees often don't realize the full extent of their actions with shades of gray often blurring their making the right decision. It may occur over a gradual period of time or even be given a pass if the outcome is good. Ineffective data handling training and lack of visibility into realtime communication flow can lead to the inappropriate distribution of sensitive information. Not understanding the impact of sending colleagues protected executive conversations or the passive forwarding of sensitive information has a direct impact on the long-term profitability of the business.

Malicious communication threats

Even with the best hiring practices and training there will always be employees that will attempt to benefit at the expense of the company. Unethical behavior can be blatant but also can stem from gradual indiscretions. Forwarding competitive information to gain advantage in a new job or sending pre-released financial results to unauthorized internal employees that then forward to media outlets for negative exposure have a direct financial impact on the business.

How CA Technologies controls insider communication threats

CA Email Supervision protects and controls sensitive information from being distributed throughout the organization as a result of accidental, negligent and malicious communication. Intellectual property, financial information, ethical behavior and other sensitive information to the company that flows through email and puts an organization’s brand image or shareholders at risk are examples of what may be controlled.

The CA Email Supervision solution provides the ability to define flexible corporate policies to meet the demands of all organizational stakeholders including security, compliance, legal and finance. These policies intelligently control email through the accurate detection and classification of sensitive content and the monitoring of email communication flow. It also allows businesses to securely manage violations across large decentralized organizations and measure performance in real-time in order to drive improvement over the life of the deployment.

CA Email Supervision

CA Email Supervision protects sensitive information distributed via corporate email within and outside the organization. The following features of the solution can be configured to meet the needs of your organization’s specific business requirements.

CA Email Supervision Features

Supported email platforms	Supported endpoints	Content detection	Context (Identity)	Context (Identity)
▪ MS Exchange ▪ Lotus Domino ▪ MTA (SendMail/ Postfix)	▪ Smartphones ▪ Laptops ▪ Virtual desktops	▪ Pre and post send ▪ Subject line ▪ Body ▪ Attachment ▪ Encryption	▪ Senders ▪ Recipients ▪ BCC ▪ Role ▪ Geography ▪ IP ▪ Domain	▪ Flag ▪ Quarantine ▪ Warn ▪ Block ▪ Encrypt ▪ DRM

How CA Email Supervision works

As part of the solution, a lightweight agent is deployed within the email server that communicates with external policy servers enabling a scalable, fault-tolerant architecture designed for enterprise-volume systems that are mission-critical to the business.

Typically email control technologies are deployed at the network boundary missing the internal flow of email communications. But with the deployment of the agent at a central location it is able to control all email communications that attempt to pass through the corporate email server. This benefits the organization by providing direct visibility and control of email between all internal functional teams, part-time contractors/vendors and traffic flow to users of mobile devices. Without this central control point, sensitive traffic flow and communications would go unchecked and the business would be at risk.

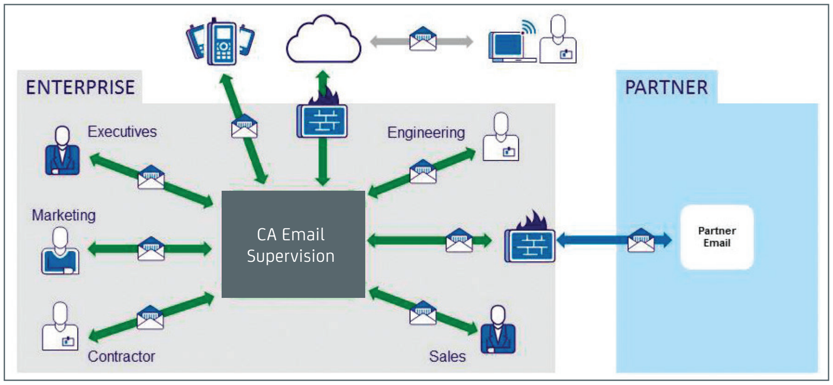
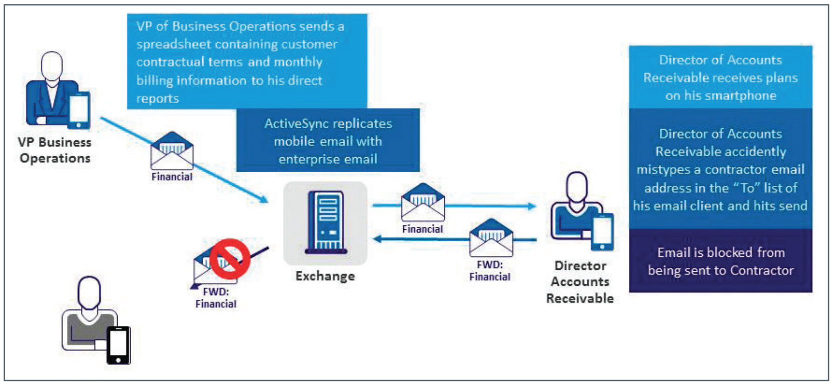


