SOLUTION BRIEF

proofpoint.

PROOFPOINT DOUBLEBLIND KEY ARCHITECTURE

UNIQUE TECHNOLOGY, UNMATCHED ENTERPRISE CONTROL

Proofpoint™ DoubleBlind Key Architecture is a patented technology (US patent No. 7,512,814) used in Proofpoint Enterprise Archive to deliver unmatchable security and privacy controls for your organization's archived information.

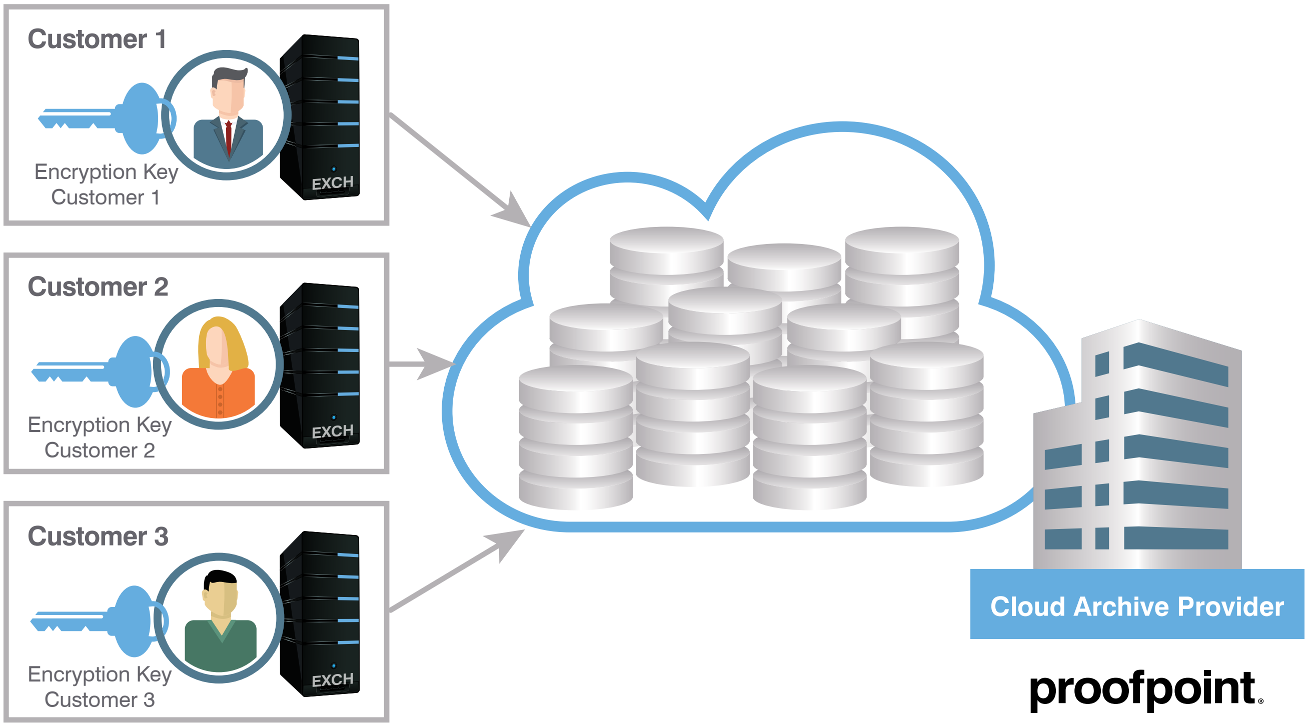
This breakthrough technology delivers guaranteed data security and enterprise-controlled privacy of the information, coupled with high-speed searchability delivered by our cloud architecture. Using DoubleBlind technology, all data stored in Proofpoint datacenters is encrypted with a key held only by the customer. At the same time, all archived email remains fully searchable. With DoubleBlind technology, you retain exclusive access to enterprise data archived in our state-of-the-art datacenters. And because your organization alone has the encryption key, it retains sole access to archived data, providing the data privacy controls that you demand from a cloud-based archiving service.

ABOUT PROOFPOINT'S PATENTED TECHNOLOGY

With this unique key management architecture, We maintain the data, but do not have the encryption or decryption keys.

Your Proofpoint Enterprise Archive appliance holds the keys, but does not maintain the archived data. The Enterprise Archive appliance encrypts information before it leaves your premises and then sends in encrypted format to the Proofpoint datacenters. The data remains encrypted while stored by us.

DOUBLEBLIND KEY ARCHITECTURE


Customer 1
Encryption Key Customer 1
EXCH
Customer 2
Encryption Key Customer 2
EXCH
Customer 3
Encryption Key Customer 3
EXCH
Cloud Archive Provider
proofpoint.

FREQUENTLY ASKED QUESTIONS

How Does DoubleBlind Key Architecture work?

With this unique key management architecture, we maintain the data, but do not have the encryption or decryption keys.

What makes DoubleBlind technology 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 accessible only when the two components come together.

We cannot see your data—we don't have the keys. Someone who obtains access to the keys cannot see the data unless they 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.

How are the encryption keys generated?

The encryption keys are generated by your Enterprise 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 DoubleBlind technology takes to generate the encryption keys is proprietary, the core encryption system uses a combination of both 2048-bit asymmetric RSA and 192-bit symmetric TripleDES encryption. We use standards-based encryption technologies for the underlying encryption to maintain the benefits of standardization. But we also utilize the unique capabilities available through DoubleBlind technology around the architecture of how keys are utilized and managed.

Are the search indexes encrypted?

Yes. All data is encrypted on the Enterprise 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.

How are the encryption keys protected?

Keys are stored in encrypted form on disk 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, such that you have exclusive access to your keys. Note that Proofpoint will optionally act as a designated third party downloader for SEC-regulated firms, in which 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.

What additional security measures are in place?

The Proofpoint storage infrastructure accepts requests only from specific IP addresses. As part of the setup process, you 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 will reject the request.

Our datacenters are designed with the highest level of security. In the unlikely event of a breach, DoubleBlind technology provides the unique safeguards that an enterprise can rely on to negate any risks of such data theft. In the event of a breach, no enterprise data would be compromised because it is all maintained in encrypted form in our datacenters, with the encryption keys stored within your network. 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.

What if Proofpoint hosts my appliances to provide the Archiving Service?

For customers on the fully hosted arching model, the same encryption described above is used to protect customer's data. As Proofpoint hosts the archiving appliances, the encryption keys used by DBKA are managed within Proofpoint datacenters and protected by our rigorous security protocols.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.