Advanced Email Security

für Acronis Cyber Protect Cloud

Verbessern Sie die Sicherheit Ihrer Kunden, indem Sie aktuelle E-Mail-basierte Angriffe stoppen, bevor sie die Endbenutzer erreichen

Blockieren Sie E-Mail-basierte Bedrohungen, einschließlich Spam, Phishing, Kompromittierungen von Firmen-E-Mail-Adressen (BEC), Kontoübernahmen (ATO), Malware, hochentwickelte permanente Bedrohungen (APTs) und Zero-Day-Angriffe, bevor sie die E-Mail-Postfächer der Endbenutzer in Microsoft 365, Google Workspace oder bei anderen Cloud-Anbietern bzw. lokalen E-Mail-Servern erreichen. Mit dieser Cloud-basierten E-Mail-Sicherheitslösung der nächsten Generation erzielen Sie ganzheitlichen Schutz mit besonders hohen Erkennungsraten und geringen False Positives – bei hervorragender Geschwindigkeit, Skalierbarkeit und Agilität.

Verbessern Sie Ihre Cyber Protection-Services mit E-Mail-Sicherheit aus der Cloud

Stoppen von Phishing- und Spoofing-Versuchen

Minimieren Sie die E-Mail-Risiken für Ihre Kunden mit leistungsstarker Threat Intelligence, Signatur-basierter Erkennung, URL-Reputationsprüfungen und einzigartigen Bilderkennungsalgorithmen sowie Machine Learning-Technologie zur Prüfung von DMARC-, DKIM- und SPF-Datensätzen.

Erkennen hochentwickelter Umgehungstechniken

Erkennen Sie verborgene böswillige Inhalte, indem Sie angehängte oder eingebettete Dateien und URLs rekursiv entpacken und separat mit dynamischen und statischen Erkennungs-Engines analysieren. Führen Sie dazu intensive Scans des gesamten Inhalts durch.

Verhindern von APTs und Zero-Day-Angriffen

Verhindern Sie hochentwickelte Bedrohungen, die herkömmliche Schutzmaßnahmen umgehen. Nutzen Sie dazu die einzigartige Perception Point-Technologie auf CPU-Ebene, die Exploits blockiert, bevor die Malware aktiv wird. Zudem sind eindeutige Bewertungen innerhalb von Sekunden möglich.

ERSCHLIESSEN NEUER EINNAHMEQUELLEN	SCHUTZ DES WICHTIGSTEN BEDROHUNGS-VEKTORS IHRER KUNDEN VOR AKTUELLEN E-MAIL-ANGRIFFEN	KONSOLIDIERUNG UND OPTIMIERUNG IHRER SERVICES – BEI WENIGER ZEIT- UND RESSOURCENAUFWAND
• Erweitern bzw. verbessern Sie Ihre Services für E-Mail-Sicherheit. • Beginnen Sie mit der Planung des Upgrades Ihrer Services, ohne dass der Zeitaufwand für die Implementierung Sorgen bereitet. Advanced Email Security wird per Knopfdruck aktiviert.	• Minimieren Sie die Risiken Ihrer Kunden bei der Kommunikation per E-Mail und stoppen Sie Bedrohungen, bevor sie die Microsoft 365-, Google Workspace- oder lokalen Postfächer der Endbenutzer erreichen. • Stoppen Sie aktuelle E-Mail-Bedrohungen, einschließlich Spam, Phishing, Kompromittierung von Firmen-E-Mail-Adressen (Business Email Compromise, BEC), Kontoübernahmen (ATO), Spoofing, Malware, böswillige URLs, Zero-Day-Angriffe und APTs (hochentwickelte permanente Bedrohungen) innerhalb weniger Sekunden und ohne False Positives.	• Sie verwalten nur eine Lösung, die E-Mail-Sicherheit, Backup, Disaster Recovery, Malware-Schutz der nächsten Generation und Cyber Protection-Verwaltung kombiniert. Dadurch benötigen Sie weniger Ressourcen für die Bereitstellung der Services. • Senken Sie die Kosten, indem Sie Lösungen konsolidieren.

- Verbessern Sie Ihre Marge, die Rentabilität und den Business-Plan und sichern Sie sich zusätzliche Einnahmequellen.
- Profitieren Sie von nutzungsabhängigen Preisen.

