DTS

DTS
Secure E-Mail

Secure E-Mail

Emails are indispensable as a means of communication. Especially in the operational environment, they are a fundamental part of most business processes. Because of its architecture, however, the medium of email is very vulnerable to cyber attacks of all kinds and thus to sabotage, industrial espionage and data theft, among other things. When you consider that more than 300 billion emails are sent every day, the scale of the threat becomes clear. It is hardly surprising that over 90% of all attacks on companies start with an email. It quickly becomes clear that email security is a high priority.

With DTS Secure Email, we offer you integrated protection against cyber attacks via email. We ensure the security of your communication channels and thus the security of the entire company. We provide this unique solution as a managed service from our certified data centers in Germany, which also allows you to benefit from DTS's extensive expertise in the field of email security.

- Complete defense against targeted email attacks and malicious attachments and content
- Identification of known & unknown threats
- Highest virus & spam detection rate
- Protection against impostor/BEC attacks
- Dynamic reputation analysis
- Targeted attack protection as a safeguard against new types of threats
- Automated email quarantine using Threat Response Auto-Pull
- DTS managed services from certified data centers in Germany
- First & second-level support (9/5)
- Import of updates & fixes

With Proofpoint's Email Protection, we enable you to secure and control incoming and outgoing email with an easy-to-use solution. You can fully protect your employees, your data and your entire organization from today's threats, including impostor emails, phishing, malware, spam and bulk emails. Dynamic reputation analysis continuously evaluates global IP addresses to determine whether email connections should be accepted, rejected or reduced.

The solution also filters out millions of possible spam attributes in each email using MLX machine learning technology. This spam detection reliably prevents spam emails and attachment-based spam. At the same time, new types of spam attacks are automatically filtered out as soon as they occur. Proofpoint's cloud-based dynamic update service keeps spam detection up-to-date at all times, ensuring maximum detection.

In addition, a local anti-virus scanner and a specially developed anti-virus engine are included. These filter out all known threats contained in emails and attachments and threats independent of anti-virus signatures – for additional protection of your email traffic against phishing attacks.

The email firewall makes it possible to define and enforce compliance policies for message content and attachments. The static filter control system can be customized. In addition, the smart search feature provides advanced real-time email message tracking with forensic logged analysis for troubleshooting purposes. Message tracking log analyses are quickly consolidated across all Proofpoint systems and indexed for fast searching.

Running your own IT security solutions always requires additional resources. At DTS, we support you in all aspects of IT security. We provide you with the solution components from our certified data centers in Germany, take care of the installation, 24/7 operation, import of updates and fixes, maintenance and first & second-level support (9/5). Our technical experts reduce the work required of you to a minimum. Of course, we customize optimal provisioning with you. Make the most of the unique combination of state-of-the-art IT security solutions and DTS managed services.

DTS Targeted Attack Protection

DTS Targeted Attack Protection (TAP) helps you stay one step ahead of attackers with an innovative approach that detects, analyzes and blocks advanced threats before they reach your inbox. This includes not only ransomware and other email threats transmitted via malicious attachments and URLs, but also zero-day threats, polymorphic malware, manipulated documents and phishing attacks, which are scanned in a sandbox environment using static code analysis.

- Defense against malicious attachments and content
- Extensive analysis for known & unknown threats
- Phishing protection through URL rewriting
- Click-time protection

DTS Threat Response Auto-Pull

DTS Threat Response Auto-Pull (TRAP) minimizes your response time and the work for your messaging and security administrators. If a malicious email is detected, TRAP analyzes delivered emails for a match and automatically moves all messages and internally forwarded copies to a quarantine area with restricted access.

- Automated quarantine of dangerous emails
- Exponential reduction in time spent by security & messaging teams
- Use of current threat data (Threat Intelligence Cloud)

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS Secure E-Mail 21112022