STEALTHMAIL

DATASHEET

Business Email Compromise (BEC) Protection

Introduction

Organizations are locked in arms race with hackers and cyber criminals.

Cybersecurity professionals have to combat not only existing threats, but find ways to predict and protect against the unknown. And among many channels to manage, email is usually the first line of defense to be under fire.

Statistically, in every 9/10 successful data breaches, email was the way for criminals to get past organization security and deliver malware or social engineering attacks.

Successfully protecting email communication significantly reduces the risks of data breaches, spilling of sensitive information, social engineering, and violating privacy regulations.

The problems with email are many. Two major ones are the dated transfer protocols and the exploitability of human error. StealthMail was developed to help organizations address both aspects of the email issue.

Key Benefits

- **Sender & Recipient validation**
- **Device fingerprinting**
- **Exclusive control over encryption keys**
- **Complete protection and control of email content**
- **Seamless integration with no operational burden**
- **Suspicious user behavior detection**
- **User account management**

Addressing the BEC Threat

According to the FBI's annual Internet Crime Report (IC3) for 2018, in the last 5 years alone, BEC has already caused over $12 billion in damages to businesses worldwide.

This statistic has been quoted by every major vendor and is a well-known fact.

Yet the majority of email security solutions can only partially address BEC threats, and that is by using an incoming email filter. It is admittedly better than nothing but still not effective enough.

StealthMail takes a different approach.

Using StealthMail allows organizations to create a communication environment within email where they can forget about BEC threats completely.

All emails sent using StealthMail are secure and fully BEC-proof.

Features and Benefits

Sender & Recipient Validation

- Exploits that enable CEO fraud, MITM, BEC, impersonation, and phishing type attacks are technically impossible to perform within StealthMail.
- Sender and recipient personas are always verified.

Device Fingerprinting

- Criminals cannot use unauthorized devices to access illegally acquired email accounts.
- Senders and recipients cannot be impersonated from another device, even if accounts have been compromised.
- Ensures employees cannot access sensitive business accounts from unsecure personal devices.

Stealth Email Network

- Enables an inner circle of secure communication within your email.
- BEC, EAC, spear phishing, and other impersonation-type attacks technically cannot exist within the Stealth Email Network.
- Close friends, business partners, and trusted contacts are always reliably verified within the Stealth Email Network.

End-to-End Encryption

- Data is always protected, whether on the device, in use, at rest, or in transit.
- No third party can access information sent using StealthMail.
- Data is never left in a vulnerable state open to attacks.

Email Recall

- Contain human error and potentially completely prevent breaches of data when email is sent to the wrong recipient.
- Organizations can manage information and revoke employee access to certain data that was previously sent to their email address.

Patented Stealth Technology

- Data cannot be read, accessed, intercepted, or altered by unauthorized parties at any point in the transfer.
- The data is transferred to the cloud and back over a proprietary patented protocol designed to address security vulnerabilities and exploits of legacy solutions.

Email Data Protection and Control

- All data is stored in the organization’s premises in its protected cloud.
- Data technically never leaves the secure company perimeter.
- Only your organization controls who sees its data.
- StealthMail has no access or backdoors to your data or keys.
- The organization has the means of retaining control over its data, even in the recipient’s inbox.

Features and Benefits

Exclusive Control Over Encryption Keys

- Organizations can deploy the encryption key server at its own facility.
- No third party or vendor can decrypt your data without your permission.
- In case CSP servers get compromised, criminals will have no means of getting to your information.

Legal Compliance

- Makes communication compliant with core regulations at the heart of HIPAA, GLBA, PCI DSS, SOX, and GDPR.
- Information is encrypted on the device, in transit, and in storage as well as transferred over encrypted channel.
- Unintentionally sent emails can be recalled to prevent breaches of data, even after the email has already landed in the recipient's inbox.

Integration & Compatibility

- Deployment does not interfere with existing IT infrastructure.
- Security Officers use their own Console and QRadar.
- StealthMail is deployed in the organization's Azure Cloud.
- StealthMail does not interfere with existing email security software.

