NetSfere
Enabling Communication.

WINNER
FROST & SULLIVAN
2023 BEST PRACTICES AWARD
GLOBAL SECURE MESSAGING SOLUTIONS

Infinite Convergence

Taking Control:

How Secure Enterprise Messaging Puts Enterprise IT Back in Charge

Overview

Secure enterprise messaging has quickly taken its place as a primary channel of communication in large organizations. In industries such as finance and health care, secure messaging solutions are meeting a critical need that enables organizations to comply with strict security and regulatory requirements.

While many organizations focus heavily on security and compliance, they often overlook an equally vital aspect of messaging technology: robust administrative controls.

Administrative control mechanisms work in tandem with security and compliance features to provide a comprehensive messaging solution. By merging security, compliance and control (the pillars of advanced enterprise messaging), IT organizations are equipped to address an increasingly complex range of challenges and use scenarios.

Leading enterprise messaging solutions deliver increased administrative control on multiple levels. When combined with best practices, sophisticated administrative controls equip enterprises in finance, health care and other industries with a highly secure, highly reliable messaging platform.

The Need for Greater Control in Enterprise Communication

Communication drives growth in enterprise organizations. By implementing advanced communication technologies, large companies are improving business outcomes by encouraging collaboration and streamlining the flow of knowledge throughout the organization.

Over the past few years, mobile messaging has entered the mainstream of enterprise communications. Armed with personal smartphones and a BYOD approach to technology, the enterprise workforce is proving the effectiveness of mobile messaging as a primary channel for sharing information and data.

One of the reasons mobile messaging is so popular is that it performs better than traditional communication channels. Citing data from mobileSQUARED and SinglePoint, a 2015 State of Mobile Messaging study conducted by Infinite Convergence reported that 90 percent of all incoming SMS messages are read within three minutes. Similarly, mobile messages result in open rates above 99 percent, outperforming email and other communication channels.

The Hidden Threat of Third-Party Messaging Apps

Although the popularity and effectiveness of enterprise messaging are positive developments for growing companies, the news isn't entirely good. Unfortunately, many enterprises are unknowingly relying on unauthorized third-party messaging apps to transmit sensitive data.

A recent Infinite Convergence study showed that 66 percent of enterprise employees routinely use third-party messaging apps in the workplace. However, the use of non-authorized, third-party messaging applications is a serious concern for most (70%) enterprise executives.

The widespread use of unauthorized messaging solutions highlights the need for greater control in enterprise communications. Messaging has the potential to deliver significant benefits to the enterprise. However, the ad hoc use of consumer-grade messaging apps that lack adequate control mechanisms leaves organizations exposed and vulnerable to internal and external threats.

What Out of Control Messaging Means: Three Potential Worst Case Outcomes

No organization is immune from the impact of out of control messaging. Here are just a few possible outcomes due to a lack of proper administrative controls over enterprise messaging:

Employee-Controlled Messaging Infrastructure

One company that deployed NetSfere, Infinite Convergence's secure messaging platform, did so after an employee left the organization to join a competitor and the impact of not having messaging controls became very apparent. The departing senior sales executive was part of a WhatsApp group that the sales team used to exchange information about sales opportunities. Because WhatsApp was not under IT's control, the former employee could not be removed from the group and could continue monitoring the group's communications, including sensitive information about new sales prospects, pricing and upcoming product features.

Inability to Control the Sharing of Information outside of the Organization

The potential for users to share sensitive or proprietary files and information outside of the organization is a very real threat in many enterprises. To prevent the unauthorized disclosure of protected information and the possibility of data loss through messaging, IT administrators need to be able to control who users can share files and information with when they communicate with external parties.

No organization is immune from the impact of out of control messaging.

Lost or Stolen Devices

Imagine a scenario in which a smart phone owned by an employee is stolen. The employee has access to sensitive data and has an archive of intra-company messaging conversations on the phone that mention proprietary information. Without proper IT administrative controls in place, there is no way to erase the messages, which means the messages may fall into the wrong hands, at a significant cost to the organization and its stakeholders.

Control Is the Linchpin of Secure, Compliant Enterprise Messaging

Unauthorized messaging solutions clearly aren't appropriate for use in the enterprise. Across industries, there is widespread agreement that enterprise messaging solutions require robust capabilities in three key areas:

1. **Security**
   The protection of data and messages during and after transmission

2. **Compliance**
   Seamless compliance with regulatory requirements for healthcare, finance and other industries

3. **Administrative Controls**
   Total administrative control for IT and others tasked with managing the organization's messaging technology

When it's time to implement enterprise-grade messaging technology, many organizations (especially those in highly regulated industries like finance and healthcare) focus on security and compliance, while neglecting the importance of administrative controls.

Migrating away from the use of unauthorized messaging apps is a valuable first step in regaining control over enterprise communications, but it is simply not enough.

Security and compliance are compromised without robust administrative controls

To achieve information security, regulatory compliance and bottom line business improvement, IT teams need to be equipped with a slate of administrative controls for managing users, monitoring activity and enforcing corporate policies.

