



SECURING COMMUNICATIONS

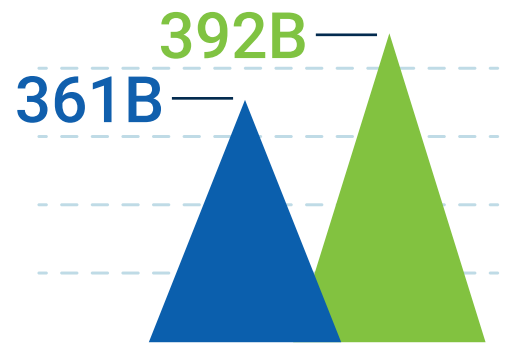
| From Phishing Defense to Automated Protection

Content

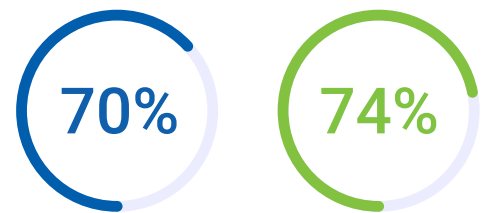
- 3 Introduction
- 4 Understanding Digital Certificates and Signatures
- 7 Email Security Threats
- 10 Introduction to S/MIME: Securing Email
- 12 Automating Secure Communication
- 14 How GlobalSign and NoSpamProxy Can Help
- 16 Best Practices for Secure Communication
- 16 Conclusion

Introduction

In today's digital landscape, email security is paramount. According to Statistica.com, approximately 361 billion emails are sent daily and received globally, with this number expected to rise to 392 billion by 2026. Given email's critical role in business communication, it is a prime target for cybercriminals. As of April 2024, gov.uk reports that 70% of medium-sized companies and 74% of large companies have experienced a cybersecurity breach in the past 12 months. 84% of these breaches were phishing attacks. This eBook provides insight into the evolving challenges in email security and delves into how automation can streamline and enhance protective measures, especially considering these alarming statistics.



Email sent daily and expected to rise by 2026



medium sized company

large company

Experienced a cypersecurity breach in the past 12 months

By exploring the partnership between GlobalSign and NoSpamProxy, we will demonstrate how our combined solutions provide a robust defense framework against email-based threats. Digital certificates and encryption play pivotal roles in this defense strategy, ensuring the authenticity, integrity, and confidentiality of email communications. Automation further strengthens security measures by simplifying the management of digital certificates, automating the implementation of security protocols like S/MIME, and reducing the risk of human error. We will further explore how automation streamlines these processes and contributes to a more resilient email defense strategy throughout this eBook.

Understanding Digital Certificates and Signatures

Understanding digital certificates and signatures is crucial as they form the foundation of secure email communications in an increasingly vulnerable digital landscape

Digital Certificates

Digital certificates are electronic credentials that verify identities. They are essential to establish trust in digital communications. This need for verification extends to AI applications, where digital certificates confirm the identities of trusted algorithms and users, reinforcing the integrity and reliability of automated decision-making processes.

- **Definition and Purpose**

Digital certificates verify the identities of individuals, devices, or services. They are issued by trusted entities known as Certificate Authorities (CAs).

- **Public Key Infrastructure (PKI)**

PKI manages digital keys and certificates, forming the backbone of secure communications. PKI creates, distributes, and verifies public and private keys, ensuring that the entities involved in the communication are authentic and trustworthy.

- **Types of Certificates**

Various types of certificates exist, including Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates for securing websites, client certificates for authenticating users, and code signing certificates for securing software/applications.



Understanding Digital Certificates and Signatures continued

Certificate Authorities (CAs), such as GlobalSign, are trusted entities that issue these certificates. They play a critical role in the certificate lifecycle by providing solutions for effective certificate management and ensuring that the entities they certify are legitimate.

Digital certificates are a key component for digital security, making it crucial for organizations to manage them properly. This management includes issuing, renewing, and revoking certificates. As a primary defense against evolving threats, including those leveraging AI, effective certificate lifecycle management is vital for maintaining secure communications.



