

# 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.

### 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.

## **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

# **Features and Benefits**

Sender & Recipient Validation	<ul> <li>Exploits that enable CEO fraud, MITM, BEC, impersonation, and phishing type attacks are technically impossible to perform within StealthMail.</li> <li>Sender and recipient personas are always verified.</li> </ul>
Device Fingerprinting	<ul> <li>Criminals cannot use unauthorized devices to access illegally acquired email accounts.</li> <li>Senders and recipients cannot be impersonated from another device, and if accounts have been communicated.</li> </ul>
	<ul> <li>even if accounts have been compromised.</li> <li>Ensures employees cannot access sensitive business accounts from unsecure personal devices.</li> </ul>
Stealth Email	<ul> <li>Enables an inner circle of secure communication within your email.</li> </ul>
Network	<ul> <li>BEC, EAC, spear phishing, and other impersonation-type attacks technically cannot exist within the Stealth Email Network.</li> </ul>
	<ul> <li>Close friends, business partners, and trusted contacts are always reliably verified within the Stealth Email Network.</li> </ul>
End-to-End	<ul> <li>Data is always protected, whether on the device, in use, at rest, or in transit.</li> </ul>
Encryption	<ul> <li>No third party can access information sent using StealthMail.</li> </ul>
—	<ul> <li>Data is never left in a vulnerable state open to attacks.</li> </ul>
Email Recall	<ul> <li>Contain human error and potentially completely prevent breaches of data when email is sent to the wrong recipient.</li> </ul>
	<ul> <li>Organizations can manage information and revoke employee access to certain data that was previously sent to their email address.</li> </ul>
Patented Stealth Technology	<ul> <li>Data cannot be read, accessed, intercepted, or altered by unauthorized parties at any point in the transfer.</li> </ul>
	<ul> <li>The data is transferred to the cloud and back over a proprietary patented protocol designed to address security vulnerabilities and exploits of legacy solutions.</li> </ul>
Email Data	<ul> <li>All data is stored in the organization's premises in its protected cloud.</li> </ul>
Protection and	<ul> <li>Data technically never leaves the secure company perimeter.</li> </ul>
Control	<ul> <li>Only your organization controls who sees its data.</li> </ul>
	<ul> <li>StealthMail has no access or backdoors to your data or keys.</li> </ul>
	<ul> <li>The organization has the means of retaining control over its data, even in the recipient's inbox.</li> </ul>



# **Features and Benefits**

Exclusive Control Over Encryption	<ul> <li>Organizations can deploy the encryption key server at its own facility.</li> <li>No third party or vendor can decrypt your data without your permission.</li> </ul>
Keys	<ul> <li>No third party of vehicle can decrypt your data without your permission.</li> <li>In case CSP servers get compromised, criminals will have no means of getting to your information.</li> </ul>
Legal Compliance	<ul> <li>Makes communication compliant with core regulations at the heart of HIPAA, GLBA, PCI DSS, SOX, and GDPR.</li> <li>Information is encrypted on the device, in transit, and in storage as well as transferred over encrypted channel.</li> </ul>
	<ul> <li>Unintentionally sent emails can be recalled to prevent breaches of data, even after the email has already landed in the recipient's inbox.</li> </ul>
Integration & Compatibility	<ul> <li>Deployment does not interfere with existing IT infrastructure.</li> <li>Security Officers use their own Console and QRadar.</li> <li>StealthMail is deployed in the organization's Azure Cloud.</li> <li>StealthMail does not interfere with existing email security software.</li> </ul>
Content Monitoring & Management	<ul> <li>Restrict the ability to reply, forward, copy &amp; print the content of secure email.</li> <li>You always know who, when, and where has accessed a secure email.</li> <li>Restrict access to sent emails at any time, even if the email has been sent months ago.</li> </ul>
Suspicious User Behavior Detection	<ul> <li>User activity is analyzed, and certain actions such as password guessing, are classified as suspicious activity.</li> </ul>
Distributed Server Architecture	<ul> <li>Real-time mail server backups to six separate locations to ensure encrypted data cannot be compromised.</li> <li>Even if a server gets compromised, your data cannot be accessed.</li> </ul>
iOS, Android, and PC Compatibility	<ul> <li>Use mobile applications or Outlook Add-in to access secure emails.</li> <li>Secure communication is not limited to a single office machine.</li> </ul>

