HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

Hochkomplexe und ausgeklügelte Attacken erkennen und verhindern – effektiv und in Echtzeit.

Schützen Sie Ihr Unternehmen mit ATP vor gezielten und individuellen Angriffen ab der ersten Schad-Mail. Hochinnovative forensische Analyse-Engines sorgen dafür, dass Attacken sofort unterbunden werden. Gleichzeitig liefert die Lösung detaillierte Informationen über die Angriffe auf das Unternehmen.

Schutz vor:

- Ransomware
- Blended Attacks
- Targeted Attacks
- digitaler Spionage

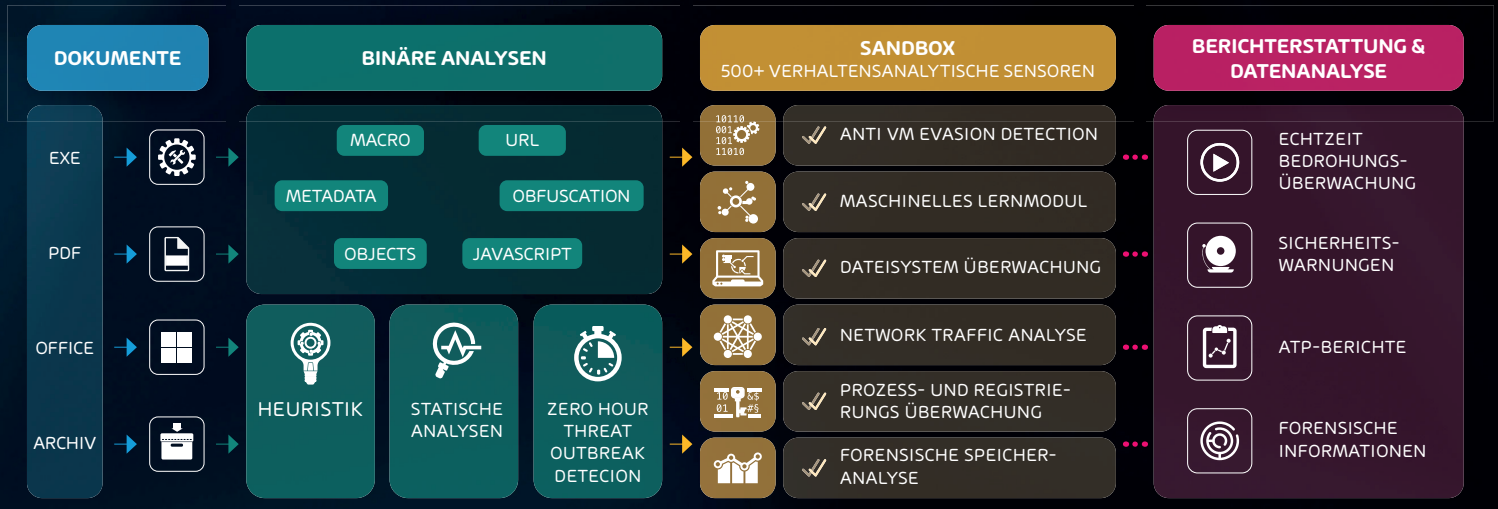
Fraud Schutzmechanismen

- Analyse von Fraud E-Mails auf **Inhalts- sowie Metaebene**
- Analyse von **SMTP Transportdaten** in Kontext mit Führungsstruktur eines Unternehmens
- Anfragen nach Geldmitteln/kritischen Informationen nur aus unternehmensinternen Quellen gestattet
- Externe E-Mails - mit als Geschäftsführer vorgetäuschten Absendern – werden blockiert.

Ransomware Schutzmechanismen

- **ATP Sandbox** greift beim Überprüfen von E-Mail Anhängen auf Threat Intelligence Datenbanken zu
- Gespeicherte **Indicators of Compromise (IoC)** werden mithilfe von über 50 auf dem Markt erhältlichen Anti-Virus Engines klassifiziert
- Anreicherung der Analysen mit Informationen zu bereits bekannten Hashsummen (z.B. von schadhaften Anhängen oder IP Adressen, die im Kontext mit bösartigen Instanzen stehen)
- **Nur ca. 5 % der IoCs zu neuartigen Ransomware Kampagnen wurden im Jahr 2018 von herkömmlichen Anti-Virus Engines bei Ersterscheinung einer Ransomware negativ bewertet.**
- **Real Time Alarmierung: Benachrichtigung der IT-Sicherheitsteams in Echtzeit über akute Angriffe auf das Unternehmen. Enthält detaillierte Informationen über Art und Umfang des Angriffes.**

Abb.: Advanced Threat Protection Sandbox vs. Ransomware & Polymorphe Viren



www.hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0

HORNETSECURITY

FACT SHEET

ATP-Engines	Funktionsweise und Vorteile
Sandbox Engine	Dateianhänge werden in einer Vielzahl verschiedener Systemumgebungen ausgeführt und ihr Verhalten analysiert. Stellt sich heraus, dass es sich um Malware handelt, werden Sie benachrichtigt. Schützt vor Ransomware und Blended Attacks.
URL Rewriting	Sichert alle Internet-Aufrufe aus E-Mails heraus über den Webfilter ab. „Time of Click Analysis" sichert die gesamte vom Link in der E-Mail ausgehende Session des Benutzers live ab.
URL Scanning	An eine E-Mail angehängte Dokumente (z.B. PDF, Microsoft Office) können Links enthalten. Diese lassen sich jedoch nicht ersetzen, da dies die Integrität des Dokumentes verletzen würde. Die URL Scanning Engine belässt das Dokument in seiner Originalform und prüft ausschließlich das Ziel dieser Links.
Freezing	Nicht sofort eindeutig klassifizierbare, aber verdächtige E-Mails werden per Freezing über einen kurzen Zeitraum zurückgehalten. Anschließend erfolgt eine weitere Prüfung mit aktualisierten Signaturen. Schützt vor Ransomware, Blended Attacks und Phishing-Angriffen.
Malicious Document Decryption	Verschlüsselte E-Mail Anhänge werden durch passende Textbausteine innerhalb einer E-Mail entschlüsselt. Das entschlüsselte Dokument wird schließlich einer tiefergehenden Virenüberprüfung unterzogen.
Targeted Fraud Forensics	Die Targeted Fraud Forensics erkennt gezielte personalisierte Angriffe ohne Malware oder Links. Dabei kommen folgende Erkennungsmechanismen zum Einsatz: **Intention Recognition System:** Alarmierung bei Inhaltsmustern, die auf bösartige Absichten schließen lassen **Fraud Attempt Analysis:** Prüft die Authentizität und Integrität von Metadaten und Mailinhalten **Identity Spoofing Recognition:** Erkennung und Blockierung gefälschter Absender-Identitäten **Spy-Out Detection:** Spionageabwehr von Attacken zur Erlangung schützenswerter Informationen **Feign Facts Identification:** Inhaltsanalyse von Nachrichten auf Basis von Vorspiegelung fingierter Tatsachen **Targeted Attack Detection:** Erkennung gezielter Angriffe auf einzelne Personen