Digital Signatures

A digital signature is an electronic signature that is backed by a digital certificate, providing proof of an identity. While digital signatures are widely used for document signing, they are also crucial in email security, ensuring the authenticity and integrity of emails. By using certificates to verify the identities of senders, digital signatures make it significantly harder for malicious actors to impersonate legitimate users or tamper with email content. Consequently, understanding the benefits of implementing digital signatures is essential for organizations aiming to enhance their security measures.

Benefits of implementing digital signatures in email security:



Enhanced Security

Digital signatures verify the sender's identity and ensure that emails remain unchanged during transmission. This helps protect against tampering and ensures the integrity of the message.



Improved Trust

They build trust between communication parties by authenticating the sender, thereby reducing the risk of phishing attacks and other email-based threats.



Cost Efficiency

By reducing the risk of fraud and data breaches, digital signatures can lower the potential costs associated with security incidents, legal disputes, and compliance violations.

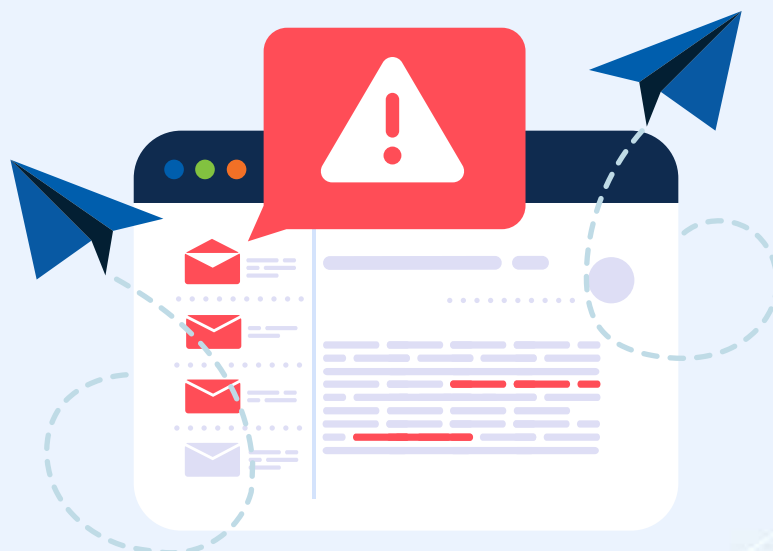


Email Security Threats

To understand how you can keep your email communications safe, it is essential to first know the kinds of threats that your business may face:

The most common types of email phishing attacks are:

- **Email Bombing**
Inboxes get flooded with an onslaught of emails, often as a smokescreen for genuine attacks, such as unauthorized financial transactions.
- **Business Email Compromise (BEC)**
Senior executives or financial departments are targeted with the aim to extract sensitive data.
- **Spear Phishing**
Attackers pose as trusted sources, using familiarity to persuade recipients into sharing confidential details.
- **General Phishing Emails**
Perpetrators lure users into clicking on malicious links or downloading harmful attachments through deceptive means.



Email Security Threats continued

AI in Cybersecurity

As cyber threats grow more complex, the role of AI in cybersecurity is expanding rapidly, offering both new defensive capabilities and presenting new risks. In this section, we will discuss key terminology and explore how AI is transforming the landscape of email security. Understanding these concepts is crucial for the effective protection against evolving threats.

Basic Terminology

AI (Artificial Intelligence):