Content Monitoring & Management

- Restrict the ability to reply, forward, copy & print the content of secure email.
- You always know who, when, and where has accessed a secure email.
- Restrict access to sent emails at any time, even if the email has been sent months ago.

Suspicious User Behavior Detection

- User activity is analyzed, and certain actions such as password guessing, are classified as suspicious activity.

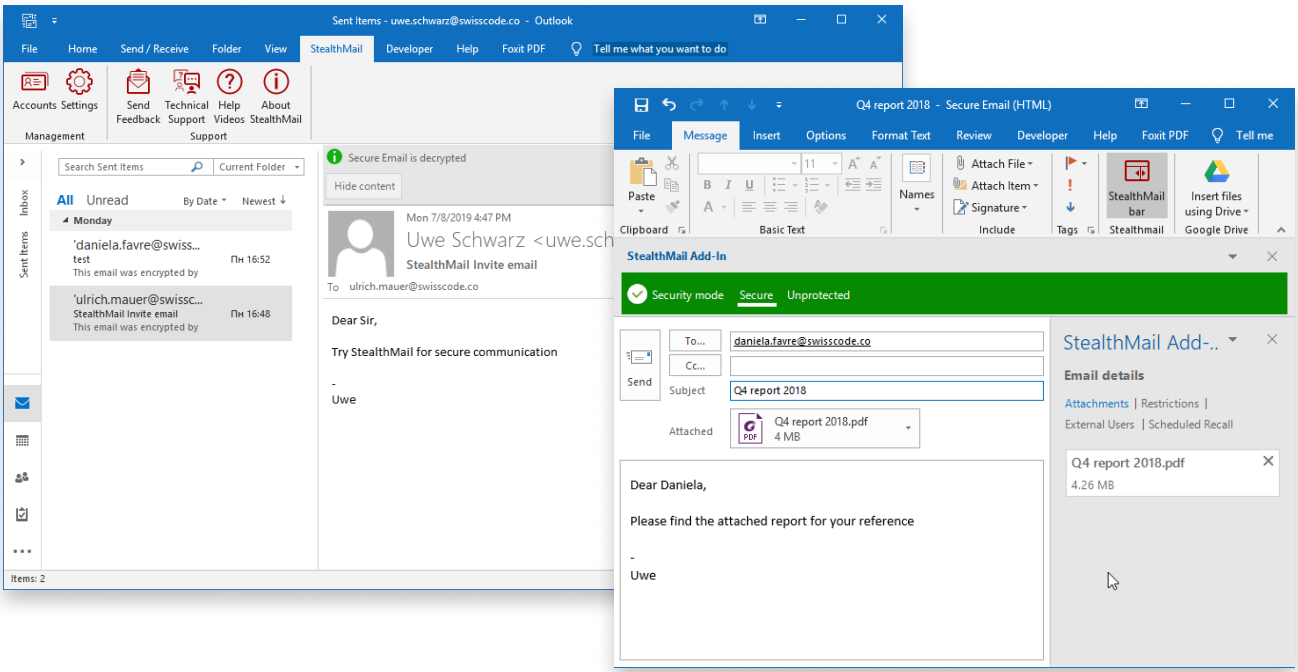
Distributed Server Architecture

- Real-time mail server backups to six separate locations to ensure encrypted data cannot be compromised.
- Even if a server gets compromised, your data cannot be accessed.

iOS, Android, and PC Compatibility

- Use mobile applications or Outlook Add-in to access secure emails.
- Secure communication is not limited to a single office machine.

