DATASHEET

NetSHIELD

NANO 25/100/254

Branch PRO

Enterprise 10/100/250

Proaktivní prevence nad pozdní detekci a nápravu

Převezměte kontrolu nad svou sítí

NetSHIELD, díky automatickým auditům a identifikaci známých zranitelností, poskytuje nástroj pro kontrolu slabých míst ve vaši síti. Přináší také ochranu proti šíření škodlivého Malware, Ransomware i Phishingu. V neposlední řadě nabízí další generaci řešení pro řízení přístupu mobilních i pevných zařízení. Poskytuje tak důležité funkce do řetězce zabezpečení. Získáte přehled a kontrolu nad nedůvěryhodnými síťovými aktivitami prostřednictvím dynamického řízení všech zařízení v síti. NetShield je non-inline zařízení, což zajišťuje, že může být připojen kdekoliv a odhalit a zajistit problém odkudkoliv.

Zabezpečte svou síť zevnitř ven

NetSHIELD přináší bohatou sadu funkcí bez-agentního Network Access Control (NAC) a kritické zabezpečení vnitřní sítě, které firewally a antivirová řešení neobsáhnou a kde dochází k 95% dnešních narušení. Pre-Cognition Engine NetSHIELD je navržen tak, aby karanténa koncového bodu předcházela infekci. Patentovaný mechanismus zajišťuje jeho umístění do karantény s nulovým výskytem false-positive chyb. Víme, že 99 % případů prolomení do systému bylo uskutečněno na základě již známé zranitelnosti! Díky NetSHIELDU máte přehled o všech zranitelnostech vaší vnitřní sítě a řádově tak zvyšujete svou bezpečnost.

Klíčové vlastnosti:

- Jednoduché nasazení a správa
- Správa lokálních i vzdálených zařízení z jedné konzole
- Zabezpečení kombinací funkcí detekce, blokace a karanténa
- Stabilní, efektivní a optimální platforma
- Agentless & Non-inline, zapojení kamkoliv, objevení a zabezpečení odkudkoliv
- Vysoce škálovatelné: pro sítě od 25 do tisíců zařízení
- Prosazení komplexní shody, audit a identifikace CVE
- Malware databáze aktualizována každé 3 hod ~ karanténa Apts & Zero-Days
- Zero-hour malware a phishing karanténa – prevence ransomware
- Vulnerability assessment a patch management
- Vykazování shody s bezpečnostními standardy
- TLD blokování & Detekce MAC spoof

Technické údaje:

(**typy zařízení:** NANO 25, NANO 100, NANO 254, Branch PRO, Enterprise 10, Enterprise 100, Enterprise 250)

Deployment Time:
15 min až 4–8 hodin (dle typu zařízení: 15 min, 30 min, 40 min, 40 min, <1 h, 1–2 h, 2–x)

Protected Assets per Site:
25 až 10 000 (dle typu zařízení: 25, 100, 254, 500, 1 000, 2 000, 4 000)

Počet Ethernetových portů:
2- mix (dle typu zařízení: 2, 2, 2, 3, 5, 7, 9)

802.1q VLANs:
15–200 (dle typu zařízení: 15, 15, 15, 30, 45, 75, 105)

Command Center:
od verze Enterprise 10

Manageable Sites per Command Center:
10–1 000 (dle typu zařízení: -, -, -, -, 10, 100, 250)

Funkce:
Dynamic Block Engine, MAC& IP Spoof Blocking, Malware and Phishing Quarantine, Compliance Enforcement, Vulnerability Assestment, Auto Device Discovery & Inventory Alerting, Command Center

NETSHIELD

NetSHIELD

Americká společnost se zabývá vyplňováním bezpečnostních mezer. Proaktivní řešení poskytuje efektivní ochranu v reálném čase před nejnovějšími metodami kyber útoků, včetně „Zero-Hour" útoků, phishingových útoků, šifrování a ransomware. Zajistí přístup do sítě pouze důvěryhodným zařízením.
NetSHIELD umožňuje IT odborníkům, aby znovu získali kontrolu nad svými sítěmi prostřednictvím účelnější správy a uplatňování bezpečnostní politiky. Dodává okamžitě použitelné řešení zahrnující vulnerability assessment a patch management.

VÁŠ PRODEJCE:

DISTRIBUTOR PRO ČR:

www.datacom.cz

VUMS DataCom spol. s r.o. | Komplexní řešení datových komunikací | Lužná 591 | 160 00 Praha 6 | tel: +420 220 999 511