15 února 2022

Zero Trust Security

Pavel Smolik

cisco

Pandemická situace zvýšila riziko kybernetických útoků

Nárůst kybernetických útoků během pandemie (2021)

Kybernetické útoky na národní cíle jako jsou zdravotnictví, WHO, burzy, utility a další kritickou infrastrukturu - nárůst o 500%

Bezprecedentní nárůst (3X) v Distributed Denial of Service (DDoS) útocích, phishingu a ransomware, hlavním cílem jsou zaměstnanci pracující vzdáleně(homeoffice)

Útočníci se soustředí na mobilní zařízení, používají škodlivé podvržené aplikace a pokouší se obejít bezpečnost tvořenou Mobile Device Management nástroji

S přechodem do cloudu se navýšily útoky na aplikace a data v cloudu. Útočníci používají cloudovou infrastrukturu pro ukládání a šíření škodlivých dat

Source: Kapersky; Checkpoint Research; Microsoft; Security Magazine; Press Search; WHO; Cisco Analysis

Zero Trust Security - hlavní otázky

Obáváte se bezpečnostních hrozeb a útoků na vaši organizaci?

Máte dotatečně zabezpečený vzdálený přístup k firemním datum pro zaměstnance na homeoffice? Jsou zaměstnanci proškoleni, aby uměli reagovat na běžné kyber. hrozby a útoky?

Jak máte zabezpečený přístup k aplikacím a datům v cloudu?

Jak chráníte zařízení vašich zaměstnanců doma a na pracovišti? Máte stejnou úroveň bezpečnosti?

Používáte zero trust principy při ochraně identity, aplikací a přístupu do sítě v celé vaší organizaci?

Source: Cisco Analysis

Vybudujte odolnou distribuovanou infrastrukturu

Zaměstnanci a IoT

Přechodná pracovní místa

Pobočky a kanceláře

Homeoffice

Zařízení a IoT

SMB
Enterprise
Veřejná správa

Bezpečná infrastructura pro organizaci

Práce bezpečně a odkudkoliv

Umožňuje používat jakákoliv zařízení

Správa sítě a zařízení odkudkoliv: Visibility, Automation, Analytics

Maximalizace uživatelské zkušenosti a produktivity

Connectivity | Zero Trust Security | Cloud Services | Collaboration

Visibility | Au

Distribuované Aplikace a Cloudové služby

Datacenter

Public Cloud

Hybrid Cloud

SaaS / VDI

Aplikace
Cloud
On Premise

Source: Cisco Analysis

Cisco implementace Zero Trust => pro 60 tis. zaměstnanců

Zabezpečení budujeme ověřováním:

- ✓ Identity uživatelů & zařízení
- ✓ Ověřením zranitelností
- ✓ Zabezpečení všech aplikací/služeb
- ✓ Sledujeme všechny hrozby

Vynucujeme přístup s oprávněními k:

- ✓ Aplikacím
- ✓ Síťovým prvkům
- ✓ K interním datům i cloudu
- ✓ Pravidla plati pro všechny uživatele i administrátory

Průběžně ověřujeme:

- ✓ Zda jsou principy a nástroje používané v bezpečnosti stále aktuální a účinné
- ✓ Zda jsme připraveni na nárůst datové komunikace
- ✓ Sledujeme jakékoli anomální nebo podezřelé činnosti
- ✓ Pokud dojde ke kompromitaci, okamžitě reagujeme