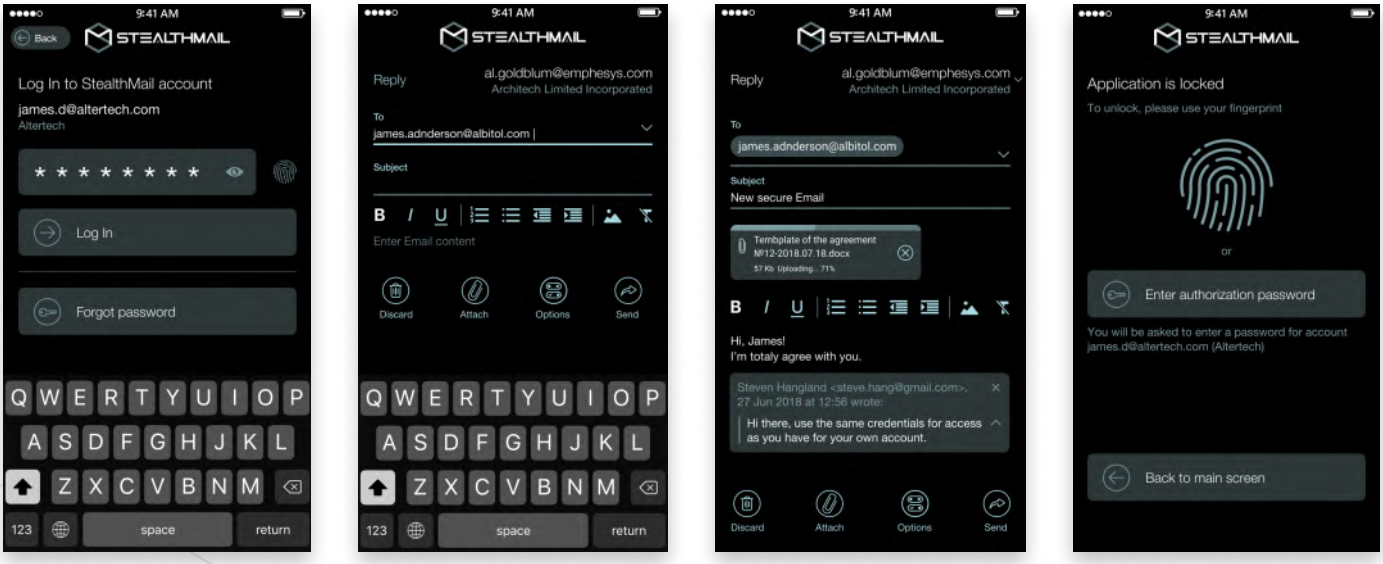
Intuitive User Interface



StealthMail seamlessly integrates with the Outlook interface, which ensures users will have an easier time building the habit of communicating securely. In addition, it significantly increases the chances of users actually using the solution instead of choosing less secure but more familiar means.

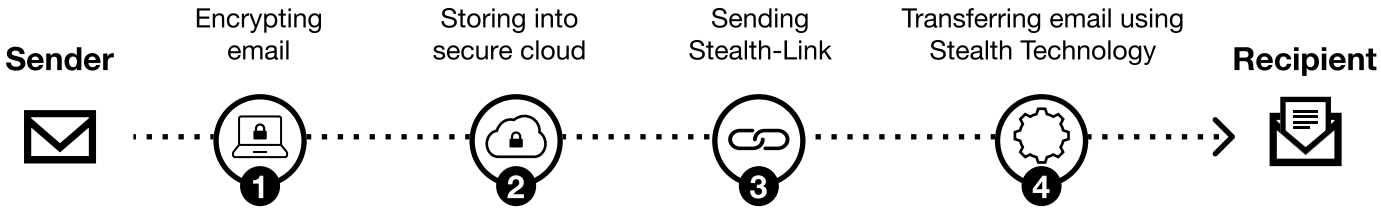
Dedicated Smartphone Application

Secure email communication is not limited to a single device that never leaves the office. StealthMail offers convenience without sacrificing security and can be used on iOS or Android devices to manage secure emails.



