Proofpoint Encryption Architecture

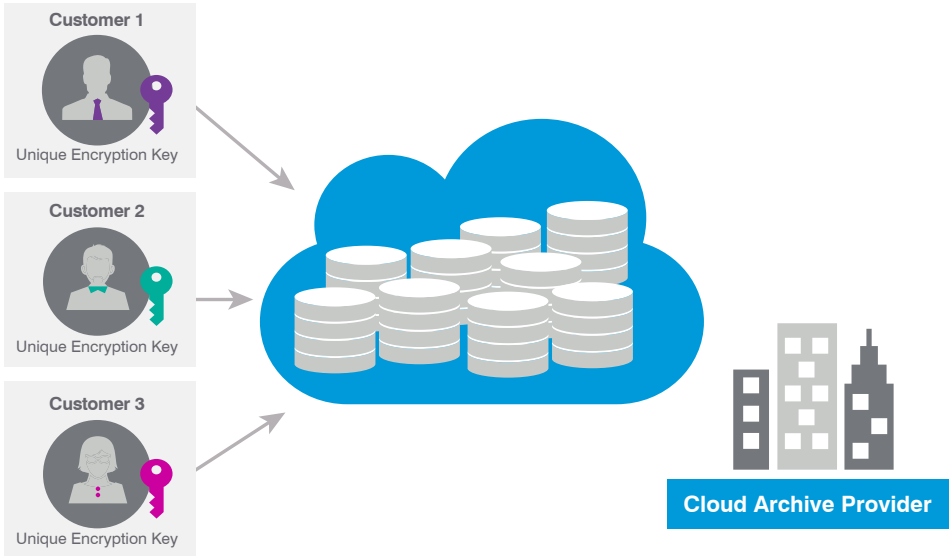
Take Control of Your Enterprise Archive

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

Cyber attackers, criminals and other bad actors are always looking for new vulnerabilities to exploit, and information repositories like backups and archives are no longer beyond the purview of malicious attacks. With Proofpoint Enterprise Archive, standards-based encryption technologies protect your data in state-of-the-art datacenters. Only you and those you authorize will be able to access it.

Our patented encryption technology gives you unmatched security and privacy controls for your archived information. You can also get search results quickly, thanks to our cloud architecture. To guarantee security, you will receive a unique encryption key. This gives you sole access to your archived data.



Proofpoint DoubleBlind Key Architecture gives you full searchable access while keeping data encrypted.

Search while encrypted with DoubleBlind Key Architecture

What makes DoubleBlind technology unique is the ability to maintain the data in encrypted form, while still providing fully searchable access to it. The encryption keys are generated by your Enterprise Archive appliance during the setup process when it is first installed. Separation of data and keys means information is accessible only when the two components come together.

We cannot see your data because we don't have the keys. Someone who obtains 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 provided by the Enterprise Archive appliance.

Use standards-based encryption for the archive

Our core encryption system uses a combination of 2048-bit asymmetric RSA and 256-bit symmetric AES256 encryption. We use standards-based encryption technologies for the underlying encryption to maintain the benefits of standardization. The exact process DoubleBlind technology uses to generate the encryption keys is proprietary, but we do take advantage of its unique capabilities to more securely use and manage keys.

What's more, all of your search indexes are encrypted. And all of the data is encrypted on the Enterprise Archive appliance before transmission. This way, you can be assured that no one other than you—not even Proofpoint employees—can see the confidential information contained in your archived messages.

Ensure keys are protected

Keys are stored in encrypted form on each of your appliances. 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. While Proofpoint covers the cost of the escrow service, you are the depositor and the sole beneficiary. And you have exclusive access to your keys. Note that Proofpoint will 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.

Leave no security "stone" unturned

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. If someone attempts to connect to our network using your Enterprise Archive appliance outside of your network, our datacenters can reject the request, if you choose to configure it that way.

Our datacenters 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 risks 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 datacenters, with the encryption keys stored separately. We also store the encrypted data across multiple datacenters 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 Enterprise Archive.

LEARN MORE

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