

Proofpoint DoubleBlind Encryption TechBrief



Proofpoint DoubleBlind Encryption™ is a patented technology (US patent #7,512,814) used in Proofpoint ARCHIVE™ to ensure the absolute security and privacy of your organization's archived information. This breakthrough encryption technology delivers guaranteed data security coupled with high-speed searchability. Using DoubleBlind Encryption technology, all data stored in Proofpoint's datacenters is encrypted by a key held only by the customer. At the same time, all archived email remains fully searchable with results returned in seconds.

about proofpoint's unique encryption technology

DoubleBlind Encryption technology allows you to retain exclusive access to email and IM data archived in Proofpoint's state-of-the-art datacenters. The technology guarantees security and privacy while still providing full search and discovery capabilities.

How does DoubleBlind Encryption work?

With DoubleBlind Encryption, Proofpoint maintains the data, but does not have the encryption keys. Your Proofpoint ARCHIVE appliance has the encryption keys, but does not maintain the archived data. The Proofpoint ARCHIVE appliance, which maintains your encryption keys, encrypts information before it is sent to the Proofpoint on Demand™ datacenters. The data remains in encrypted form while stored by Proofpoint.

What makes DoubleBlind Encryption unique is the ability to maintain the data in encrypted form, while still providing fully searchable access to it. The separation of the data and the keys means that information is only accessible when the two components come together. Proofpoint cannot see your data as we don't have the keys. Someone that has access to the keys cannot see the data unless they have access to the Proofpoint on Demand storage infrastructure. Messages are decrypted only when an authorized user conducts search and discovery using the web-based user interface provided by the Proofpoint ARCHIVE appliance.

How are the encryption keys generated?

The encryption keys are generated by your Proofpoint ARCHIVE appliance during the setup process when it is first installed within your corporate network.

What type of encryption is used?

While the exact process of DoubleBlind Encryption is proprietary, the core encryption system uses a combination of both 1024-bit asymmetric RSA and 192-bit symmetric TripleDES encryption.

Are the search indexes encrypted?

Yes. All data is encrypted on the Proofpoint ARCHIVE appliance before transmission. In this way, you can be assured that no one other than you—not even Proofpoint employees—can see the confidential information contained in your messages.

What happens if someone steals the Proofpoint ARCHIVE appliance?

The Proofpoint on Demand storage infrastructure only accepts requests from specific IP addresses. As part of the setup process, you provide Proofpoint 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 the Proofpoint Network using your Proofpoint ARCHIVE appliance outside of your network, our datacenters will reject the request.

What if someone breaks into the Proofpoint on Demand infrastructure?

While Proofpoint's datacenters are designed with the highest level of security, in the unlikely event of a breach, no data would be compromised as it is all maintained in encrypted form, with the encryption keys stored only at your location. In addition, redundant storage across multiple datacenters and continuous data validation ensure that any block of data that has been tampered with is automatically identified and restored to its true state.



Guaranteed Data Privacy

Proofpoint's patented DoubleBlind Encryption™ technology guarantees the security of your data, ensuring that no one outside your organization can access your archived data. When a message reaches the Proofpoint ARCHIVE appliance, it is encrypted before being sent outside the customer firewall over a secure connection to Proofpoint's datacenters. Messages are decrypted only when an authorized user on your network conducts a search from Outlook or from Proofpoint's web-based user interface.

This separation of encrypted email data in the cloud and encryption keys on the customer's premises means that protected information is only accessible when the two components are used together. DoubleBlind Encryption is unique in that it maintains data in encrypted form while still providing full search and discovery capabilities. When an authorized user conducts a search, returned email messages are decrypted via the appliance. Without the appliance, DoubleBlind encrypted messages remain indecipherable.

Your data can never be viewed without access to both your Proofpoint ARCHIVE appliance (which resides within your network) and the Proofpoint on Demand datacenters. Not even Proofpoint's own staff can access the contents of your encrypted, archived data.

©2009 Proofpoint, Inc. Proofpoint, Proofpoint ARCHIVE and DoubleBlind Encryption are trademarks or registered trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 06/09