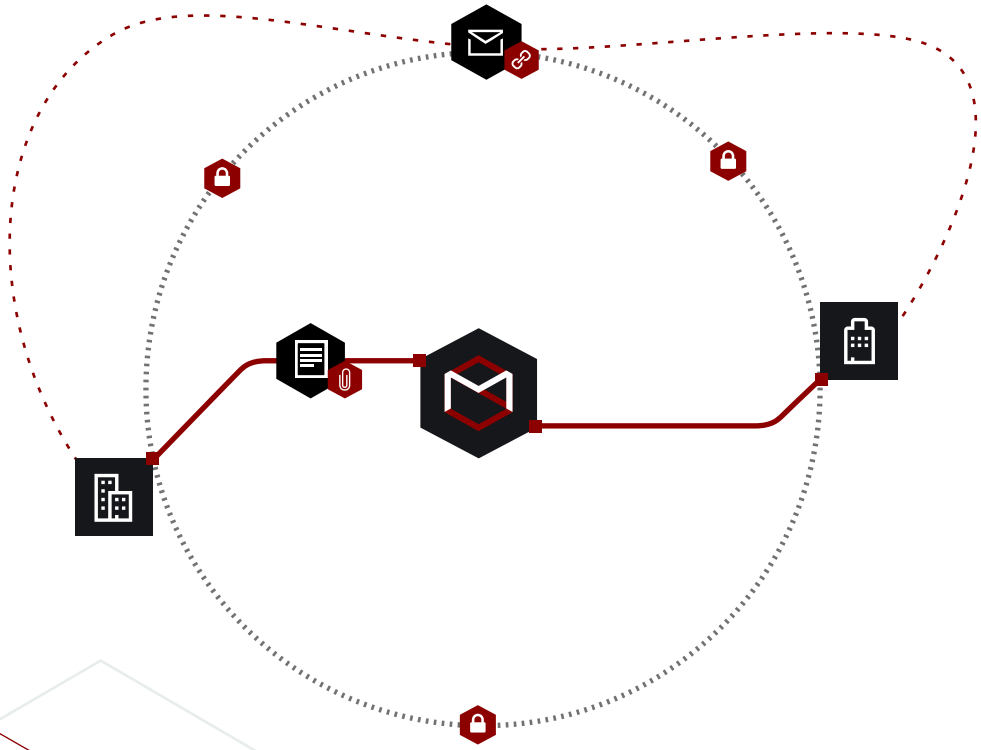
If you are ready for the next step, schedule free deployment call now [SCHEDULE]

StealthMail Solution



How StealthMail Works

1. Encryption is performed on the user's device and is never decrypted until it reaches the verified recipient.
2. Encrypted data is placed in the organization's cloud storage. Data is always encrypted when stored and transmitted. It is never exposed to SMTP or the public internet.
3. StealthMail uses email to send only Stealth-Links that do not contain any sensitive information.
4. After the recipient identity is verified, encrypted data is transmitted through secure channels using Stealth Technology.



StealthMail separates content and attachments from email and delivers it via Stealth-Channel

Encryption Specifications*

Encryption Keys
ECC 512+

Messaging
512-bit HMAC key

Data storage
AES 256 bit

Data transfer
Twofish 256 bit

Signing and authentication
RSA 8182 bit

Message signing, getting hash passwords
SHA-3 512 bit

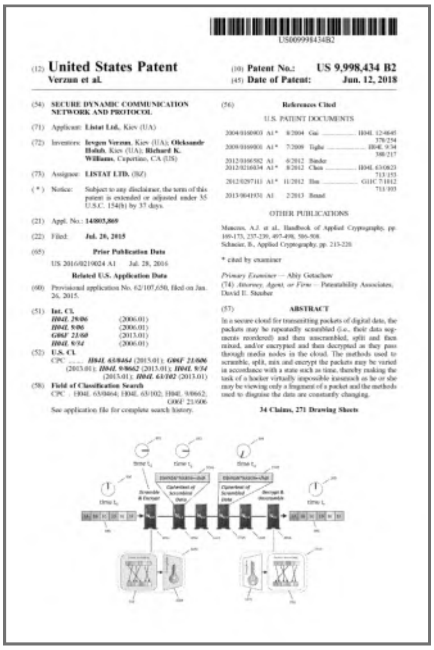
** Encryption specs can be downgraded to fit your computational power requirements.*