# **Intuitive User Interface**

문 구 File Home Send / Receive Folder View St	Sent Items - uwe.schwarz@swisscode.co - Outlook tealthMail Developer Help Foxit PDF Q Ti	ell me what you want to do	
Accounts Settings     Send Technical Help About Feedback       Accounts Settings     Send Technical Help About Feedback       Send Technical Help About Feedback     Support Videos Stealt/Mail       Management     Support Videos Stealt/Mail       Search Sent Items     Current Folder       * Monday     'daniel Aavre@swiss       * Monday     This email was encrypted by       'Ulrich.Maule@swissc       StattMail Imter@swissc       StattMail Imter@swissc       'Ulrich.Maule@swissc       This email was encrypted by       This email was encrypted by       Imter@swissc       This email was encrypted by       This email was encrypted by       Imter@swissc       This email was encrypted by       Imter@swissc       This email was encrypted by       This email was encrypted by	Secure Email is decrypted     Hide content     Mon 7/8/2019 4:47 PM     Uwe Schwarz < uwe.sc     StathMail nvite email     To ulrich.mauer@swisscode.co     Dear Sir,     Try StealthMail for secure communication     .     Uwe	Image: State of the state	

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.

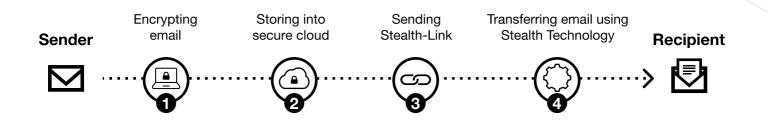
## **Dedicated Smartphone Application**

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.

•••••         9:41 AM           Back         STEALTHMAIL			
Log In to StealthMail account james.d@attertech.com Altertech	Reply al.goldblum@emphesys.com Architech Limited Incorporated To james.adnderson@albitol.com	Reply al.goldblum@emphesys.com , Architech Limited Incorporated	Application is locked To unlock, please use your lingerprint
****** •	sutpect B / U \ 注 注 理 理   ▲ %	james.adnderson@albitol.com Subject New secure Email	
→ Log In	Enter Email content	Tembplate of the agreement M122018.07.18.docx ⊗ 57 Kb tydrawfrag71%     B / U   := := := := := :	or Enter authorization password
Every Forgot password	Decard Attach Options Send	Hi, Jamesl I'm totaly agree with you. Steven Hangland «steve hang@gmail.com», ×	You will be asked to enter a password for account james.d@altertech.com (Altertech)
Q W E R T Y U I O P A S D F G H J K L	Q W E R T Y U I O P A S D F G H J K L	27 Jun 2018 at 12:56 wrote: Hi there, use the same credentials for access as you have for your own account.	
◆         Z         X         C         V         B         N         M         ⊗           123         ⊕         space         return	★         Z         X         C         V         B         N         M         ≪           123         ⊕         space         return	Image: Constant         Image: Con	(←) Back to main screen

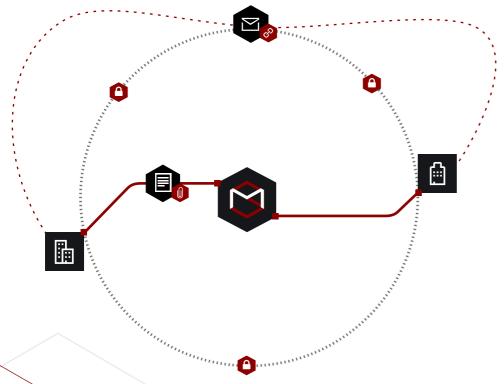


# StealthMail Solution



### 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.



# **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.

12)	United States Patent Verzun et al.	(10) Patent No.: US 9,998,434 B2 (45) Date of Patent: Jun. 12, 2018	
(54)	SECURE DYNAMIC COMMUNICATION NETWORK AND PROTOCOL	(26) References Cited	
-	Applicant: Listat Ltd., Kiev (UA)	U.S. PATIENT DOCUMENTS	
(72)	Investors: Jeogen Verzun, Kiev (UA); Oleksande Holub, Kiev (UA); Biehard K.	2004/0169900 A1* #2004 Gai104L.124645 2008/0169000 A1* 72009 Tighe106E.924 380/17	
	Williams, Capertine, CA (US)	2012/0166582 A1 0/2012 Binder 2012/0216034 A1* 8/2012 Chen	
(7))	The second second second second	2022029703 AL* 10202 Bm 000 713/253	
(*)	Notice: Subject to any disclaimer, the term of this patient is extended or adjusted under M U.S.C. 154(h) by 37 days.	2013/964H31 AI 22013 Beam	
	Appl. No.: 14800,869	OTHER PUBLICATIONS	
(22)		Mancros, A.J. et al., Handbook of Applied Cryptography, pp. 195-173, 235-229, 495-498, 586-508.Schaoler, B., Applied Cryptography, pp. 213-228.	
(65)	Prior Publication Data US 2016/0219024 A1 Jul. 28, 2006	* cited by examiner	
	US 2016/0210024 Al Jul. 28, 2006 Related U.S. Application Data	Primary Economy - Abig Gotachew	
(60)			
(51)	Int. Cl.	(57) ABSTRACT	
(52)	NML 2496         (2006.01)           NML 596         (2006.01)           GMJ 2466         (2015.01)           NML 974         (2006.01)           U.S. CL         (2006.01)           (2003.01)         NML 974           (2003.01)         (2006.01)           U.S. CL         (2003.01)           (2003.01)         NML 69462 (2015.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2005.01)           (2003.01)         (2003.01)	in accordance with a state such as time, thereby ranking t	
(58)		may be viewing only a frequent of a packet and the methods used to discusse the data are constantly character.	
	See application file for complete search history.	34 Claims, 271 Drawing Shorts	