Zero Trust

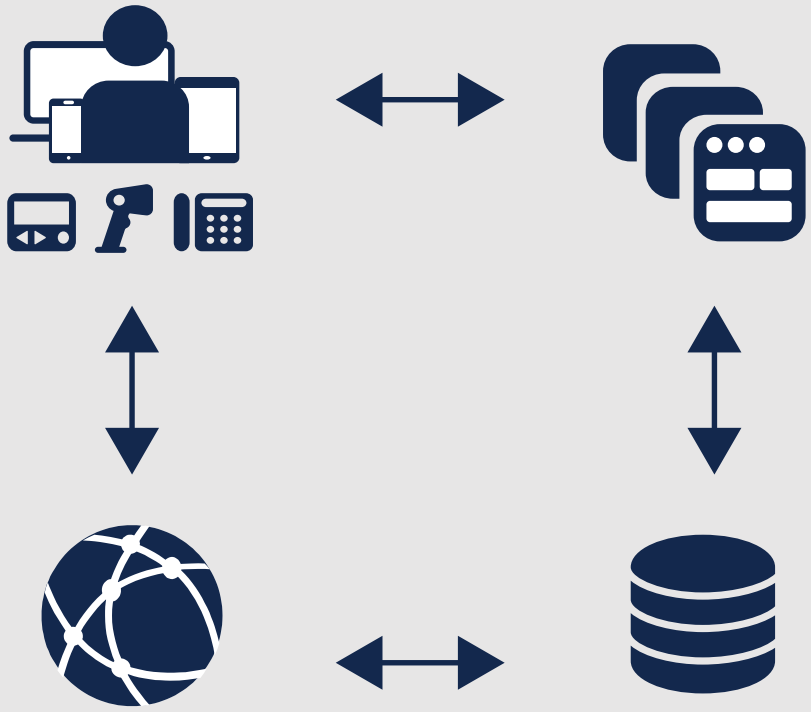
Řešení od Cisco

Cisco Zero Trust

Princip nulové důvěry = zabezpečení přístupu napříč aplikacemi a prostředím, od jakéhokoli uživatele, zařízení a pracoviště.

Workforce

Zajistěte, aby k aplikacím měli přístup pouze oprávnění uživatelé a zabezpečená zařízení.



Workplace

Zabezpečte všechny druhy připojení uživatelů a zařízení v síti, včetně IoT.

Workload

Zabezpečte připojení ke svým aplikacím v privátním i veřejném cloudu.

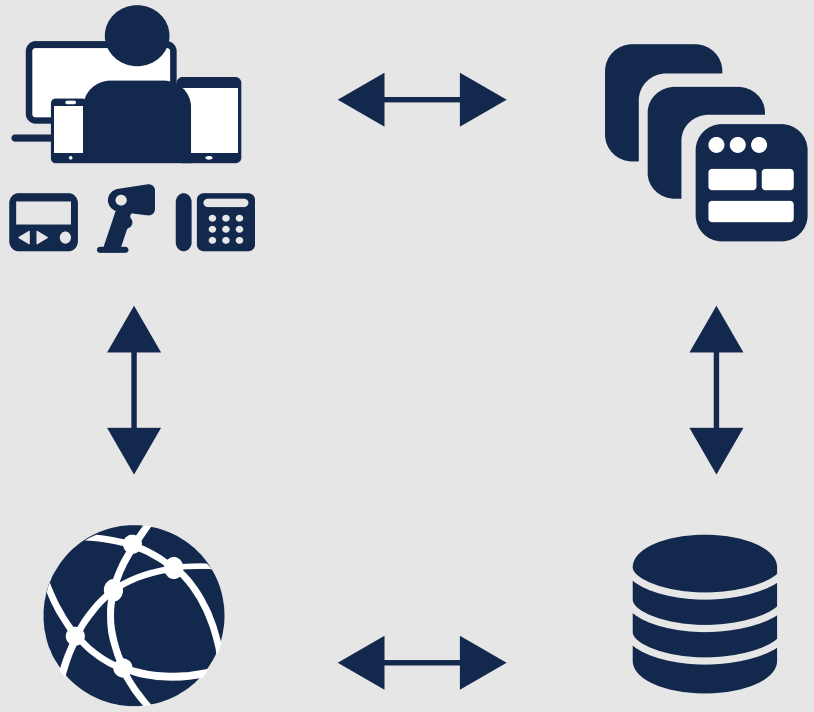
Enforce Policy-Based Controls

Cisco Zero Trust

Zabezpečte přístup pro vaše zaměstnance odkudkoliv a přes jakékoliv zařízení

Duo MFA zaměstnance

Zajistěte, aby k aplikacím měli přístup pouze oprávnění uživatelé a zařízení.



SD-Access pro pracoviště + ISE pro zařízení

Zabezpečte všechny druhy připojení uživatelů a zařízení v síti, včetně IoT.

Tetration Data a aplikace

Zabezpečte připojení ke svým aplikacím v privátním i veřejném cloudu.

Zero Trust pro zaměstnance

Hlavní hrozby

- Phishing
- Malware
- Krádež přihlašovacích údajů

Hlavní část řešení: Duo security

Díky Duo Security zajistíte, že k aplikacím budou mít přístup pouze oprávnění uživatelé a zařízení.