If you are ready for the next step, schedule free deployment call now SCHEDULE

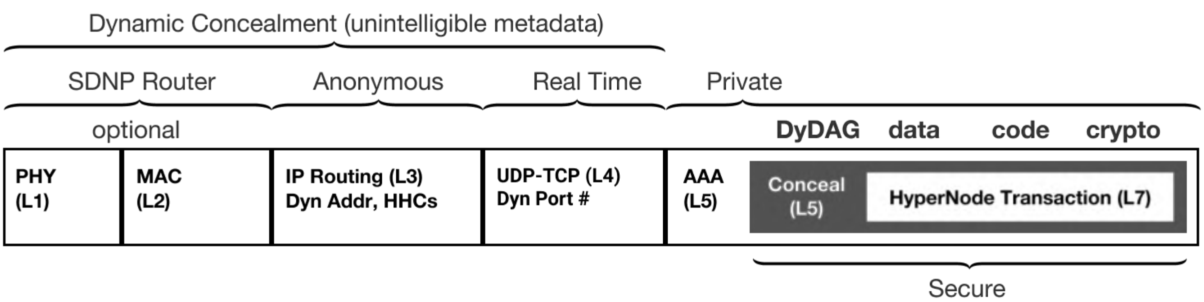
Patented Stealth Technology

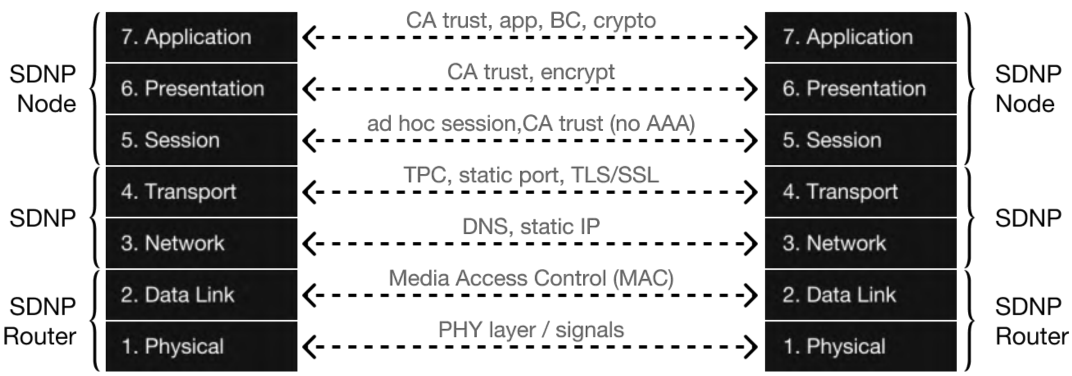
To ensure the security of email communication and protect organizations from email-based attacks, vulnerabilities of legacy protocols had to be addressed.

StealthMail uses a proprietary Stealth Technology to transfer data over Stealth-Channels that can withstand advanced threats and meet the highest security demands.


United States Patent
Verzun et al.
Patent No.: US 9,998,434 B2
Date of Patent: Jun. 12, 2018
SECURE DYNAMIC COMMUNICATION NETWORK AND PROTOCOL
ABSTRACT
34 Claims, 271 Drawing Sheets


US 9,998,434 B2
SECURE DYNAMIC COMMUNICATION NETWORK AND PROTOCOL
FIELD OF THE INVENTION
BACKGROUND OF THE INVENTION





If you are ready for the next step, schedule free deployment call now

SCHEDULE

Deployment

Deployment of the StealthMail service is a simple 3-step process that requires less than 1 hour to complete. Existing infrastructure is not affected.

To deploy and begin using StealthMail, the following components are required:

Domain

Active Directory

(Can be created during the deployment)

Azure subscription

(Can be created during the deployment)

StealthMail Deployment

The majority of StealthMail solution deployment is automated. VMs, databases, and services are all launched automatically within your active Azure subscription.

