HORNETSECURITY
BY proofpoint

FACTSHEET
AI POWERED

ADVANCED THREAT PROTECTION

AI-POWERED ADVANCED PROTECTION OF EMAILS AND DATA, EVEN FROM THE MOST SOPHISTICATED THREATS.

Cybercriminals work tirelessly to develop new cyber threats, making it difficult for security software to keep up and protect users from newly emerging attack methods. Ransomware, CEO fraud, spear phishing, blended attacks are just examples of the dangers lurking in the cyberspace.

With the rise of widely available AI tools, cybercriminals can effortlessly create flawless-looking phishing emails, and even bypass safeguards and use AI text generating tools to create malicious codes.

With Advanced Threat Protection, you don't need to worry about anything of the above. Using AI to its advantage, Advanced Threat Protection keeps you ahead of cybercriminals, securing you from zero-day attacks and even the most sophisticated threats.

HOW DOES **ADVANCED THREAT PROTECTION** HELP YOU WITH EMAIL COMMUNICATION?

AI-based Targeted Forensics – Detect brand-new and even the most sophisticated threats.

Sandbox-Engine – Tests email attachments for malicious files in a controlled environment.

Reporting – Get a comprehensive overview of all attempted attacks, security alerts, ATP reports, and forensic information.

ADVANCED THREAT PROTECTION keeps your email mailboxes secure

ADVANCED THREAT PROTECTION SANDBOX VS. RANSOMWARE & POLYMORPHE VIREN

FILETYPES	BINARY ANALYTICS	SANDBOX 500+ BEHAVIOURAL ANALYSIS SENSORS	REPORTING AND DATA ANALYTICS
EXE	MACRO OBFUSCATION	ANTI VM EVASION DETECTION	LIVE THREAT MONITOR
PDF	URL OBJECTS	MACHINE LEARNING ENGINE	SECURITY ALERTS
OFFICE	METADATA JAVASCRIPT	FILESYSTEM MONITOR	ATP-REPORTS
ARCHIVE	HEURISTIC	NETWORK TRAFFIC ANALYSIS	FORENSIC INFORMATION
	STATIC ANALYSIS	PROCESS- AND REGISTRY MONITOR	
	ZERO HOUR THREAT OUTBREAK DETECION	FORENSIC MEMORY ANALYSIS	

ATP-ENGINES	FUNCTIONALITY AND ADVANTAGES
Sandbox Engine	Email attachments are scanned for possible malicious codes by running the suspicious file in a virtual test environment and identifying potentially dangerous effects. If the document sent with the email is found to be malware, the email is moved directly to quarantine.
Secure Links	No more risky link clicks in emails. Secure Links replaces the original link with a rewritten version that goes through Hornetsecurity's secure web gateway. Secure Links uses artificial intelligence, including machine learning and deep learning, to provide advanced protection against phishing, even in short-wave, highly targeted attacks. Supervised and unsupervised machine learning algorithms analyze more than 47 characteristics of URLs and web pages, scanning for malicious behaviors, obfuscation techniques, and URL redirects, while computer vision models analyze images to extract relevant features used in phishing attacks, including brand logos, QR codes, and suspicious textual content embedded within images.
URL Scanning	Leaves the document attached to an email in its original form and only checks the target of links contained in it.
Freezing	Emails that are not able to be clearly classified immediately are held back for a short period of time. The emails are then subjected to a further check with updated signatures.
Malicious Document Decryption	Encrypted email attachments are decrypted using appropriate text modules within an email. The decrypted document is then subjected to an in-depth virus scan.
KI-unterstützte Targeted Fraud Forensics	**Fraud attempt analysis:** Checks the authenticity and integrity of metadata and mail content. **Identity spoofing recognition:** Detection and blocking of forged sender identities. **Intention recognition system:** Alerting to content patterns that suggest malicious intent. **Spy-out detection:** Defense against espionage attacks to obtain sensitive information. **Feign facts identification:** Identity-independent content analysis of news on the basis of falsified facts. **Targeted attack detection:** Detection of targeted attacks on individuals who are particularly at risk.
QR Code Analyzer	Hornetsecurity's QR Code Analyzer is able to detect QR codes embedded directly into an email or an image. All QR codes are detected and scanned at the speed of light for malicious content. It supports all common image types such as GIF, JPEG, PNG and BMP.
AutoRemediate AutoRemediate Alert	AutoRemediate allows 365 Total Protection administrators to delete emails from users' Microsoft 365 mailboxes even after they have been delivered. Additionally, emails that were previously delivered to Microsoft 365 mailboxes and later identified as a threat are automatically deleted from users mailboxes. AutoRemediate Alert notifies administrators if already delivered emails are later classified as malicious, allowing them to immediately initiate actions.