Figure A.

CA Email Supervision is deployed within the network and protects internal and external communications disseminated via client, Web and mobile usage.



VP of Business Operations sends a spreadsheet containing customer contractual terms and monthly billing information to his direct reports

ActiveSync replicates mobile email with enterprise email

Director of Accounts Receivable receives plans on his smartphone

Director of Accounts Receivable accidently mistypes a contractor email address in the "To" list of his email client and hits send

Email is blocked from being sent to Contractor

Figure B.

CA Email Supervision understands who the messge is being sent to internally and blocks it from being sent.

Use Case 1 – Accidental communication of intellectual property via mobile devices

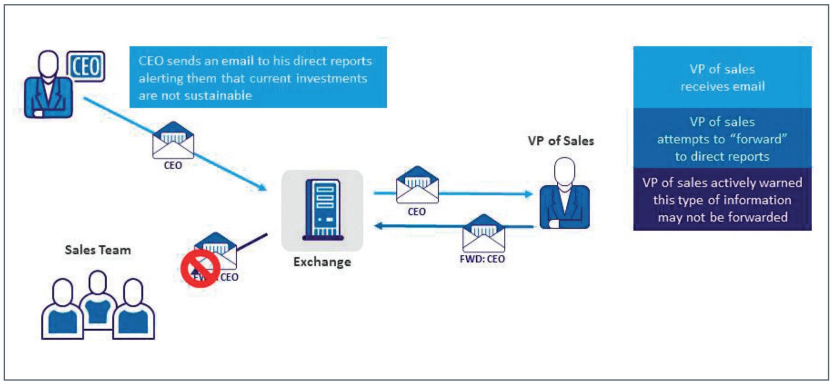
The following use case depicts a common form of "accidental" communication that results in CA Technologies protecting against sensitive data loss.

1. VP of Business Operations sends plans of a spreadsheet containing customer contractual terms and monthly billing information to his direct reports.
2. The Director of Accounts Receivable receives the information on his iPhone.

3. But the Director of Accounts Receivable mistakenly types in the wrong recipient within his email client and forwards the email to an internal contractor.
4. The CA Email Supervision solution identifies that the contact and the recipient together are outside of policy and blocks the email.

Figure C.

CA Email Supervision prevents email from being forwarded because it automatically triggers DRM.


CEO sends an email to his direct reports alerting them that current investments are not sustainable

VP of sales receives email

VP of sales attempts to "forward" to direct reports

VP of sales actively warned this type of information may not be forwarded

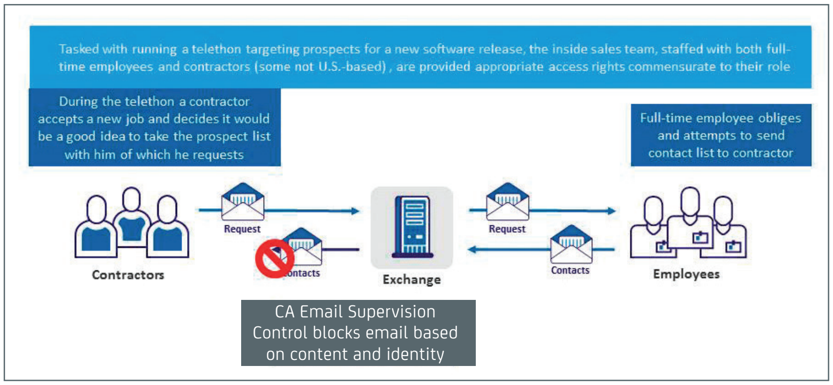
Use Case 2 – Negligent exposure of executive language

The following use case depicts a common form of "negligent" communication that results in CA Technologies protecting sensitive data loss.

