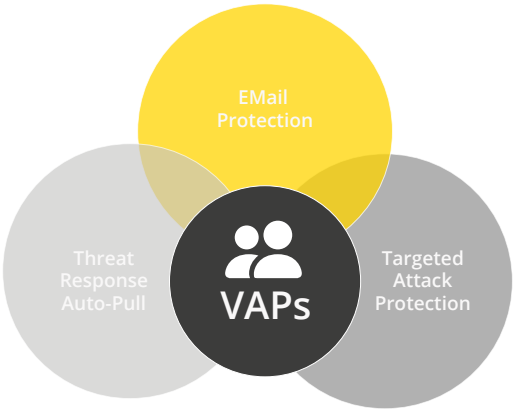
DTS
EMAIL SECURITY

EMAIL SECURITY

Emails are an essential tool for communication and an elementary component of most business processes. However, due to its architecture, email is vulnerable to cyberattacks, including sabotage, industrial spying and data theft. When you consider that more than 300 billion emails are sent every day, the extent of the danger becomes clear. It is no coincidence that over 90% of all attacks on companies start with an email.

The target of the attackers has shifted. Of course, security vulnerabilities and incorrect infrastructure configurations are popular targets. However, the focus is on people, who are "exploited" to execute malicious programs, make bank transfers or enter access data. Identities and information provide the attacker with massive added value for further targeted attacks. It quickly becomes clear that the high prioritization of holistic email security is essential. We provide you with the world's leading solution for defending against email attacks.

- Complete defense against targeted email attacks & 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 protection against new types of threats
- Automated email quarantine using Threat Response Auto-Pull
- DTS managed services, incl. first & second level support (9/5) & updates
- Provision from the certified German DTS data centers on request



Three basic building blocks enable complete email protection for your company and your very attacked people (VAP):

EMAIL PROTECTION

Email Protection helps you secure and control inbound and outbound email with an easy-to-use solution. You can fully protect your employees, data and your entire organization from today's threats, whether impostor emails, phishing, malware, spam or bulk emails. Dynamic Reputation, a dynamic reputation analysis, is a sender reputation check service, it continuously evaluates global IP addresses to determine whether email connections should be accepted, rejected or reduced.

Based on a patented MLX machine learning technology, the solution examines and filters millions of possible spam attributes in each email, including email headers and structure, included images, sender reputation and unstructured content in the body of the message. This spam detection reliably prevents spam emails and attachment-based spam, including PDF and image spam. At the same time, new types of spam attacks are automatically filtered as soon as they occur. The cloud-based dynamic update service keeps spam detection up to date at all times and ensures maximum detection.

Impostor emails, known as business email compromise, are particularly popular. Email Protection also recognizes and classifies such targeted, fraudulent emails thanks to the combination of authentication (DMARC), predefined rules and dynamic classification. The technology actively evaluates the sender's reputation for comprehensive protection without additional administrative effort.

Virus Protection also includes a local antivirus scanner that runs on the gateway and filters out all known threats contained in the emails or attachments. The additional Zero-Hour Antivirus is an antivirus engine that works independently of antivirus signatures and therefore offers additional protection for your email traffic against phishing.

As a real-time email content filter, the email firewall allows you to define and enforce compliance policies for message content and attachments. You can customize the static filter ruleset to your needs, e.g. by specifying the allowed message sizes or attachments.

In addition, the Smart Search function offers extended email message tracking in real time with forensic and logged analysis for troubleshooting purposes. Message tracking log analytics are quickly consolidated across all systems and indexed for fast searching. The analysis information is also continuously updated so that detailed analysis of any email message can be tracked within minutes via the user-friendly interface.

TARGETED ATTACK PROTECTION (TAP)

With TAP you are always one step ahead of attacks. The innovative approach detects, analyzes and blocks advanced threats before they reach your inbox. This includes not only ransomware and threats transmitted via malicious attachments and URLs, but also zero-day threats, polymorphic malware, manipulated documents and phishing. TAP also detects risks in cloud applications and correlates email attacks with credential theft or other attacks.