US 9.9	98	434 B2
1		
SECURE DYNAMIC COMMUNICATION NETWORK AND PROTOCOL		"Hackers Made Seart emails," <i>BGR</i> (www. "Nest Google Privacy
FIELD OF THE INVENTION		Hocked," Slave Geor "Account Hijackings C
This invention relates to communication networks includ- ing methods and appartitis designed to optimize perfor- mance and quality of service, instandata integrity, maximize system optime and network stability, and maintain privacy and security.		tion. Line, the free- rocked by a secent sy app has seen hundred by parties other than <i>Review</i> : 2 Jul 2014 "Ordinary Americans"
BACKOROUND OF THE INVENTION		Report Claims," AP - "Senart LED Light Be
Improving means of communication have fields the programs of civilization from manking? a mritest beginnings. From the use of oundeex and nearsengers traveling by first or foreshock; through mail possal delivery by train, track and implance to the solvent of the telegram and telegraph, tele-	19	News 8 Jul. 2014 "Sin People Chargad Ov Stabilish was targete words and credit card of takets for pop-en New York authorities
phone, radio, television, companers, the cell phone; the Interact, enail and World Wide Web; and more recently, through social media, voice-over-latenet, machine-to-ena-	21	"Internet Of Things" Vi Shores," Journation mes.com) 4 Aug. 201
chine (M2M) connectivity, the Internet of Things (IoT), and the Internet of Ilverything (IoT), communication has always		"Rossian Hackers Ann words", New Juri 70
led the way in exploiting the newest technologies of the day. With each new generation of telecommunications technol- ogy employed, the number of people connected and the rate by which information is transferred among them has also increased.	20	"New Leaker Disclosin chades," CNN 6 Aug. "Hackers Root Google" The Enquirer (www.) "Dairy Onega Hacked 1
The officer of this trend is that humanity is more connected than at any time in history, with peeple transing and relying on communication technology to safely and reliably deliver their private, personal, humly, and fluencial information to	*	Christian Science Me "Celebrity Victims in Lo nembility in Kloud / "Home Depot May be
only those to which they intend to contact. Knowledge and information can now be distributed in seconds to millions of people, and friends and family can contact one another half	10	Breach Home Dep Targat (40M cards its 2014
way around the world as ensembly as pushing a button. It is often unid, "the world has become a very small place." While such progress is treasandously beneficial to every- one, there are also requirive ensemptions of our heavy		"Mysterious Fake Cellp All Over The US," B "Back Attack: From B fare?" Takso Finance
refinere on technology. It is not supprising that when the communication system fails to perform, e.g. during an earthquake or severe worther, people become disoriented or own panicked by their being "umplugged", own if only		"Home Depot Confirm And Canadian Stores "Yuloo Waged Coart Surveillance," CRSA
temporarily. The quality of service, or QoS, of a communi- cation system or media is then a critical measurement of a communication network's performance. Peoples' pence-of-	40	"Year Medical Record i Credit Card," Rester "Red Alert: HTTPS H
mind, ficancial assuts, identity, and even their very lives roly on dependable and secure communication. Another key consideration of a communication network is		against SSL/TLS (H) worst hacks [sic] bee nections handreds of
its ability to insure privacy, safety, and security to the client using it. As communication technology has evolved, so too hus the sophistication of criminals and "hackers" intending		day," Joh Blodd, 26 9 "Sony Cyberntlack, Fin Finestorm," New Kerl
to inflict mischief, disrupt systems, steal money, and acci- dentally or multicionely here, others. Credit cord front, stolen passwords, identity theft, and the transformed pub- ficiency of confidential information, private pictures, files,	55	In what appears to be security broaches, ident bega the question, "how and what can be done to
month, test messages, and private tweets (either sticlet, to enable, test messages, and private tweets (either sticlet, to enthursas or blackmall victims) are but a few examples of modure syber-crists.		society socks greater pr want greater connectivit cation, and more conver-
Notable examples of privacy violations and cyberonine at the time of this parent application are listed below to		octions. To understand the p
highlight the epidemic proportion of the security problem in today's open communication networks (arranged clavato- logically):	40	abilities in modern com and connected devices, how today's electronic.
"Taget: Stolen Information Involved at Least 70 million Provide " CNRC 10 Jan. 2014		operates, transports, and text, and/o, and video in