Doplňkové nástroje: Umbrella & AMP

Umbrella & AMP – tyto produkty zajišťují bezpečnost pro vzdálené uživatele a AMP také umožňuje aplikaci Duo přizpůsobit se novým hrozbám

Workforce: Establish Trust

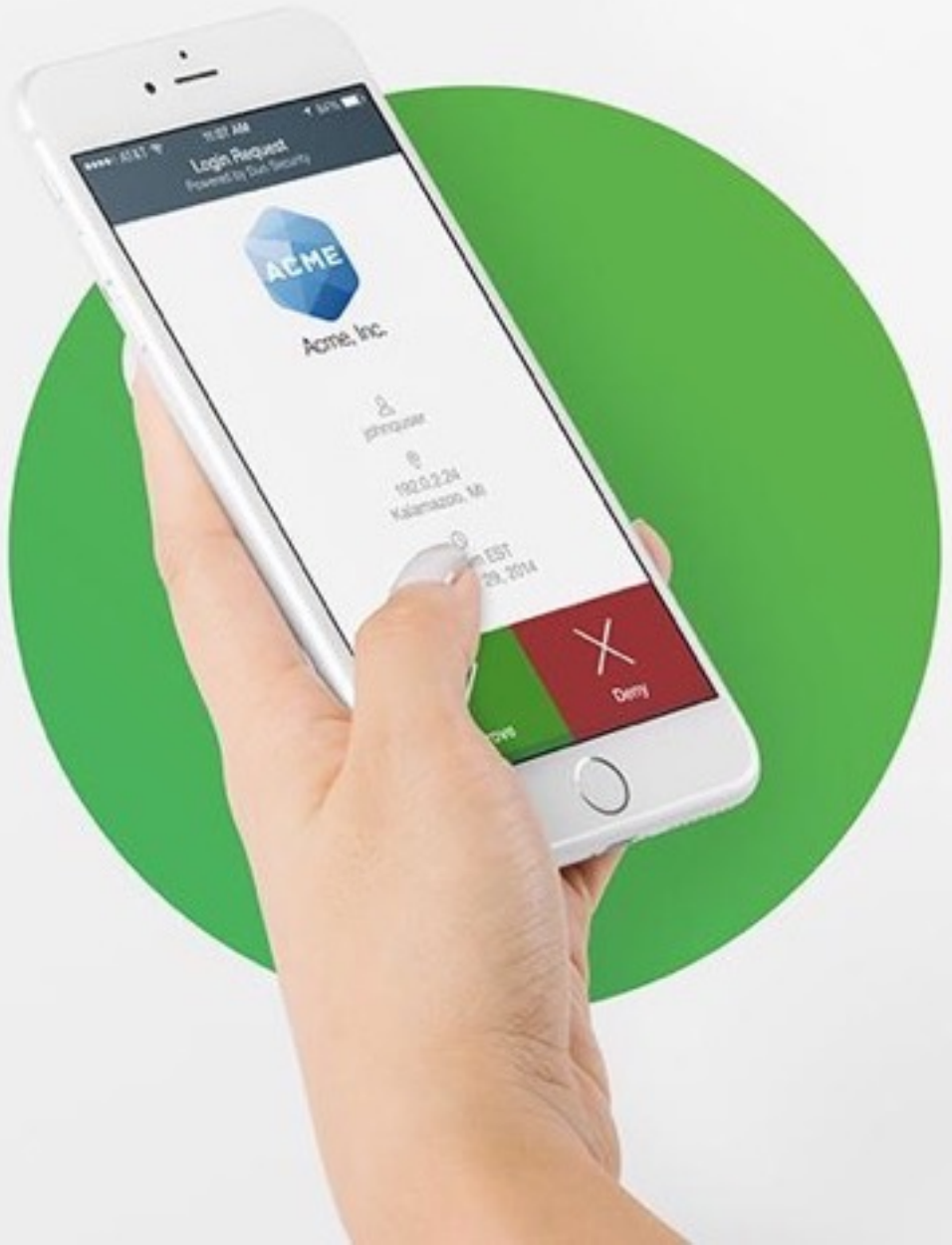
Ověření uživatele & zařízení

Duo's Multi-Factor Authentication (MFA)

- Uživatelé se ověří během několika sekund – schválení jedním klepnutím
- Škálovatelná služba, kterou lze nasadit během několika hodin
- Nativně se integruje se všemi aplikacemi