A few additional steps, which need to be performed manually take between 30 to 60 minutes which includes the time required for the operation to be performed.

1. **Prepare Azure** (~20 minutes)
   - Register StealthMail application in Azure Active Directory (~10 minutes)
   - Validate your main domain (~5 minutes)*

     **Depending on your domain registrar, it may take up to 72 hours for Azure to verify your domain.*
   - Add users to Azure Active Directory (~5 minutes)
2. **Register StealthMail account** (~10 minutes)**

   ***Depending on your domain registrar, it may take up to 72 hours for StealthMail to verify your domain.*
3. **Deploy StealthMail to Azure** (~10 minutes)

Application System Requirements

To ensure stable performance, StealthMail requires:

StealthMail for Windows	StealthMail for Android / iOS	StealthMail Outlook Add-In
Windows 7+	Android 5+ iOS 10+	Microsoft Outlook 2013+

If you are ready for the next step, schedule free deployment call now SCHEDULE

Corporate Awareness Training “The Art Of Email Security” for FREE

StealthMail solution covers the technological aspect of the email issues. To reduce the risk of human error even further StealthMail offers a comprehensive employee awareness course for free to its customers.

The updated set of course materials features the flagship book, The Art of Email Security, that was created in collaboration with cybersecurity experts from all around the world. The book includes insights from security specialists from HBO, Gartner, IBM, Deloitte, etc. and will save you time and effort in educating your employees.

Niels Trads Pedersen,
Partner at Deloitte, former Business Unit Leader at IBM

“No hard teaching, a good mix of engaging stories, fascinating case studies, memorable quotes, striking insights, and easy-to-follow recommendations for users.”

Tom Patterson,
Senior Information Assurance Manager at Cotton & Company LLP

“A great read for non-technical executives! Highly recommended.”

Stephanie Buscayret,
Chief Information Security Officer at LATÉCOÈRE Group

“Amazing job by the authors, I am really impressed! Read it while my family was sleeping, couldn’t do so myself after starting.”

Course materials include practical guides, which are characterized by the use of simple language to break down complex subjects. This allows employees to self-educate on the importance of email security, matters of cyber-hygiene, and answer a number security-related questions which they felt too uncomfortable to ask.

If you are ready for the next step, schedule free deployment call now

SCHEDULE

What To Do Next

Despite the considerable number of common cybersecurity threats organizations are facing, each organization has its own set of unique issues addressing which it chooses to prioritize.

To help you customize our solution to the needs of your organization and allow you to save time, we offer a free Deployment Call with our technical specialist.

You will be speaking with a technical specialist, who will talk you through the aspects of service deployment and configuration to tailor the service to your security needs. Once you are satisfied with the answers to all your questions, our specialist will guide you through the trial registration and help define the criteria of what can be considered a "successful" trial. This will allow you to save time and make sure that our solution is the right tool to help you meet your security goals.

Click the link to schedule your free Deployment Call today:

https://calendly.com/stealthmail

Server Infrastructure Cost

Number of users	**Price of Azure cloud** per month
50	$40
150	$70
1500	$200
5000	$245

About The Company

Team Expertise

14 years of professional telecommunication and cyber-security experience in mission-critical projects and emergency services in the United States, Europe, Middle East and Asia.

Microsoft One Commercial Partner

StealthMail earned Co-Sell Ready Status through the Microsoft One Commercial Partner (OCP) Program. The Co-Sell Program aligns Microsoft's large, global salesforce behind partners like StealthMail to drive top-notch solutions for customers.

To be eligible, businesses must submit customer references that demonstrate successful projects, meet a performance commitment, and pass technology and sales assessments, all of which StealthMail was able to demonstrate.

Microsoft

Try StealthMail for FREE

Step 1 ✓
Read StealthMail Datasheet

Step 2
SCHEDULE FREE DEPLOYMENT CALL

Step 3
Start FREE 30-Day Trial