1. CEO sends an email to his direct reports alerting them that their current organizational investments are "unaffordable".
2. VP of Sales receives the email and feels his entire team should see this information and then attempts to "forward" it to them.
3. The CA Email Supervision solution warns the VP of Sales that the content is inappropriate for distribution beyond him and prevents him from sending.

Figure D.

CA Email Supervision blocks email from reaching the contractor based on content and identity of the contractor.


Tasked with running a telethon targeting prospects for a new software release, the inside sales team, staffed with both full-time employees and contractors (some not U.S.-based), are provided appropriate access rights commensurate to their role

During the telethon a contractor accepts a new job and decides it would be a good idea to take the prospect list with him of which he requests

Full-time employee obliges and attempts to send contact list to contractor

CA Email Supervision Control blocks email based on content and identity

Use Case 3 – Malicious attempt to compromise customer contact information

The following use case depicts a common form of "malicious" communication that results in CA Technologies protecting sensitive data loss.

1. The inside sales team of an enterprise software company is tasked with running an email campaign targeting prospects for a recently released software product.
2. The team has a combination of full time employees and contractors of which some of the contractors are non US-based. The organization grants appropriate access to information between both roles. But all contractors are on corporate email.
3. Prior to the contract being terminated a contractor finds a new job at a competitor as a full-time employee.
4. During the middle of the campaign the contractor requests the prospect list (which he doesn't have access to) from a full time employee.
5. The full time employee obliges and then attempts to send the contractor the prospect list but it is blocked based on the content and the recipient being a contractor.

Mitigate the Risk of Insider Threats

Precisely control insider email threats at a lower operational cost

As data volumes grow and modes of communications evolve, email consistently remains at the top of the most used communication list. CA Email Supervision provides broad and precise control of email in order to mitigate the risk of sensitive information from being exposed through accidental, negligent or malicious email communications.

Broad email coverage

Controlling email from exiting the network is not the only vector that must be covered in order to adequately protect sensitive information. Partners, contractors and vendors often are not external to a network but sit directly on the enterprise email server. In addition, they often communicate on mobile devices while off the local network. In order to effectively protect the organization from the sensitive distribution of email, businesses must control email at the source. CA Email Supervision provides this protection through its agent-based technology controlling all email that flows through the email server. This mitigates risk to the business by centrally controlling all email destined internally and externally via client, Web and mobile usage.

Precise email control

The ability to precisely monitor and take action on the contextual relationship of employees, contractors and partners within an email is the difference between protection and control. Traditional data protection vendors broadly block communications with little visibility into identity ultimately trading off critical business flow for security. CA Technologies does not trade off one for the other but instead delivers both. By understanding the identity of the individuals involved in the communication flow CA Technologies is able to paint a richer picture of the event and in turn apply more precise controls to the higher risk elements of the communication. This enables the business to protect information from individuals that shouldn't have access while enabling information flow for those that should, allowing for a more fluid communication experience.

Fast and simple deployment

Alternative email control solutions require a control point at every potential threat vector. CA Technologies avoids this by controlling email at the source. Through the deployment of its lightweight agent directly on the centralized email server it's able to avoid the expensive and unnecessary deployment of controls throughout the network while reducing time-to-value.

The CA Technologies Advantage

Content aware Identity and Access Mangement from CA Technologies enables you to not only control user identities and access but information usage. Effective information protection and control is imperative not only to meeting both corporate compliance requirements and security polices but also to enabling critical business processes. With CA Email Control for the Enterprise organizations can control the highest risk insider threats to their organization while allowing critical communication flow to continue.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative security capabilities to the marketplace. We have a large and dedicated group of security experts who know how to make security deployments successful, and to help our customers achieve accelerated time-to-value.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.