Device Trust

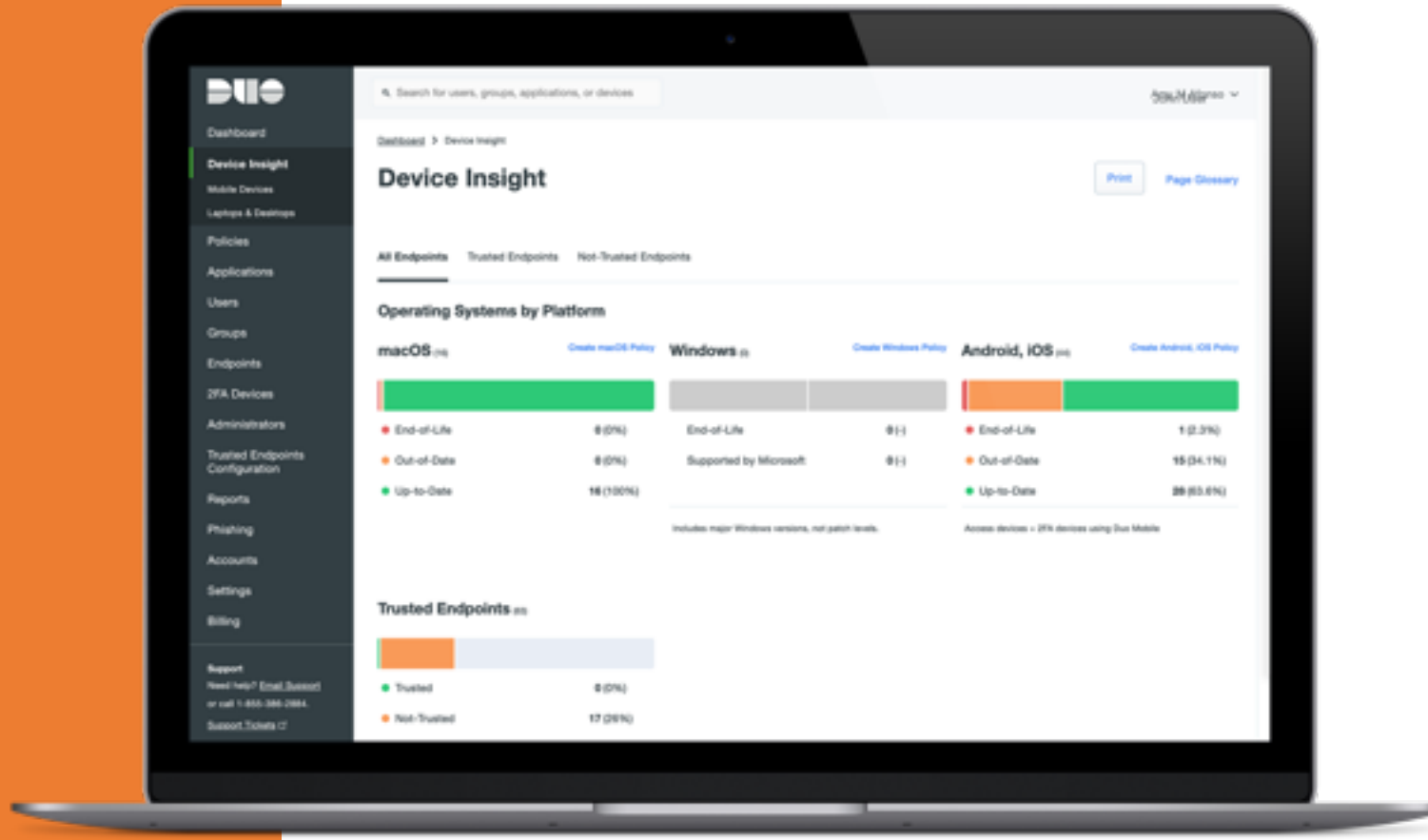
- Zkontrolujte, zda zařízení neobsahuje zranitelný software a bezpečnostní funkce
- Identifikujte spravovaná a nespravovaná zařízení
- Informujte uživatele o nepodporovaných typech zařízeních (out-of-date)



Monitoruj všechna zařízení a hrozby

Duo's Device Trust:

- Při každém přihlášení Duo kontroluje stav a stav zabezpečení zařízení uživatelů
- Duo detekuje spravovaná a nespravovaná mobilní a stolní zařízení
- Vynucuje zásady přístupu založené na ochraně vnitřní sítě před zranitelnými, neověřenými zařízeními



Use Case: Bezpečný přístup k aplikacím

Zákazníci často řeší:

- Jak zajistit bezpečný přístup ke cloudovým aplikacím
- Jak zajistit bezpečný přístup k interním aplikacím
- Jak dostatečně ověřit uživatele a jeho zařízení (spravované/nespravované)
- Jak zajistit ochranu před odcizenými nebo kompromitovanými přihlašovacími údaji
- Jak zajistit zjednodušené přihlášení pro všechny typy uživatelů