2 Thickers Mude Senset Fridge and TV Send Mit emails," NGP (www.hgr.com) 20 Jan. 2014 "Next Geogle Privace Researces as The Hacked," Scient Geore (www.dashgem.com) 24 An "Account Highships, Cell Land: Thats Security into the Line, the free cell and rearrough up, the test is not hearthy of an ext account cheath or ore has no methody of an ext account cheath or ore has no methody of an ext account cheath or

The send matrices of the recorder designed particles of the send matrices of the recorder designed particles between 2 14d 2014 and 2014 and 2014 and 2014 and 2014 behaves Americans Couple up in NSA Data Sweep, Report Chines, "A 5 4d, 2014 beam 12D Light Bells Leak Wi-Ei Passweeps," ABC: Nove 3 3 dd, 2014 beams for Ab Ab 2014 beams for Private Telefans. Subdisk was imposed by hackers who used wirken parvorts, and excite and annihous the bay and will freesands.

which exclusions using "Alconduce, 22 Inf. 2014. net Of Thing," Volumetheric Direct (Indexing, Study ens." *Journational Burliness Theory* (www.idicompl. A.ug. 2014) in Hackers Annus Own a Billion Internet Pasdr, Nev Eoil Fourder 5 Aug. 2014. Lenker Diselesing U.S. Secrets, Government Conlor, "CNO 6 Aug. 2014 area Root Google's Next Thermostic In 15 seconds," *Tophysics* (Work Next). 2014.

Virdand Science Meeting 29, Aug. 2004 http://within.in.ide/.cf.fbade/biston-Sciencity/Vidability in Cloud Accounty, "CBS News, 1 Sep. 2014 and an Dipate May to the Latowic Tanget of Crafta Card and ... Home Depth breach world be rando larger ham with the Cardination word Swedowic/ Fordware, 2 Sep. 14 Web Cardin station word Swedowic/ Fordware, 2 Sep. 14 Web Cardin station word Swedowic/ Fordware, 2 Sep. 14 Web Cardin Santon Web Swedowicz, 2 Sep. 2014. Discussion Science Science S Sep. 2014.

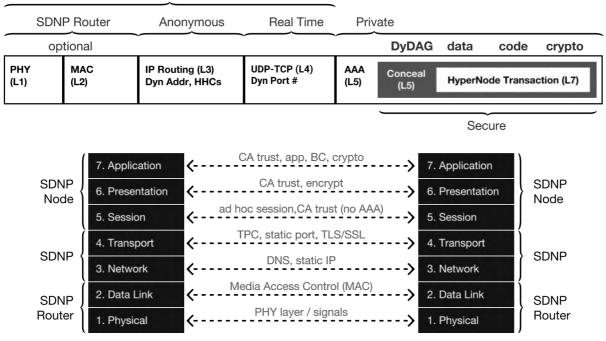
etc?" likes Finance 3 Spp. 2014 end Days Conference Payson Hacked In U.S. ad Canadian Stores," Fars Neur 9 Sep. 2014 zoo Wagad Coard Fight with U.S. Government Over arcellance," CIRS(#? 11 Sep. 2014 Medical Records 16 Worth Nove to Hocken than Your relif Conf." *Rooters* 24 Sep. 2014 J. Adre: IUTIPS Has Boon. Hocked. Reveser exploit 1 Martin Filter Has Boon. Hocked.

paint networks in the output attack twit rate, annuag me out hacks food sectors it companies however outerform hacks food or millions of paople rely on every age / hadibudd, 200 Sap. 2014 or Qibentack, First A Nisionne, Swith Gene Iano a intentrum. *New New Thrue*, 50 Dec, 2014 what papeans to be an occulating poce of cybererine, or hyberotype haching heritor, and privary insoines, it

and what can be done to stop theor?" At the same then that soviety socks gender privacy and security, constraints also want greater connectivity, cheaper higher-quality contentracation, and more conversionce in conducting financial transactions.

This is modern commutation networks, this storage, d consected devices, it is first important to understand w isday's electronic, radio, and optical communication emits, transport, and stores data including files, omail, it, and/so, and video images.

#### Dynamic Concealment (unintelligible metadata)



# 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:





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)
- 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+	Microsoft Outlook 2013+
	iOS 10+	



# **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

<sup>66</sup> 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

<sup>44</sup> 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.



# 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.



## Try StealthMail for FREE

Step 1 Read StealthMail Datasheet Step 2

SCHEDULE FREE DEPLOYMENT CALL Step 3
 Start FREE 30-Day Trial