NetAttest LAP One
Sicher und geschützt in drei Schritten

Soliton Systems

Unbekannte Geräte sind unkalkulierbare Risiken

“Irgend Etwas” ist mit Ihrem Unternehmensnetzwerk verbunden!?

In unserer zunehmend vernetzten Welt können Endgeräte immer einfacher in unsere Netze gelangen.

Das mag angenehm und praktisch sein, birgt aber erhöhte Risiken in Bezug auf die Verbreitung von Viren und Malware und entstehende Datenlecks, wenn unautorisierte Geräte oder illegale Wireless Access Points in Ihr Netzwerk gebracht werden.

Zur Vermeidung solcher Risiken und um das Firmennetzwerk sicher und geschützt zu halten, ist es wichtig, nicht autorisierte und illegale Zugangsversuche zu blockieren.

Beeinträchtigung der Geschäftsabläufe

Gefahr von Datenverlust

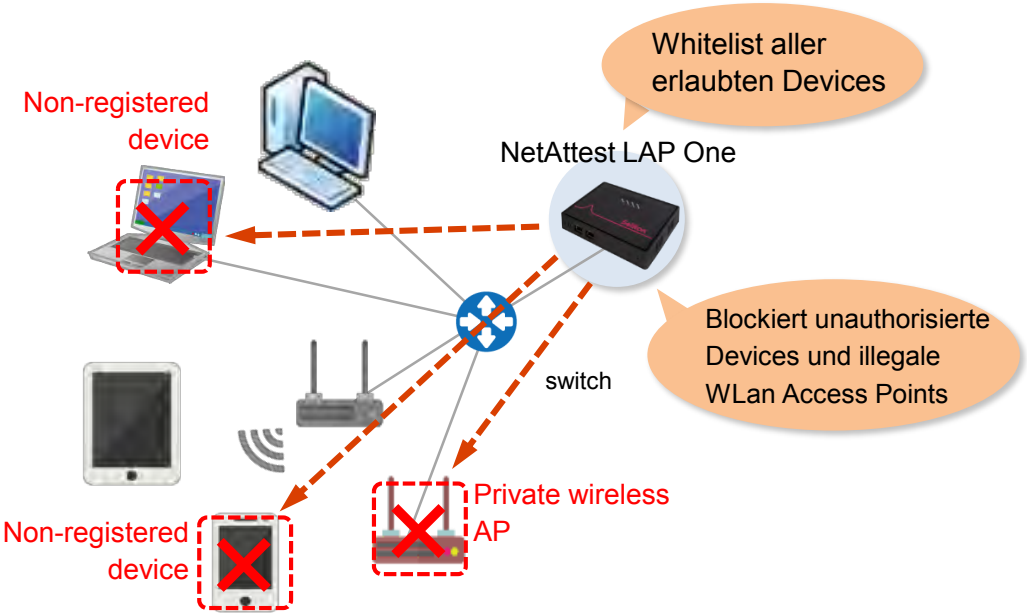
Beschädigung von Instanzen

NetAttest LAP One

Einfaches Setup einer Device Blocking Appliance

NetAttest LAP One ist eine Plug & Play Appliance zum Schutz vor Schäden und Gefahren, die durch unautorisierte Geräte im Firmennetzwerk verursacht werden könnten.

NetAttest LAP One erkennt und blockiert unbekannte MAC-Adressen neuer Devices innerhalb des überwachten W(Lan) Segments. Neue, berechtigte Geräte können schnell und einfach freigegeben werden, unberechtigte Geräte bleiben dauerhaft blockiert.



Einfach
Plug & Play
Installation & Betrieb

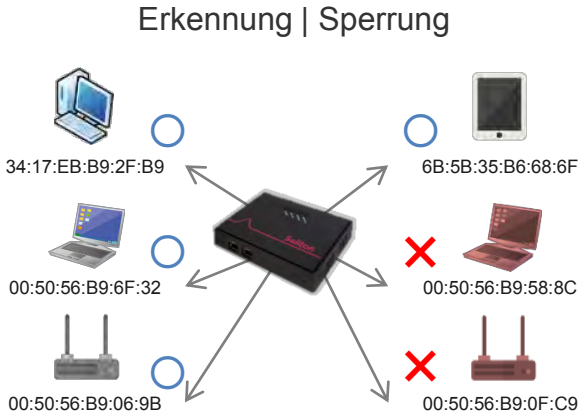
non invasiv
Keinerlei Modifikationen im Intranet erforderlich