Protect VPNs:

- Duo secures AnyConnect thick client & SSL VPN
- Available on ASA & FTD

Ochrana všech aplikací

Start Here

Then Expand

VPN RA	Multicloud	Email/MSFT	On-Prem	SSO	Custom
Cisco	Google Apps	Office 365	Epic	Microsoft Azure	REST APIS
Juniper Networks	salesforce	Outlook	Oracle PeopleSoft	AD FS	WEB SDK
Citrix	aws	Microsoft Remote Desktop Services	vmware Horizon View	okta	RADIUS
paloalto Networks	box	Windows Server	>_SSH	Centrify	SAML
Pulse Secure	Dropbox	RRAS	Shibboleth	onelogin	OIDC

Detekce a ověření uživatelů & koncových zařízení

AnyConnect

- Získejte informace o zařízeních, operačním systému, rozhraní, podrobnostech datového toku
- Shromažďování telemetrie z modulu AnyConnect Network Visibility Module (NVM)
- Integrace s LDAP pro další uživatelský kontext

Identity Services Engine (ISE)

- Ověří typ zařízení (IP telefon, tiskárna atd.), uživatelská jména, polohu zařízení, atd.
- Umožňuje sběr informací o koncových stanicích z ISE
- Použití LDAP pro další uživatelský kontext

Network Visibility

SD-Access’s identity context zajišťuje:

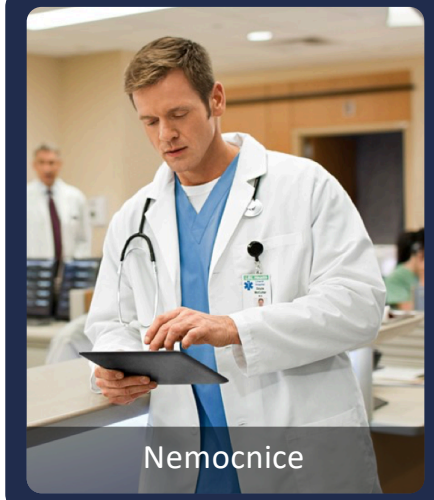
Viditelnost:

- Uživatelů a zařízení(IoT) v datové síti

Poskytuje informace o uživatelích a zařízeních včetně:
Autentifikace

- Ověření oprávnění přístupu
- Ověření zařízení

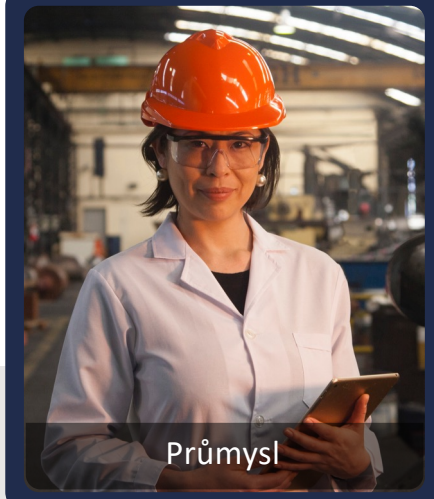
Use Case: kontrola přístupu uživatelů & IoT zařízení

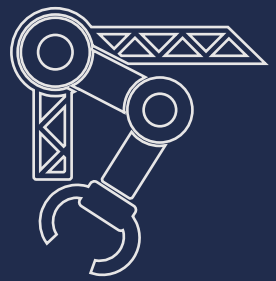


Zaměstnanci a
lékařské přístroje

250+ různých
zdravotnických zařízení

- Pharma-Smart-Device
- Philips-Analytical-X-Ray-Device
- Philips-CareServant-Device
- Philips-Healthcare-PCCI-Device
- Philips-Medical-Systems-Device
- Philips-Oral-Healthcare-Device
- Philips-Patient-Monitoring-Device
- Philips-Personal-Health-Device
- Philips-Respironics-Device
- Phonak-Communications-Device





Průmyslová zařízení

Cisco CyberVision

- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device

Cisco Zero Trust - Shrnutí

Cisco Zero Trust Architecture poskytuje kompletní řešení

Jaký problém zákazníci řeší?	Jak Cisco může pomoci:
Potřebuji ověřovat a spravovat jakákoliv zařízení a aplikace	Cisco SDA, Tetration, Duo
Potřebuji nasadit zero trust access control policy v celé organizaci	Cisco SDA, Tetration, Duo
Potřebuji průběžně ověřovat, zda jsou uživatelé, zařízení a aplikace zabezpečeni	Cisco SDA, Tetration, Duo