- Ermöglichen Sie Audits und Sicherheitsuntersuchungen mit einem umfassenden Überprüfungsprotokoll.
- Decken Sie den gesamten Datenverkehr in Echtzeit ab und skalieren Sie die Analysekapazitäten, sodass jeder Content geprüft werden kann.
- Stören Sie keine Prozesse und stellen Sie sicher, dass Verzögerungen minimal bleiben. Sie erhalten eindeutige Bewertungsergebnisse – praktisch ohne False Positives – innerhalb von 10 Sekunden, verglichen mit 7–20 Minuten bei Sandbox-Lösungen.
- Bauen Sie Ihre Services auf branchenführenden Technologien auf, die bei unabhängigen Untersuchungen (SE Labs) als führend hervorgehen.

- Das Deployment der E-Mail-Sicherheit ist innerhalb weniger Minuten möglich, außerdem sind keine zusätzlichen Konfigurationen erforderlich.
- Sie erhalten einen besseren Überblick über alle Warnmeldungen und Vorfälle in Bezug auf E-Mail-Sicherheit.
- Unterstützen Sie Ihre Service-Bereitstellungsteams und Ihre Sicherheitsexperten, indem Sie ihnen direkten Zugang zu Cyberanalysten und E-Mail-Sicherheitsexperten ermöglichen.

Schützen Sie die am stärksten gefährdeten Kommunikationskanäle Ihrer Kunden mit unerreichten Schutzfunktionen

Spam-Filter

Blockieren Sie böswillige Kommunikation mit Spam-Schutz und Reputations-basierten Filtern, die Daten aus mehreren marktführenden Technologien nutzen.

Umgehungsschutz * Einzigartig

Erkennen Sie verborgene böswillige Inhalte, indem Inhalte rekursiv in kleinere Einheiten entpackt werden, die anschließend dynamisch von mehreren Engines geprüft werden. Das dauert weniger als 30 Sekunden und damit deutlich weniger als die mehr als die 20 Minuten bei herkömmlichen Sandbox-Lösungen.

Threat Intelligence

Bleiben Sie neuen Bedrohungen immer einen Schritt voraus. Nutzen Sie dazu die kombinierte Threat Intelligence von sechs marktführenden Quellen plus die Perception Point-Engine, die URLs und Dateien im Umlauf prüft.

Statische signaturbasierte Analyse

Identifizieren Sie bekannte Bedrohungen mithilfe erstklassiger signaturbasierter Virenschutz-Engines von Perception Point, die auch äußerst komplexe Signaturen identifizieren.

Phishing-Schutz-Engine * Einzigartig

Erkennen Sie böswillige URLs basierend auf vier führenden URL-Reputations-Engines in Kombination mit der hochentwickelten Bilderkennungstechnologie von Perception Point.

Spoofing-Schutz

Verhindern Sie äußerst zuverlässig Angriffe ohne Schaddaten (z. B. Spoofing, Doppelgänger-Domains und Anzeigenamen-Täuschung) mit Machine Learning-Algorithmen mit IP-Reputation, SPF-, DKIM- und DMARC-Prüfungen.

Dynamische Erkennung der nächsten Generation * Einzigartig

Stoppen Sie hochentwickelte Bedrohungen wie APTs und Zero-Day-Angriffe mit der einzigartigen Perception Point-Technologie auf CPU-Ebene, die Angriffe noch in der Ausnutzungsphase erkennt und blockiert, indem sie während der Laufzeit Abweichungen von Standardabläufen identifiziert.

Vorfallreaktions-Service

Sie erhalten direkten Zugang zu Cyberanalysten, die als Erweiterung Ihres eigenen Service-Bereitstellungsteams agieren. Dadurch wird der gesamte Datenverkehr überwacht und nach böswilligen Verhaltensweisen gesucht. Sie erhalten kontinuierliche Berichte und Support, einschließlich Handhabung von False Positives, Behebungen und Freigaben bei Bedarf.

Bewährte Einhaltung von Vorschriften

AICPA SOC 2 – AICPA Service Organization Control Reports – Formerly SAS 70 Reports

HIPAA

GDPR

CCPA

BESTANDTEIL VON ACRONIS CYBER PROTECT CLOUD

Advanced Email Security ist eines von mehreren Advanced Protection-Paketen für die Lösung Acronis Cyber Protect Cloud, die Cyber Security, Data Protection und Verwaltung für den Schutz von Endpunkten in einer integrierten Lösung abdeckt, die für Service Provider konzipiert wurde. Jedes Advanced-Paket bietet zusätzliche Funktionen, damit Service Provider ihre Services erweitern, Kundenanforderungen erfüllen und für jeden Workload optimale Cyber Protection bieten können.

JETZT TESTEN

Acronis

Weitere Informationen unter www.acronis.com