Migrating away from the use of unauthorized messaging apps is a valuable first step in regaining control over enterprise communications, but it is simply not enough.

Understanding the Risks: Scenarios That Demand Increased Administrative Controls in Enterprise Messaging

Enterprise workflows are complex. They require sophisticated communication technologies, including messaging platforms that give IT administrators the ability to effectively monitor and manage a constantly evolving list of user behaviors and preferences.

In fact, there are several common enterprise scenarios that underscore the need for IT teams to ensure security and compliance through improved administrative control:

1. Use of Personal Devices in the Workplace

BYOD policies have become commonplace as the lines between the workplace and employees' personal lives continues to blur. Nearly all (91%) enterprise employees communicate with colleagues, clients or partners outside of normal work hours and 28 percent engage in work-related communication every day of the week. But whether they are sending work messages at the office or at home, in most cases employees' devices of choice are personal mobile phones.

Managing messaging across personal devices is a serious challenge for IT administrators. Although BYOD presents opportunities for enterprises to substantially improve communication and collaboration without the cost of company-owned hardware, administrators have to be able to manage and control messaging activities – even when those activities occur on employee-owned devices.

2. High Employee Turnover Rates

In 2015, a CareerBuilder study found that one in five employees was interested in changing jobs in 2016, a 5 percent year-over-year increase from a similar survey conducted in 2014. Although employee turnover rates vary by industry, many enterprises are experiencing churn in their workforces, creating challenges for those who are responsible for managing communication and messaging technologies.

As a result, IT administrators need the ability to quickly activate and de-activate user accounts. Additionally, administrators must be able to mitigate the risks posed by sensitive

Nearly all (91%) enterprise employees communicate with colleagues, clients or partners outside of normal work hours.

data contained on the personal devices of employees who leave the organization.

3. Communication With External Stakeholders

In many industries, workflows require employees to use messaging as a primary channel of communication with external stakeholders. From professional services firms that communicate with clients to manufacturing and retail operations that share data with vendors, messaging provides a fast and convenient way for team members to connect with individuals outside of the organization.

Managing access for a constantly shifting user base creates opportunities for unauthorized account access, data breaches and other messaging disasters. To protect the integrity of data and sensitive information, IT administrators need control mechanisms that allow them to provide and manage temporary access for clients, vendors and other external stakeholders.

4. Regulatory Compliance in the Healthcare and Financial Industries

In certain industries, enterprise messaging is subject to strict regulatory requirements. Whether it's compliance with FINRA and Sarbanes-Oxley in finance or compliance with HIPAA and privacy regulations in healthcare, the regulatory burdens on today's enterprises call for a strategic and measured approach to compliance.

Anemic administrative controls jeopardize the organization's ability to meet its regulatory obligations. To reduce the risk of fines and penalties, decision makers need to know that IT administrators have control mechanisms in place to accurately monitor compliance at all times.

5. Internal Barriers to Adoption

Recent research by SAP showed that 78 percent of enterprise apps are abandoned after their first use, hampering the organization's efforts to introduce new technology for process enhancements and improved business outcomes.

Comprehensive IT control features increase adoption rates by providing real-time insights into usage and user behaviors. Armed with this information, administrators can more accurately target trouble spots and create strategies to overcome barriers to adoption.

Levels of Control

In the enterprise workplace, IT administrators require more than a basic set of administrative controls. To properly manage the organization's messaging platform and ensure the security of protected information, enterprise IT teams need multiple levels of control capabilities.

Platform-Level Controls

At the platform level, secure enterprise messaging solutions must provide robust control mechanisms that give IT teams the flexibility to adapt the technology to the needs of the organization and the industry. Most importantly, platform-level controls equip IT with the ability to manage and control the messaging activities of all users within the organization.

- **Customizable, role-based policy administration to control key features like message lifetime, sharing of attachments outside the enterprise and messaging encryption requirements**
- **Ability to deploy the messaging platform and configure message archiving settings in a manner that complies with regulatory requirements and corporate data retention policies**
- **Real-time tracking of KPIs like number of accounts, active sessions by user, messages transmitted and usage by device type**

Platform-level controls equip IT with the ability to manage and control the messaging activities of all users within the organization.

App-Level Controls

App-level controls empower IT teams to manage and monitor the internal and external users who access the messaging platform. These features enable IT administrators to provide an intuitive and convenient user experience, but protect the organization's security and compliance interests.

App-level controls empower IT teams to manage and monitor the internal and external users who access the messaging platform.