TAP's Attachment Defense is used to detect and protect against malware contained in PDF, Microsoft Office and file attachments. During message processing, the Protection Server determines whether a message contains attachments for which attachment defense analysis is supported. If this is the case, a SHA256 hash is calculated for each attachment. For emails with unknown attachments, TAP Attachment Defense then forwards a copy of the attachments to both the TAP sandbox and Palo Alto Networks WildFire Cloud for adjudication. The actual email is withheld until a verdict is reached on the attachment. If a threat is detected in a sandbox, the email is handled according to the rules. All information, both from TAP and WildFire, is collected and organized via the TAP dashboard.

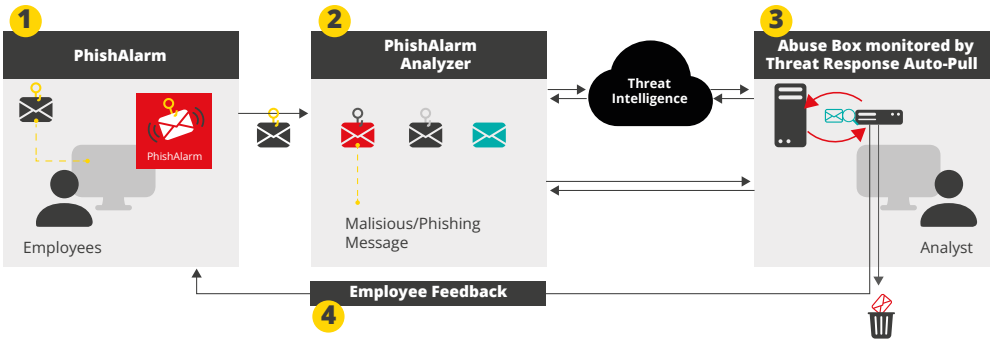
TAP's URL Defense is also used to track and subsequently block clicks on malicious websites without compromising the user experience or other URL filtering technologies. During message processing, URLs are transparently rewritten and forwarded to the cloud-based service. The identified URLs are also sent to the cloud-based sandbox for predictive analysis, which preemptively identifies suspicious URLs based on email traffic patterns. Due to URL re-writing, an additional check of the link takes place at the time a user clicks on the link (click-time defense). It does not matter on which end device the link is clicked, as the URL is permanently redirected to the gateway and thus offers protection for forwarded emails.

THREAT RESPONSE AUTO-PULL (TRAP)

If a malicious email is detected, the detection systems send a warning to the Threat Response System with information about the message. Threat Response then moves the message to quarantine. However, even with the most effective solution, there will always be messages that make it into a user's inbox. The auto-pull function therefore searches for forwarded copies of the message as well as distribution lists of recipients and the message in other inboxes on the same server and also moves these to a quarantine with restricted access. In this way, automation can reduce the workload of the security team and helpdesk staff.

CLOSED LOOP EMAIL ANALYSIS AND RESPONSE (CLEAR)

A trained employee can be your last line of defense against a cyberattack. With CLEAR, the cycle of reporting, analyzing and remediating potentially damaging emails is reduced from days to minutes. Enriched with our leading cybersecurity threat intelligence solutions and security awareness training, CLEAR can block active attacks with a single click. And by automatically responding to malicious messages, your team saves valuable time and effort. Using the PhishAlarm plug-in, which is installed in your employees' email application, they can report suspicious emails directly. The reported emails are moved to a specially set up mailbox, where they are checked for various parameters by PhishAlarm Analyzer and Threat Intelligence. This makes it easier for the email administrator to check for maliciousness. Clearly malicious emails can then be automatically removed from all mailboxes via Threat Response Auto-Pull.



DTS MANAGED SERVICES

Operating IT security solutions yourself always involves additional resources. As DTS, we support you across the entire scope of IT security. We provide you with the solution components from our certified German data centers, take care of installation, 24/7 operation, the installation of updates and fixes, maintenance and first and second level support (9/5). Our technical experts reduce your workload to a minimum. Of course, we work with you to customize the optimal deployment. Benefit from the unique combination of state-of-the-art IT security solutions and DTS managed services.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS E-Mail Security E 04032024