Proofpoint Encryption Architecture

Take control of your Proofpoint Archive

Key Benefits

- Secure data in transit from source applications, while maintaining its encryption in the archive
- Search data without first having to unencrypt it
- Protect your data using standards-based encryption technologies

Proofpoint Archive protects your data in state-of-the-art data centers. It gives you unmatched security and privacy controls for your archived information. And its cloud architecture makes it easy for you to get your search results quickly.

This document takes a look at the encryption architecture at the heart of Proofpoint Archive. It discusses our DoubleBlind key technology, standards-based encryption key protection and more.

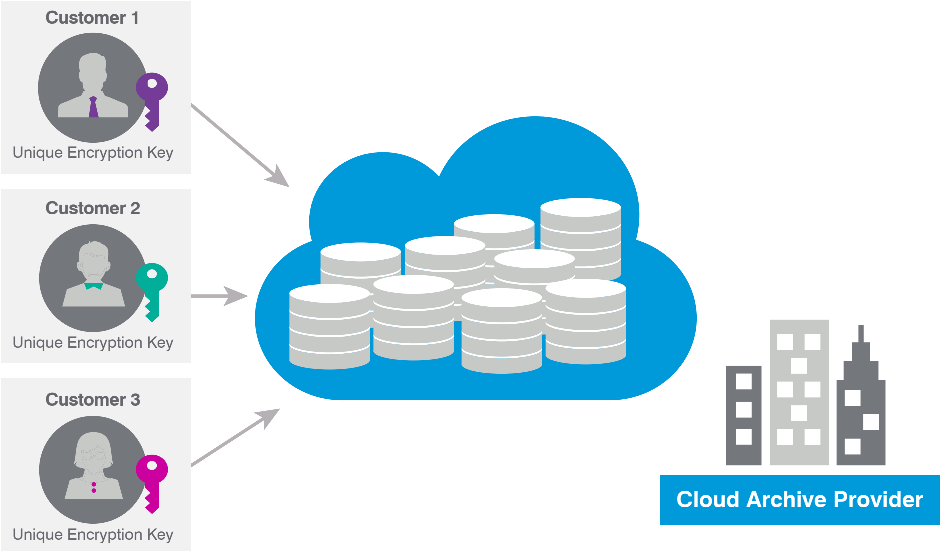

Figure 1: Proofpoint’s DoubleBlind key architecture gives you fully searchable access to your archive data while the data stays encrypted.

DoubleBlind Key Architecture

Proofpoint's DoubleBlind technology is unique in that it provides fully searchable access to your data while keeping that data encrypted. Proofpoint Archive generates the encryption keys during the setup process. Because the data and keys are separated, the information is accessible only when the two components come together.

Separation of key management from data management ensures that nobody at Proofpoint can see or access your data. Even people who get access to the keys cannot see the data unless they also have access to the Proofpoint storage infrastructure. Messages are decrypted only when an authorized user conducts search and discovery using the web-based user interface.

Standards-based Encryption

Our core encryption system uses a combination of 2048-bit asymmetric RSA and 256-bit symmetric AES-256 encryption. We use standards-based encryption technologies for the underlying encryption to maintain the benefits of standardization. The exact process that DoubleBlind technology uses to generate the encryption keys, however, is proprietary. We take advantage of DoubleBlind's unique capabilities to use and manage keys more securely.

All search indexes are encrypted. And all of the data is encrypted in the archive. This way, no one other than you and those you authorize—not even Proofpoint employees—can see the confidential information contained in your archived messages.

Key Protection

Keys are stored in encrypted form. While we encourage you to back up the keys internally, Proofpoint also partners with an escrow service to maintain a copy of them on your behalf. Proofpoint covers the cost of the escrow service, but you are the depositor and the sole beneficiary. Note that Proofpoint can optionally act as a designated third-party downloader for SEC-regulated firms. In this case, Proofpoint is added as a beneficiary, and the release conditions of the escrow agreement require that access to the key is only granted when documentation of a regulator request can be provided.

Additional Security

For extra security, the Proofpoint storage infrastructure can accept requests only from specific IP addresses. As part of the set-up process, you can provide us with the IP address used for communications from your corporate network. Typically, this is the IP address of your firewall. When someone attempts to connect to our network outside of your network, our data centers can reject the request if you choose to configure it that way.

Our data centers are designed with the highest level of security. In the event of a breach, DoubleBlind technology, whether deployed in a hybrid configuration or fully hosted, provides unique safeguards to negate any risk of data theft. Even if there is a security breach, no data would be compromised because it is all maintained in encrypted form in our data centers and the encryption keys are stored separately. We also store the encrypted data across multiple data centers and continuously validate it. These safeguards ensure that any individual block of data that has been tampered with or damaged is automatically identified and restored to its true state.

To know more visit **Proofpoint Archive**.

"Proofpoint Archive" was formerly "Proofpoint Enterprise Archive."

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.