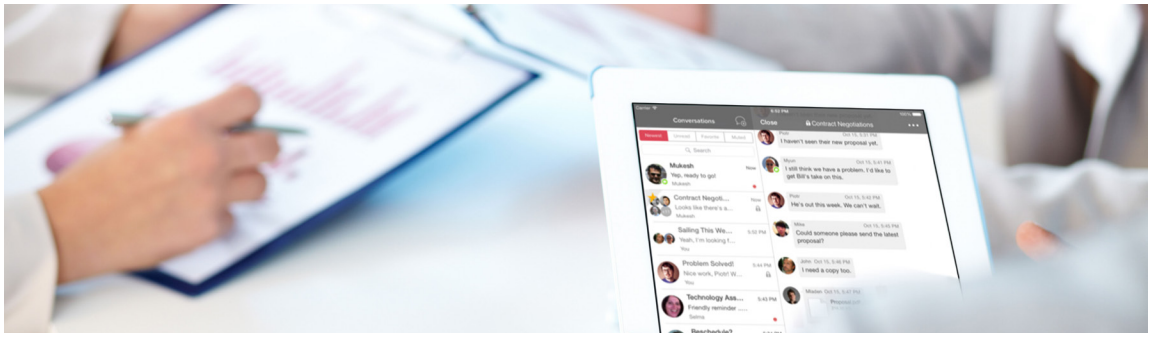
- **Management of accounts and data from a single, centralized repository**
- **Temporary guest access controls that facilitate communication with external stakeholders**
- **Total account management with remote wipe for sensitive data and the ability to quickly invalidate expired accounts**

Security-Based Controls

Security-based controls provide assurances that the enterprise messaging solution can accommodate the organization's strict security requirements. In addition to transport layer controls, security-based controls cover a full range of concerns.

- **256-bit encryption with elliptical curve key exchange to protect data and maintain the privacy of company communications**
- **Cloud-based deployment to give IT total control over security upgrades and requires zero effort from users**
- **IT in control of multi-device capabilities, allowing employees to securely access conversations and share multimedia content across permitted platforms and devices**

Best Practices for Regaining Control in Enterprise Messaging



Enterprise executives need to be proactive about improving the controls provided to IT teams and others who are responsible for managing the organization's enterprise messaging technology.

At Infinite Convergence, we have equipped the world's largest and fastest growing enterprises with NetSfere, the industry's most advanced enterprise messaging technology. Along the way, we have gained important insights about how organizations can give IT greater control over messaging and enterprise communications.

1. Understand your organization's messaging requirements.

Not all enterprises face the same risks. The first step toward leveraging controls for improved security and compliance is to accurately identify the capabilities system administrators need to effectively monitor and manage messaging activity. From a comprehensive slate of management and control capabilities to features that enable seamless compliance with regulations in finance, health care and other industries, NetSfere empowers IT administrators to align messaging technology with the organization's unique needs and requirements.

2. Implement a feature-rich secure enterprise messaging solution.

Our research shows that 92 percent of healthcare employees are willing to embrace a company-wide mobile messaging platform; in finance, the percentage rises to 94 percent. By prioritizing the implementation of a secure enterprise messaging solution with robust control features (such as NetSfere), organizations can simultaneously satisfy employees and equip IT teams with the tools to do their jobs even more effectively.

3. Document and update enterprise messaging policies.

As a best-in-class enterprise messaging solution, NetSfere includes control features that enforce corporate policies governing

messaging activities, data retention, message lifetimes and more. But the prerequisite for enforcement is the identification, evaluation and documentation of the organization's messaging policies. Organizations that regularly review and update enterprise messaging policies are positioned to achieve optimal results from their messaging technologies.

4. Monitor messaging activity.

Organizations that implement NetSfere take a big step forward in the push for more secure messaging and greater administrative control. But the implementation of secure enterprise messaging technology extends beyond a single event – it's an ongoing process that requires administrators to adapt systems and policies to the evolving needs of the organization. The IT mantra "Trust, but verify" is particularly relevant for enterprise messaging deployments. Supported by administrative controls that deliver real-time visibility to usage and other characteristics, IT teams should routinely monitor messaging activity to proactively respond to emerging threats and opportunities.

Organizations that regularly review and update enterprise messaging policies are positioned to achieve optimal results from their messaging technologies.

NetSfere
Enabling Communication.

WINNER
FROST & SULLIVAN
2023 BEST PRACTICES AWARD
GLOBAL SECURE MESSAGING SOLUTIONS

It's Time to Take Control of Your Messaging Technology.

At Infinite Convergence, we understand the importance of administrative control in secure enterprise messaging. Designed to meet the unique demands of organizations in finance, health care and other industries, our NetSfere enterprise messaging solutions integrate the world's most advanced administrative control features with best-in-class security and compliance capabilities.

To learn how NetSfere can benefit your organization, contact us today.

About Infinite Convergence and Netsfere

*Infinite Convergence Solutions, Inc. provides next-generation messaging and mobility solutions to carriers and enterprises around the world. The company's technology supports more than **500** million subscribers by sending nearly one trillion messages per year. Infinite Convergence Solutions is a subsidiary of Infinite Computer Solutions, with offices in the United States, Germany, India and Singapore.*

NetSfere is a secure enterprise messaging service created by Infinite Convergence Solutions. A best-in-class enterprise messaging solution, NetSfere equips large healthcare organizations with highly secure and reliable, cloud-based messaging technology, enabling them to meet performance, control and compliance requirements.