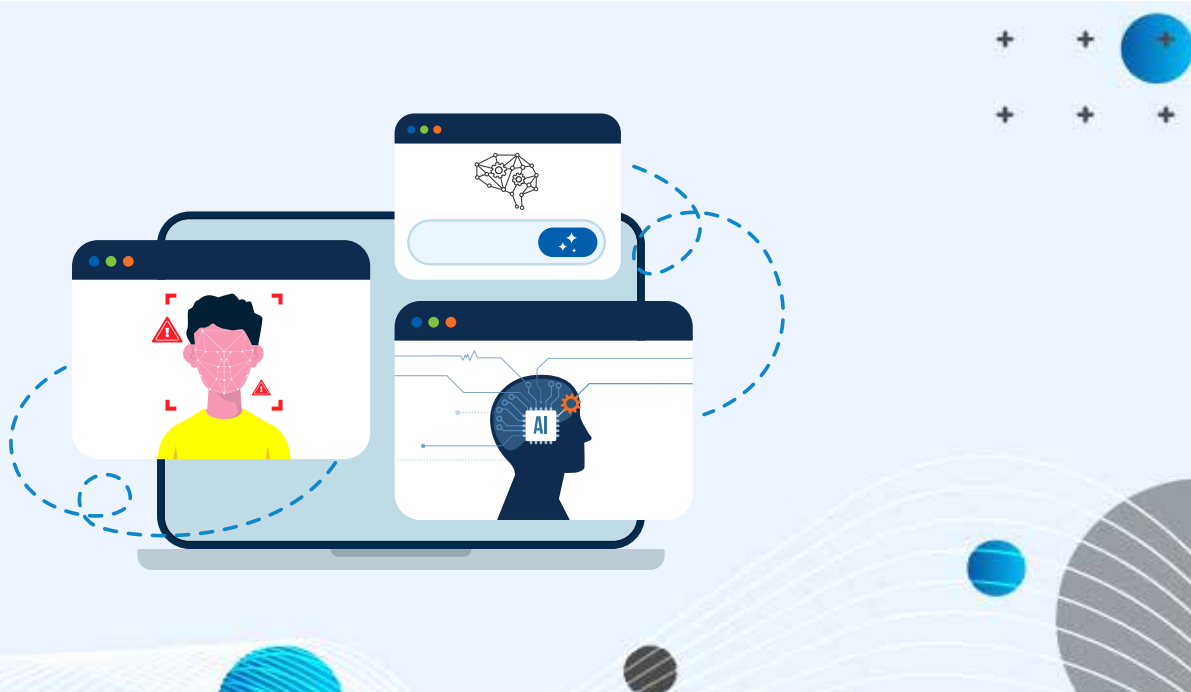
- Refers to computer systems capable of performing tasks that typically require human intelligence.
- Includes learning from data, reasoning, problem-solving, perception, and language understanding.
- Utilizes algorithms and data to make decisions and predictions.

Deep Fake:

- Uses artificial intelligence to create or manipulate audio, video, or images.
- Can generate highly realistic fake content that is difficult to distinguish from real media.

GPT (Generative Pre-trained Transformer):

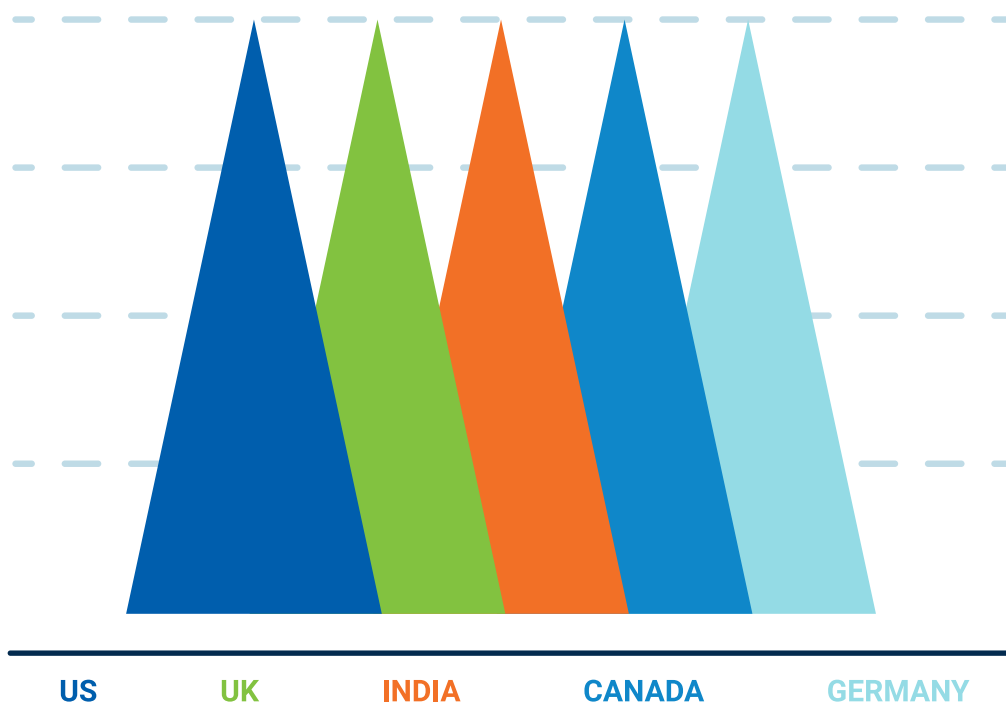
- Large language models developed by OpenAI.
- Uses deep learning to generate human-like text based on input.
- Trained on large datasets to understand and produce coherent text.



