EDR und EPP – umfassender Schutz im perfekten Zusammenspiel

Zur Abwehr komplexer Cyberbedrohungen reichen traditionelle Endpoint-Schutzlösungen (EPP) nicht. Nur eine Kombination von klassischen Endpoint-Protection-Mechanismen mit modernen Technologien für Endpoint Detection and Response (EDR) liefert das nötige Schutzniveau.

Praktisch alle Unternehmen sehen sich mit immer herausfordernderen Cyberbedrohungen konfrontiert. Täglich werden hunderttausendfach neue Viren, Trojaner und anderer Schadcode entdeckt. Dazu kommen stets raffiniertere und komplexere Angriffsmethoden wie etwa Attacken auf Zero-Day-Schwachstellen, die das Zeitfenster zwischen dem Erscheinen eines neuen Virus und der Entwicklung eines Gegenmittels ausnutzen, oder gezielte Angriffe auf bestimmte Mitarbeitende sowie Advanced Persistent Threats, die sich im Unternehmensnetz einnisten und langfristig Schaden verursachen. Solche fortgeschrittenen Bedrohungen können zum Beispiel wichtige Dokumente verschlüsseln, um Lösegeld zu erpressen, oder vertrauliche Daten zum Zweck der Industriespionage abgreifen.

Antivirus genügt nicht mehr

Traditionelle Endpoint-Schutzlösungen, die auf Vorbeugung setzen sowie Signaturdateien und heuristische Algorithmen nutzen, bieten einen guten Schutz vor bekanntem Schadcode. Doch gegen neuartige und ausgeklügelte Angriffe helfen sie nur bedingt, da sie die im Netzwerk laufenden Prozesse und Anwendungen nicht permanent überwachen. Manches IT-Security-Team setzt deshalb zusätzlich weitere Schutzlösungen ein, darunter sogenannte EDR-Plattformen (Endpoint Detection and Response). Diese erkennen auch bisher unbekannte Bedrohungen und liefern wichtige Informationen zu deren Abwehr. Doch wenn verschiedene Produkte unterschiedlicher Hersteller im Einsatz sind, fehlt die Gesamtübersicht und der Verwaltungsaufwand steigt ins Unermessliche.

Adaptive Defense 360 ist die erste und einzige Lösung, die die Endpoint-Protection-Plattform (EPP) von WatchGuard mit Endpoint-Detection-and-Response-Technologien (EDR) kombiniert.

Umfassender Schutz dank Kombination von EPP und EDR

«Panda Adaptive Defense 360» (AD360) ist die wegweisende Antwort von WatchGuard auf diese Problematik. Dabei handelt es sich um die erste und bisher einzige Lösung, die eine hocheffektive Endpoint-Protection-Plattform (EPP) mit EDR-Technologien der nächsten Generation unter einem Dach vereint. Der EDR-Service von AD360 sorgt dafür, dass nur vertrauenswürdige Prozesse ausgeführt werden. Das Sicherheitsmodell beruht auf drei Säulen: Alle Anwendungen auf Firmencomputern und Servern sowie sämtliche Aktivitäten auf den Endpoints werden erstens gemäss dem Zero-Trust-Ansatz ständig überwacht. Dabei findet zweitens in Echtzeit eine Klassifizierung durch eine innovative Kombination von KI-Technologien wie Big Data, Machine Learning und Deep Learning statt. Als böswillig erkannte Vorgänge unterbindet AD360 vollautomatisch, ohne dass das IT-Team eingreifen muss. Und drittens werden nicht automatisch klassifizierbare Anwendungen blockiert und durch spezialisierte Threat-Hunting-Techniker der PandaLabs analysiert.

Entlastung für die IT, attraktiv für Partner

Auf diese Weise automatisiert AD360 viele bisher manuell zu erledigenden IT-Security-Prozesse und reduziert die Arbeitsbelastung der IT-Mitarbeitenden massgeblich. Teil der Gesamtlösung ist die EPP-Plattform von WatchGuard, die einfache und zentralisierbare Sicherheit, Wiederherstellungsmassnahmen, Echtzeit-Monitoring und Reports, profilbasierten Schutz, zentrale Gerätesteuerung sowie Web-Filtering bietet. Im Zusammenspiel mit der EDR-Funktionalität ergibt sich der bestmögliche Malware-Schutz auf neuestem technischen Stand der Prävention, Erkennung, Forensik und Desinfektion in einer ganzheitlichen Lösung kombiniert.

Adaptive Defense 360 eignet sich als cloudbasierte Lösung in Form einer Kombination verschiedener Managed Services ideal für KMUs, die nur über minimale interne IT-Ressourcen verfügen. Die Lösung ist zudem in die Aether-Plattform von Panda integriert. Unternehmen können damit ihre AD360-Clients zentral über ein einheitliches Dashboard verwalten. Aether ist darüber hinaus mandantenfähig. Dies erlaubt WatchGuard-Partnern den Bezug von Pool-Lizenzen, die sie dann individuell verschiedenen Kunden zuteilen und so AD360 als innovative Cyber-Protection-Lösung anbieten können.

Adaptive Defense 360: die Highlights

- Kombination von EPP und EDR mit zentraler Verwaltung
- Schnellere Analyse von und Reaktion auf Cybersicherheitsproblematik
- Automatische Klassifizierung aller laufenden Prozesse und Anwendungen
- Automatisierte Erkennung und Behebung bösartiger Aktivitäten
- Kontinuierliche Überwachung und zentrale Visualisierung der Endpoints
- Mandantenfähige Managed-Service-Lösung – ideal für KMUs und Reseller

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch