Proofpoint Essentials Email Encryption

The need to secure communications that contain sensitive data has never been greater. Fines, negative publicity and loss of customer trust await companies, both large and small, who lose confidential or customer information

Proofpoint Essentials Email Encryption is a cloud-based solution that enables organizations to help reduce the potential negative impact of data loss through the ability to automatically encrypt emails in which sensitive or other confidential data contained is identified. In this document we will walk through the steps we take to ensure your data and all aspects of the solution can meet the enterprise security, availability, and resiliency needs.

Application Security Controls

Administrator Account Control: Administrators can enable and disable the Email Encryption feature within the Proofpoint Essentials user interface.

End User Account Control: End-users use their existing email client to compose emails designated for encryption. The encryption can be manually triggered by the user or automatically triggered by custom filters. In addition, replies to secure mails from external users are sent encrypted and for ease of use are delivered as a standard emails to internal end-user inboxes.

Policy: Administrators can create custom filters that identify sensitive emails that should be encrypted based on content.

Data and File Management

Email Delivery: Data between the Organization and the Proofpoint Essentials service can delivered over TLS. Data in transit is encrypted over a secure channel using 256-bit SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections.

Data Loss Prevention (DLP): DLP enables organizations to securely send and monitor the contents of the files, based on corporate policy. This can help you protect sensitive information and comply with regulations. Proofpoint Essentials Email Encryption supports DLP policy defined within the Essentials interface for licensed internal users.

Encryption: Data is encrypted at rest using AES-256 symmetric key encryption to store messages. A FIPS 140-2 Level 1 compliant encryption algorithm is also used. Keys are managed separately from the message storage and are stored in a separate service.

Data Storage: The uploaded messages are stored in Proofpoint's cloud storage infrastructure utilizing Tier 3 data centers for the purposes of external authentication, processing, notifications, and encrypted storage.

Data Retention: Once a message expires, we delete the encrypted data blob from the storage service.

Infrastructure Security and Resiliency

Secure Facilities: Proofpoint utilizes top-tier data center providers around the world to ensure the most secure and reliable operating environment. All facilities carry SSAE 16 reports and follow ISO 27002 security standards for physical access. All facilities feature:

- On-premise security guards
- Security systems on the building exterior: cameras, false entrances, vehicle blockades, parking lot design, bulletproof glass/walls, and unmarked buildings
- Biometric systems, including palm scanners
- Security cameras with digital recorders and pan-tilt-zoom (PTZ) capabilities
- Portals and man traps that authenticate one person at a time

Physical access to the data centers is enforced, monitored, and logged via badge readers, biometrics, video, and in-person identity verification by on-site personnel. Only named, approved Proofpoint personnel are allowed physical access to the data centers. Access to Proofpoint systems is further restricted within locked cages which are monitored via video.

Resiliency: Customers are deployed in a redundant architecture to ensure high availability. Each datacenter features clean, continuous power, backed by redundant generators. Local short-notice refueling contracts for the backup generators are maintained at each facility.

To maintain optimal environmental conditions, all data centers are built on raised floors with high-volume, zoned temperature and humidity controls. Redundant (N+1) HVAC units maintain flow of air conditioning and are powered by normal and emergency electrical systems.

Multiple Gig-E connection points to the Internet from different service providers to ensure consistent bandwidth and connectivity during heavy volume spikes and peer-wide outages. Firewalls at each point of presence enforce strict access policies that explicitly deny all traffic destined for an unknown address or port.

All network devices (Firewalls, Routers, Switches, Load Balancers) are redundant within each datacenter.

Proofpoint Operations: All Proofpoint employees and contractors must pass a 3rd party background check prior to commencing any work at Proofpoint. This background check includes employment verification, education verification, in person and/or phone based reference checks, criminal background check, driving record check, and a credit background check.

System Monitoring: Managing dedicated resources requires extensive automation and control of production resources. Proofpoint has integrated a variety of widely adopted systems management tools and custom-developed solutions to deliver the highest degree of automation and consistency throughout our infrastructure. Our system inventory is continuously updated and provides the visibility and control necessary to respond to a rapidly growing, highly diverse customer base. A team of dedicated engineers ensures that system administration tasks are documented, automated, and audited for efficiency and consistency.

Infrastructure Monitoring: All systems are actively monitored with local agents collecting hundreds of metrics specific to hardware, networking, and OS. All metrics on each host are continuously measured against a baseline compiled from historical data. Acceptable thresholds are defined based on a combination of optimal performance targets and historical baselines. Alerts are automatically generated when thresholds are crossed and escalation schemes are systematically enforced to ensure potential issues are acknowledged in a timely manner. Hosting operations engineers are available 24 hours a day, 7 days a week to respond to any infrastructure issue.

Vulnerability scanning is performed regularly both with externally available and internally designed tools to verify the integrity of Proofpoint on Demand infrastructure.

Application Monitoring: In addition to our extensive infrastructure monitoring, we actively monitor, trend, and alert on application-specific metrics. By maintaining consistent, optimized configurations, aberrant behavior can be identified and resolved quickly before it impacts performance or capacity. Our core engineering team constantly reviews any incidents and reviews performance metrics from our SaaS environment as a feedback mechanism to ensure continuous improvements in stability and throughput.

Database Infrastructure: Proofpoint Email Encryption is built utilizing a multi-tenant cloud service using shared infrastructure. All messages are stored encrypted and the keys are stored completely separate than the data, so data and keys are not stored together. Additionally only key requests from authenticated systems are allowed. If an attacker were to access the files that are in storage, they would not be able to view or access the data in the clear, all they would see is encrypted blobs of data.

Personnel: The Proofpoint Information security program guides all security-related activities at Proofpoint. This includes physical and logical security for corporate and production environments, threat detection and remediation, policy/standard/procedure generation, business continuity and disaster recovery, and awareness training. Proofpoint requires all employees and contractors to adhere to Proofpoint Security, Non-Disclosure and Confidentiality agreements. Background screening is performed on all Proofpoint staff prior to commencement of employment. In addition a very restricted group of individuals who work for Proofpoint are able to access the data.

Proofpoint also requires that third parties complete the same Security Awareness training as Proofpoint employees and contractors. Proofpoint conducts annual Security Awareness training. All employees, contractors, and 3rd parties are required to complete the training, which is tracked and validated for compliance.

Vulnerability Management: Proofpoint performs monthly internal vulnerability scans and contracts with a third-party security vendor to provide quarterly external vulnerability scans. Results of the scans are regularly reviewed and prioritized by the Proofpoint Information Security Team.

Incident Response and Law Enforcement Process: Proofpoint has a documented Incident Response Plan that is owned by the Information Security team. Included in the plan are processes for alerting, investigation, remediation, customer communications and the involvement of regulators and law enforcement, if appropriate.

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com