Kosten-günstig
Segmentüberwachung für bis zu 512 Devices zu geringen Kosten

NetAttest LAP One: „Safe and Secure“

Kein Access für unautorisierte Devices

- **Erkennt viele Gerätetypen netzwerkfähiger, kabelgebundener oder kabelloser Devices**
  - Unterstützt Geräte mit statischer IP, DHCP, über LAN Kabel oder per WiFi
  - Erkennt die MAC-Adresse *1 des Geräts
    ※ Erkennung erfolgt anhand der ARP *2 bzw. DHCP Anfrage des Devices
- **Sperrung über “white list” Kontrolle**
  - Die white list kann automatisch (Lernmodus) oder manuell oder durch Datei-Import erstellt werden
  - Im “nur-Erkennungs-Modus” findet eine Erkennung aller Endgeräte ohne Sperrmaßnahmen statt. Dies dient zu Analysezwecken
    ※ Die Sperrmaßnahmen erfolgen in Form eines “ARP cache poisoning”*3
- **Werte und Limite**
  - Maximale Anzahl MAC Adressen: 512
  - Eine NetAttest LAP One Appliance kann zwei Netzwerk Segmente überwachen (Voraussetzung = eine gemeinsame “white list”)



*1 MAC Adresse: Eine physikalische Adresse zur eindeutigen Identifikation von Netzwerk HW-Komponenten (allgemeingültig)

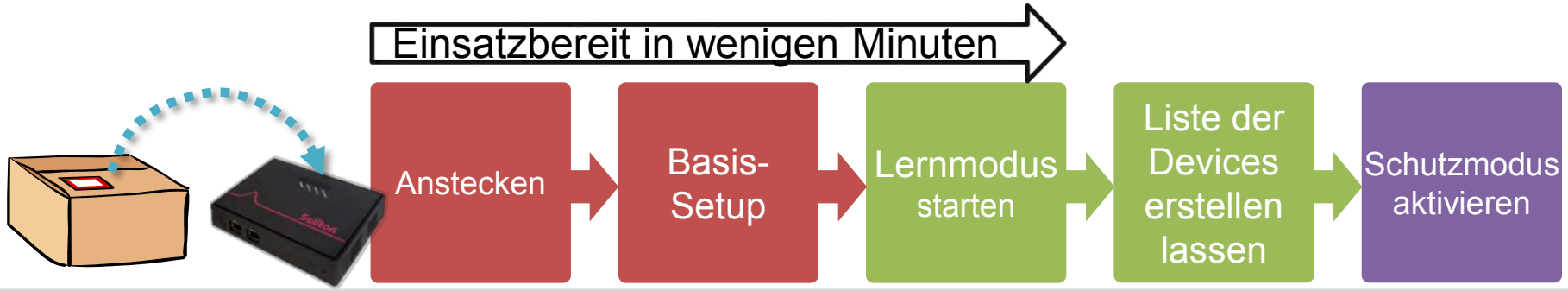
*2 ARP Protokoll: setzt IP-Adressen in Hardware- und MAC-Adressen um. ARP Anfragen werden per Broadcast gesendet.

*3 ARP cache poisoning : Täuschung. Vermittelt dem „Eindringling“ falsche Antworten auf seine ARP Anfrage. Damit ist keine gültige Zuordnung zwischen MAC- und IP- Adresse möglich und kann kein Netzwerkprotokoll initiiert werden.

„Safe and Secure“ in drei Schritten

Plug & Play Security

1. **Appliance an einen freien LAN Port anschliessen**
   - Basiskonfiguration (Passwort, IP Adresse und SMTP Anbindung)
   - Ansonsten sind keine weiteren LAN-Maßnahmen erforderlich
2. **“Lernmodus” aktivieren**
   - Erfasst die MAC Adressen und Devices im spezifischen (W)Lan
3. **Wechsel in den “Schutzmodus”**
   - Erfolgt entweder automatisch nach Zeitvorgabe oder manuell.
     Ab dann erhalten nur noch zuvor “gelernte” Devices Netzwerkzugang.
     (neue, zusätzliche Devices müssen explizit freigegeben werden)



Hardware Specifikationen

NetAttest LAP One

Model : LAPO-MX02

Product	NetAttest LAP One (LAPO-MX02)
Product number	LAPO-MX02
Max MAC addresses # to moniter※1	512 addresses
Network interface	10/100/1000BASE-T Auto MDI/MDIX x 2 port
Configuration method	Web browse (Internet Explorer 11, Chrome)
External dimensions	(w)155 x (H)32 x (D)120 (mm)
Max power consumption	24VA
Heating value	81.8 BTU/h、20.6 kcal/h
Weight	240g (excluded accessories)
Operating temperature	0℃～40℃
Operating humidity	20～80%
Compatible Standards	VCCI(ClassA), FCC(Class A), CE(Class A), RoHS,

Herstellerangaben