Email Security Threats continued

Due to the increasing popularity of Artificial Intelligence and Deep Fake technologies, cyber-attacks are rapidly becoming more sophisticated and harder to detect. Attackers are turning to AI to enhance social engineering tactics, resulting in a significant 60% increase in AI-driven phishing attacks, as highlighted by Zscaler research. The US, UK, India, Canada, and Germany topped the list of countries targeted by phishing scams, particularly impacting the finance and insurance sector, which saw a staggering 393% year-over-year rise in attacks.

393% Rise in Phishing Attacks year-over-year



While AI enhances defenses by detecting fraudulent emails, analyzing phishing attempts, and bolstering threat detection capabilities, it also introduces new risks. Attackers leverage AI to automate and optimize attacks, creating convincing phishing emails and manipulating digital content with unprecedented realism. According to the IBM X-Force Threat Intelligence Index 2024 report, AI and GPT were mentioned in over 800,000 posts on illicit markets and dark web forums in 2023, highlighting cybercriminals' growing interest in these technologies. This dual nature of AI underscores the urgent need for robust cybersecurity measures that can adapt to evolving threats. One effective approach to mitigating these risks is the implementation of S/MIME (Secure/Multipurpose Internet Mail Extensions) to secure email communications.

Introduction to S/MIME

Securing Email

S/MIME, or Secure/Multipurpose Internet Mail Extensions, are crucial for sending digitally signed and encrypted messages. They enhance email security by ensuring the authenticity, integrity, and confidentiality of email communications.

- **Digital Signatures**

S/MIME uses digital signatures to verify the sender and ensure the message has not been altered. This provides assurance that the email is genuinely from the stated sender.

- **Encryption**

Encryption converts information into code to prevent unauthorized access using public and private keys. This ensures that only intended recipients can read the information. S/MIME also encrypts the email content, protecting it from unauthorized access. Only the intended recipient can decrypt and read the email.



Introduction to S/MIME continued

Setting up S/MIME involves several steps:



Generating Keys

The first step is to create a pair of public and private keys. The public key is shared with others, while the private key is kept secure.



