EveryCloud®

Advanced Threat Protection

Detect and prevent highly complex and sophisticated attacks - effectively and in real time.

Working with our technology partner, Hornetsecurity, EveryCloud brings you Advanced Threat Protection ATP, which allows you to protect your business against individually targeted attacks starting from the first malicious email. Highly innovative forensic analysis engines ensure that the attacks are stopped immediately.

At the same time as protecting you, the solution provides detailed information about the attacks on the company.

Protection against ransomware

Ransomware attacks have increased sharply since the beginning of 2016: these are viruses that cripple the computer or an entire network by encrypting the locally stored files. It is only by paying a ransom - that users have a chance to re-access their data. Locky, Tesla, Petya and the like are polymorphic viruses that can be very difficult to detect. To do so, ATP uses, amongst other things, a sandbox engine to enable safe analysis of the behaviour of attachments when they are opened and filters out the email in the event of a positive find. ATP also “freezes” suspicious emails, and once the virus signatures of the filters have been updated, the emails are re-scanned after a few minutes.

Protection against blended attacks

Blended attacks combine different avenues of attack to be successful. The email can for example, include a document that can hide a link to a download page with malware. Hornetsecurity ATP combats these types of attacks by means of URL scanning and URL rewriting, as well as sandboxing and freezing.

Protection against targeted attacks

High-ranking employees of companies are often the target of individual attacks, so-called spear phishing, whaling or CEO fraud. The attackers try to obtain passwords or credit card information, or convince the employees to transfer funds to a specific account. These attacks are virtually undetectable by conventional means. With Hornetsecurity ATP, the internal communication between particular persons in the company is specifically examined for such attacks in order to prevent abuse through identity spoofing.

Protection against digital espionage

According to a survey conducted by the IT industry association Bitkom, more than half of German companies have already been the victim of data theft, sabotage, or espionage. The Hornetsecurity Spy-Out forensic system detects both known and completely new patterns for spying out information. This system reacts instantly and alerts you before information needing protection leaves the company. The Hornetsecurity real time alerts notify you of acute attacks on your company and allow the rapid initiation of further internal measures and legal procedures.

Notifications of attacks

The EveryCloud real-time alerts notify you of acute attacks on your company and allow the rapid initiation of further internal measures and legal procedures. The notification system provides detailed analysis results for this purpose. The customer security team can also train employees to identify additional avenues of attack, for example, by telephone. If already delivered emails are later identified as potentially harmful, ex-post alerting enables the IT security team to undertake an investigation into the accounts or systems affected.

EveryCloud®

Integration of EveryCloud ATP into email security management.

EveryCloud ATP integrates seamlessly into spam and virus filters. Emails that have passed this first examination are subjected to further detailed analyses by EveryCloud ATP. Amongst other things, the service opens any attached files and observes it's behaviour in more detail.

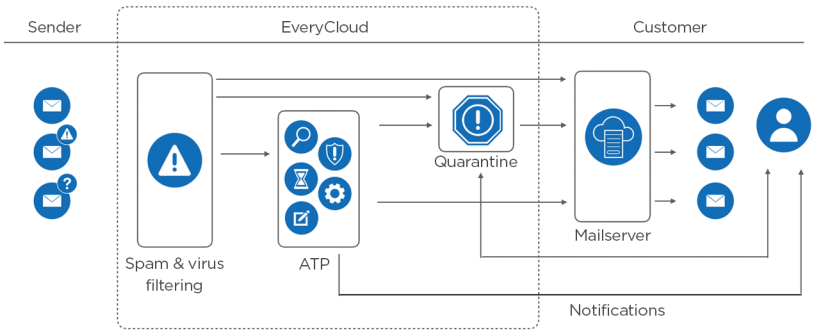

Fig: Spam and Virus filter procedure with EveryCloud ATP.

EveryCloud®

EveryCloud Advanced Threat Protection - Real Time Alert

The EveryCloud Advanced Threat Protection Service has just detected the following email attack:

Classification:	
User:	accounting@everycloudtech.com
Date:	03/09/2018 10:22pm CEST
Sender	phisher@hackeddomain.com phisher@hackeddomain.com
Server Address:	123.123.123.123, relay42.hackerserver.com
Reason:	EveryCloud-ATP01
URL:	http://bit.lyaxJMehl

Real-time notifications

As soon as EveryCloud's ATP detects an attack, an alert is sent to the respective company's IT security team to inform it immediately about a possible threat. The person in charge is given various details on the nature and objective of the attack, the sender, and why the email was intercepted.

Fig: Real-time notification by EveryCloud

EveryCloud ATP engines

Functioning and advantages

Integration of Hornetsecurity ATP into email security management	Hornetsecurity ATP integrates seamlessly into spam and virus filters. Emails that have passed this first test are subjected to further analysis by Hornetsecurity ATP
Sandbox engine	Sandbox engine attachments are executed in a variety of system environments, and their behavior is analyzed. If it turns out to be malware, you are notified
URL rewriting	The URL rewriting engine secures all Internet calls from emails via the Hornetsecurity web filter. In the process, the sandbox engine also analyses downloads.
URL scanning	A document (such as PDF, Microsoft Office) attached to an email may contain links. However, these cannot be replaced, as this would violate the integrity of the document. The Hornetsecurity URL scanning engine leaves the document in its original form and only checks the target of such links
Freezing	Emails that cannot immediately be clearly classified but look suspicious are retained for a short period by freezing. A further test is later performed with updated signatures. Protects against ransomware, blended attacks, and phishing attacks
Targeted fraud forensics	Targeted fraud forensics detects targeted personalised attacks without malware or links. The following detection mechanisms are used for this: • Intention recognition system: alerting about content patterns that indicate malicious intent • Fraud attempt analysis: checks the authenticity and integrity of metadata and email content • Identity spoofing recognition: detection and blocking of forged sender identities • Spy-out detection: counter-espionage against attacks trying to obtain sensitive information • Feign facts identification: the content analysis of messages based on the provision of feigned facts • Targeted attack detection: detection of targeted attacks on individuals
Active threat intelligence collection	Our threat intelligence is taken from our customers' active live traffic of 1 billion emails a month across 50,000 domains. We use this data to keep our stats at 99.99% detection for Viruses/Spam with our standard email filter and with a false-positive rate of 0.0015%