Cisco Zero Trust - přehled produktů

Umbrella

AMP

Meraki

AnyConnect

SD-WAN

Email Security

Next-Generation Firewall

ACI

+ Detect & Respond

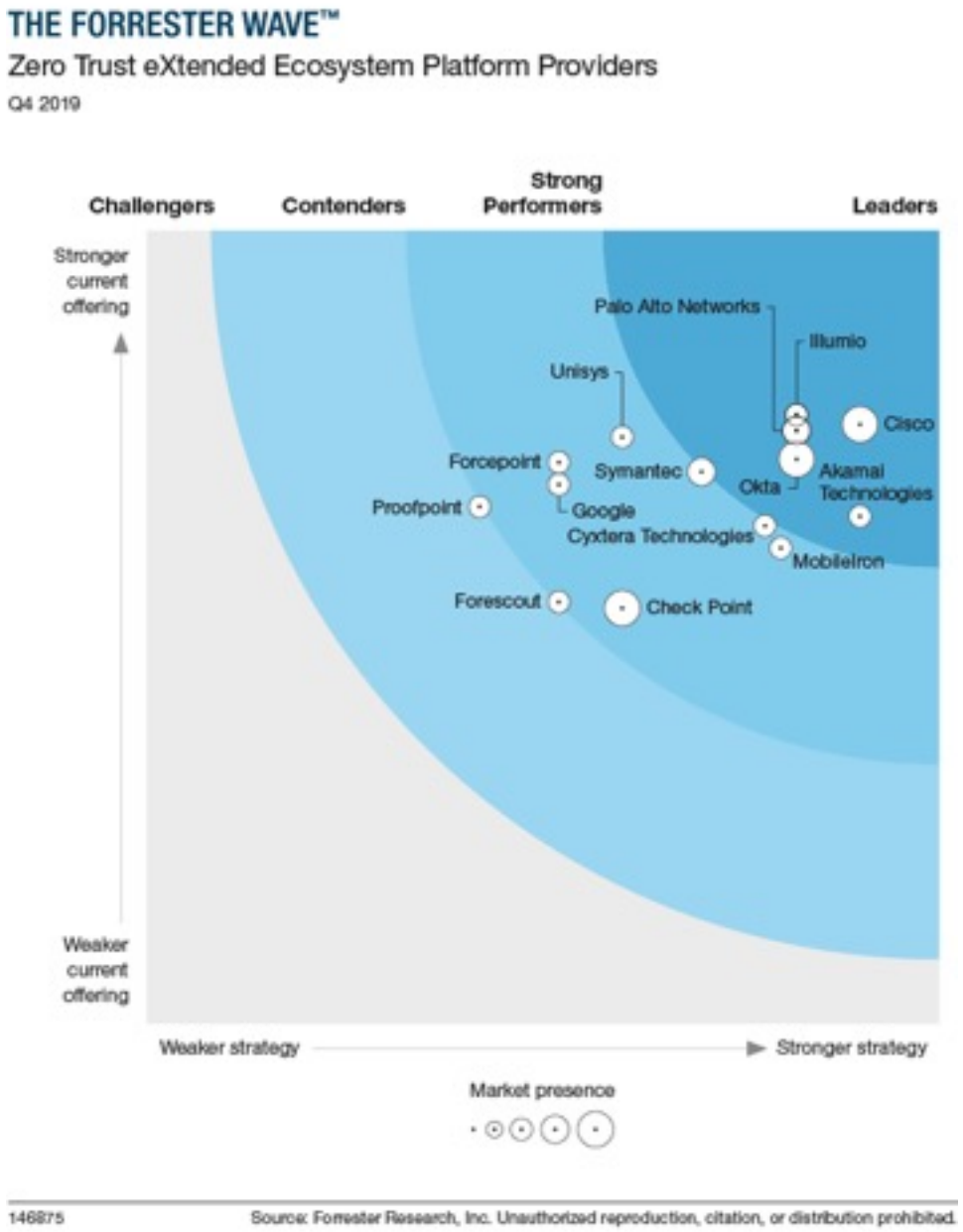
Cisco Threat Response (CTR)

Stealthwatch

Cisco byl označen Forrester Wave Zero Trust lídrem na trhu

“Cisco has adopted a zero-trust strategy and is well-positioned as a prominent zero-trust player.”

“Organizations seeking to enable Zero Trust as a long-term goal can get real benefits from choosing this vendor.”



The bridge to possible