

AGENT

powered by



DURCHGÄNGIGE SICHTBARKEIT UND KONTROLLE

NETZWERKINTEGRITÄT BIS ZUM ENDPOINT

Die Zahl der Endgeräte im Netzwerk und die Komplexität von IT-Infrastrukturen wächst stetig. Geht hier die Übersicht verloren, entstehen schnell neue Angriffsvektoren. Diese blinden Flecken im Netzwerk und ungeschützten Endgeräte werden vermehrt zum Ziel von Cyberangriffen. Das Add-on liefert in Verbindung mit der ARP-GUARD NAC Lösung eine wertvolle Unterstützung, die Sicherheitslage der IT-Assets im Netzwerk zu analysieren. Der vertiefte Einblick in alle netzwerkfähigen Geräte eines Unternehmens ermöglicht, Schwachstellen frühzeitig zu erkennen und zu bewerten. Damit steht eine Plattform bereit, um die gesamte Prozesskette des Asset- und Schwachstellen-Managements abzubilden.

DURCHGÄNGIGE IT-HYGIENE IN ECHTZEIT

Durch eine permanente Überprüfung der IT-Hygiene der angebotenen Endgeräte wird die Einhaltung der vordefinierten Sicherheitsrichtlinien durchgehend gewährleistet.

Die Erkennung und Meldung von Bedrohungen in Echtzeit verhindert, dass sich Schadsoftware unbemerkt im Unternehmensnetzwerk ausbreiten kann.

GEFAHRENPOTENZIALE ERKENNEN UND BEWERTEN

Anhand einer integrierten Threat Intelligence wird das reale Gefahrenpotenzial einer Schwachstelle ermittelt, unter Berücksichtigung des Common Vulnerability Scoring System (CVSS) als Industriestandard. Der Fokus liegt hierbei auf dem echten Risk Score, dieser Score spiegelt die Anfälligkeit und den Ausnutzungsgrad der Sicherheitslücke wider. Dementsprechend werden Priorisierungen und Handlungsempfehlungen ausgegeben und das betroffene Gerät in ein vorhandenes Quarantäne-VLAN verschoben. In diesem gesicherten Bereich erfolgt die weitergehende Analyse der entdeckten Schwachstellen.

UNTERNEHMENSWEITE COMPLIANCE-RICHTLINIEN

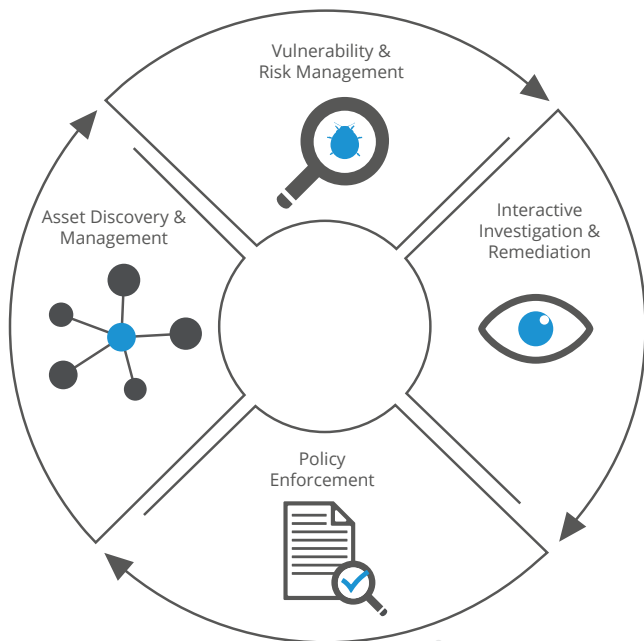
Mit definierbaren Policy Enforcements zur Herstellung der Geräte-Compliance wird die Befolgung der Unternehmensrichtlinien gewährleistet, bevor der Zugang zum Unternehmensnetzwerk bereitgestellt wird.

INTEGRATION IN DIE NETZWERKUMGEBUNG

Die Bereitstellung und Nutzung des AGENTS innerhalb der ARP-GUARD Lösung erfolgt „on-the-fly“. Durch die schnelle Inbetriebnahme und einfache Integration wird das operative Tagesgeschäft nicht beeinflusst.

PROZESSKETTE DER LÖSUNG

Die grafische Übersicht zeigt die vier Kernbereiche auf und stellt die strukturelle Funktionsweise der Lösung dar.



MEHRWERTE DER ERWEITERUNG

Der ARP-GUARD erweitert das Leistungsspektrum der Netzwerkzugangskontrolle, um eine optimierte Lösung zur granularen Analyse und Administration sämtlicher IT-Assets. Diese Konstellation bietet die vollständige Absicherung der Netzwerkumgebung mit einer tiefgehenden Risikoanalyse sämtlicher Endgeräte. Dies ermöglicht den Betrieb von bestehenden IT-Infrastrukturen nach höchsten IT-Sicherheitsstandards.

IHRE VORTEILE AUF EINEN BLICK

- Detaillierte Auswertung der Endgeräte für eine bessere Klassifizierung innerhalb der Netzwerkumgebung
- Risikobasiertes Schwachstellenmanagement
- Datenerfassung und -verarbeitung in Echtzeit
- Durchsetzung von Compliance-Standards auf den Endgeräten in Echtzeit
- Standardisierte und individuelle Abfragen (OSquery) und Skripte (Batch, Bash und weitere) ausführbar
- Kompatibel zu Geräten mit Microsoft Windows, Apple macOS, Linux Derivate, Server und IoT-Devices (clientless)
- API-Schnittstelle zur automatisierten Datenübermittlung