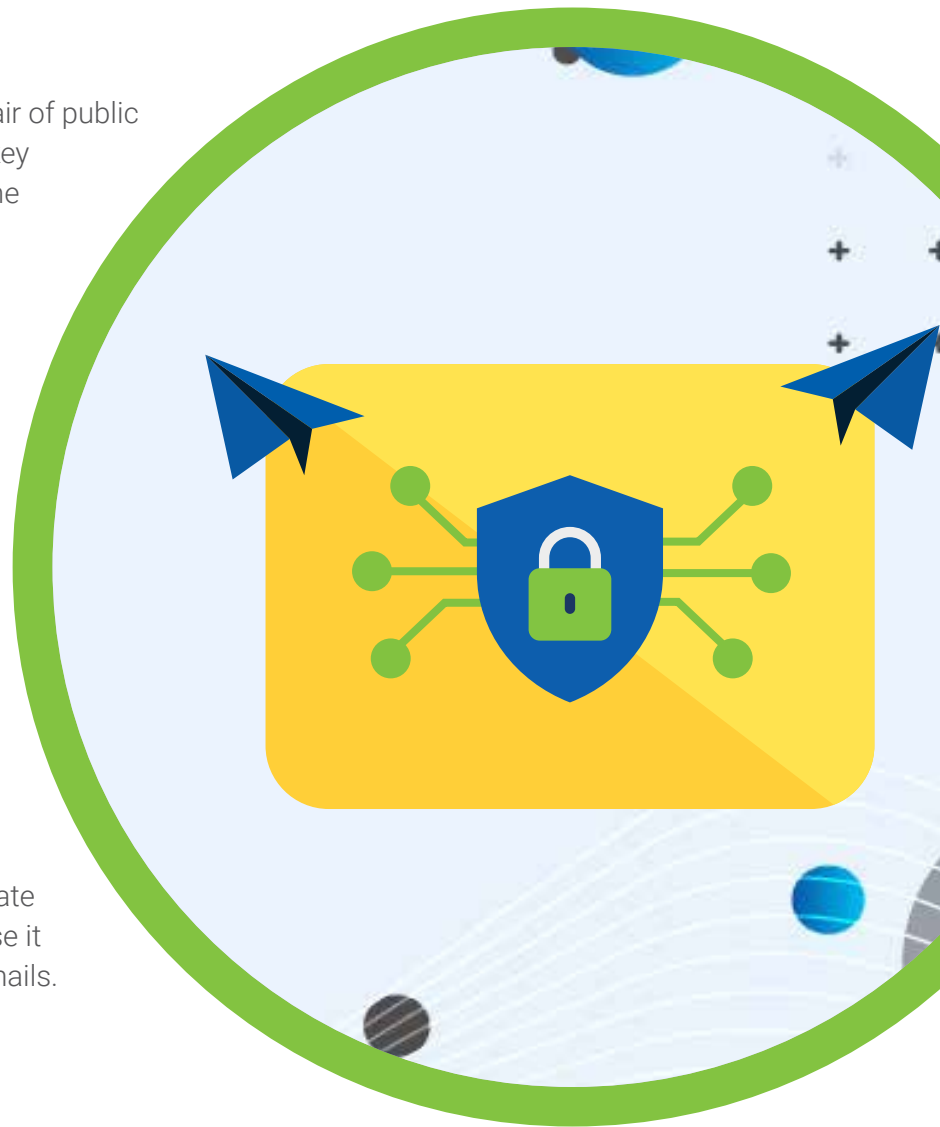
Requesting a Digital Certificate

A publicly trusted S/MIME certificate is obtained from a CA. The certificate links the public key to the identity of the certificate holder.



Configuring Email Clients

Email clients must be configured to use S/MIME. This typically involves installing the S/MIME certificate and setting up the client to use it for signing and encrypting emails.



Benefits of implementing S/MIME:



Authenticity

Verifies the sender's identity, ensuring that the email is from a legitimate source.



Integrity

Ensures the email content has not been altered during transit.



Confidentiality

Protects sensitive information by making it accessible only to the intended recipient.



Administration

Streamlines security and administration processes without requiring extensive user training or IT resources.

Automating Secure Communication

Automation is key to efficiently managing certificates, especially in large-scale environments. It reduces manual effort, enhances security, and ensures compliance. In the context of secure email, automating the implementation of S/MIME certificates is essential. By automating the provisioning and renewal of S/MIME certificates, organizations can ensure that all email communications remain encrypted and authenticated without the risk of expired or misconfigured certificates. Despite the increasing significance of automation, some organizations remain cautious about the potential challenges it may introduce.

Overcoming Challenges with Automation: Why We Offer Automated Solutions

Automated solutions offered by trusted companies, such as GlobalSign and NoSpamProxy, are designed to turn potential challenges into opportunities:

Administrative Concerns

Challenge: Frequent root certificate updates can be a hassle.

Solution: Our automated workflows manage updates effortlessly, reducing administrative tasks and ensuring timely updates. Costs and Overheads.

Costs and Overheads

Challenge: Automation can seem costly, especially for smaller businesses.

Solution: Our solutions lower operational costs by minimizing manual effort, making automation affordable and efficient for businesses of all sizes.

Technical Limitations and Compatibility Issues

Challenge: Technical limitations and compatibility issues can be daunting.

Solution: Automation improves system integration, streamlining processes and reducing technical barriers, ensuring smooth compatibility.

Lack of Knowledge

Challenge: Implementing automation can be complex without the right expertise.

Solution: We offer expert support and knowledge, automating processes so that organizations can seamlessly implement and maintain automated systems without the need for additional resources.

Security Concerns

Challenge: Ensuring governance and control of automated systems can be challenging.

Solution: Our automated systems enhance security by minimizing human error and providing robust monitoring and alert mechanisms, ensuring proper certificate management.

Automating Secure Communication continued

Benefits of Automated Solutions:

Furthermore, through the utilization of automated certification workflows, organizations can unlock several more benefits:



Enhanced Efficiency

By reducing manual effort, automated systems enable faster and more accurate certificate deployment, renewal, and revocation processes. This efficiency translates into significant time savings and improved operational agility.



Improved Security

Automated systems minimize the risk of human error associated with certificate management. They ensure timely issuance, renewal, and revocation, supported by robust monitoring and alert mechanisms that proactively detect and mitigate potential vulnerabilities.



Scalability and Consistency

Organizations can effortlessly manage large-scale PKI deployments with automated solutions. This capability ensures consistency in certificate configurations, eliminating inconsistencies that could compromise security.



Regulatory Compliance

Automated systems streamline compliance with industry regulations and standards. They facilitate consistent monitoring, auditing, and management of certificates, reducing the likelihood of non-compliance penalties.



How GlobalSign and NoSpamProxy Can Help

Keeping on top of ever-changing validity periods and the management of certificate lifecycles can be challenging for companies as it is time-consuming and costly. By partnering with GlobalSign and NoSpamProxy, organizations can implement a secure, automated, and scalable email security solution, safeguarding their communications against the evolving landscape of cyber threats whilst saving time and resources.

GlobalSign and NoSpamProxy offer comprehensive solutions that integrate seamlessly to provide end-to-end email security. Our combined approach ensures robust protection against phishing, spam, and other email-based threats, while automating certificate management to enhance efficiency and compliance. Moreover, our decade-long partnership provides an extra layer of trust and stability.

- **NoSpamProxy**

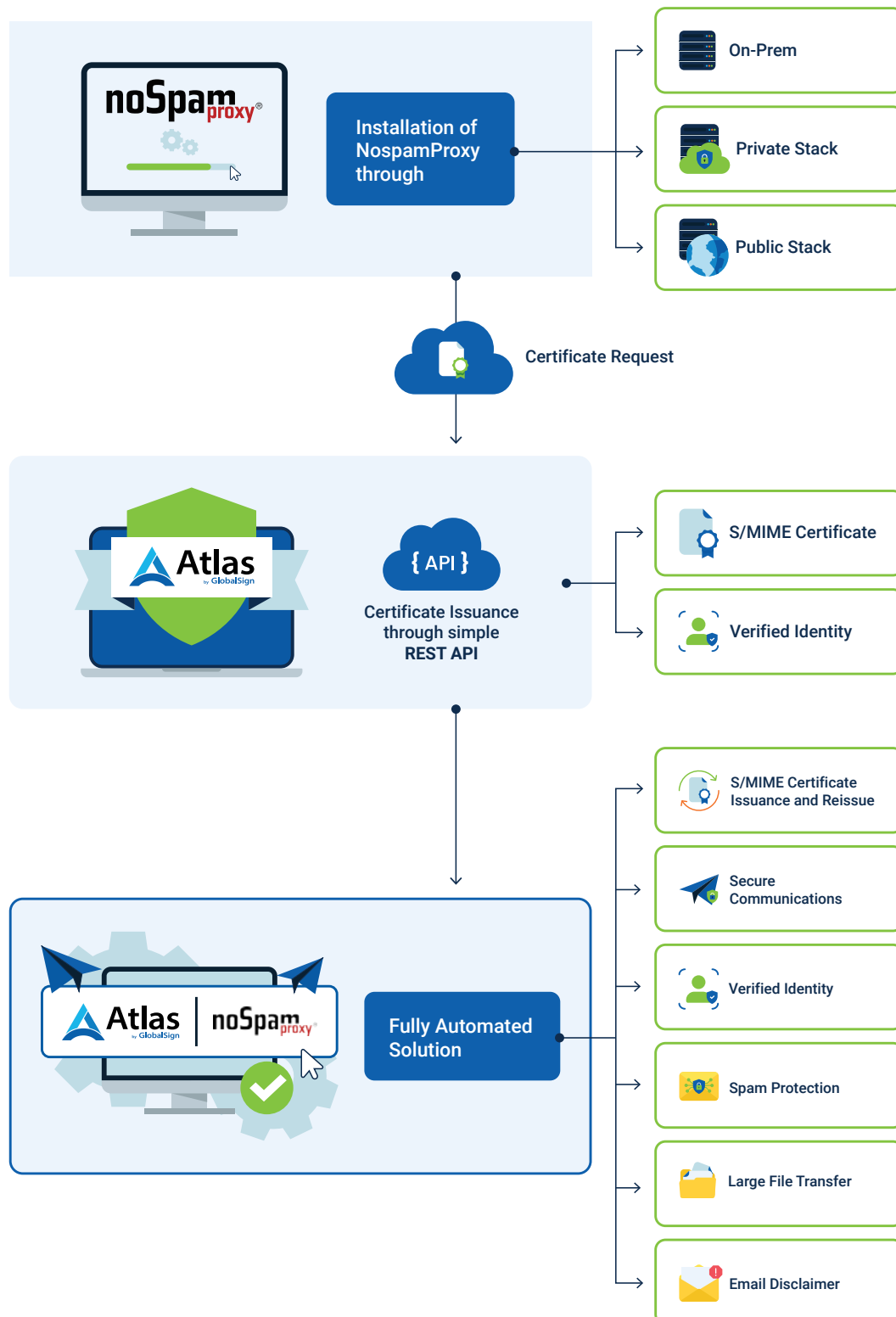
Specializes in email security, providing comprehensive protection against spam, phishing, and other email-borne threats. By leveraging advanced algorithms and machine learning, NoSpamProxy ensures that only legitimate emails reach your inbox, significantly reducing the risk of cyberattacks originating from email communication.

- **GlobalSign**

As a leading provider of digital certificates and identity services, we offer solutions that enable secure email communication through encryption and digital signatures. This ensures that the integrity and confidentiality of your messages are maintained, protecting sensitive information from unauthorized access.



Integration of NoSpamProxy and GlobalSign's combined solution



Best Practices for Secure Communication

To further enhance your company's communication security, you should consider the following best practices:

- **Educate Employees**

Conduct regular training sessions to educate employees about the importance of secure communication practices, recognizing phishing attempts, and responsibly handling sensitive information.

- **Regular Certificate Renewals**

Ensure that certificates, such as S/MIME certificates, are regularly renewed to maintain their validity and effectiveness in securing communications.

- **Keep Software and Tools Up-to-date**

Regularly update software and tools to protect against vulnerabilities.

- **Implement Encryption**

Utilize encryption for all sensitive communications to safeguard data during transit, preventing unauthorized access and maintaining confidentiality.

- **Automate Monitoring and Alert Systems**

Implement automated systems to continuously monitor communication channels. These systems can detect potential vulnerabilities, unauthorized access attempts, or anomalies in real-time. Automated alerts ensure swift response and adherence to security policies. unauthorized access and maintaining confidentiality.

By adopting these best practices, your organization can significantly strengthen its defenses against cyber threats and ensure the secure transmission of sensitive information.

Conclusion

In conclusion, as the digital landscape continues to evolve, enhanced by machine learning, the importance of secure communication cannot be overstated. The various types and frequency of phishing attacks showcase the critical need for robust defense mechanisms against these threats. A basic understanding of best practices and the implementation of high-level S/MIME certificates and automation are key to tackling these issues head on and ensuring the authenticity, integrity and confidentiality of email communications.

Take proactive steps today to secure your organization's communications against evolving cyber threats. Partner with GlobalSign and NoSpamProxy to deploy automated email security solutions that not only protect your business but also enhance operational efficiency and ensure regulatory compliance



Contact us today to discuss your email security needs – visit
<https://www.globalsign.com/en/lp/nospamproxy>

About GMO GlobalSign

As one of the world's most deeply rooted Certificate Authorities, GlobalSign is the leading provider of trusted identity and security solutions enabling organizations, large enterprises, cloud-based service providers and IoT innovators worldwide to conduct secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and identity solutions support the billions of services, devices, people and things comprising the IoT. A subsidiary of Japan-based GMO Cloud KK and GMO Internet Group, GMO GlobalSign has offices in the Americas, Europe and Asia. For more information, visit <https://www.globalsign.com>.