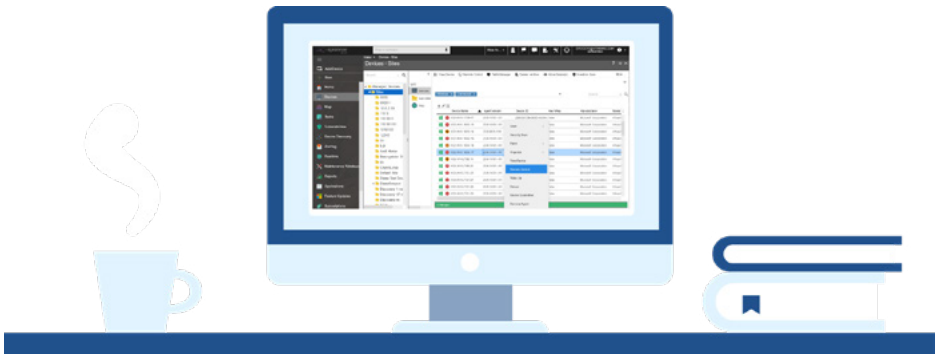
SYXSENSE

Úvod do Syxsense

Technologie Syxsense Endpoint Security Cloud always-on pracuje neustále v reálném čase 24/7/365 a je základním stavebním kamenem nástroje pro jednotnou správu a zabezpečení koncových bodů, UNIFIED ENDPOINT MANAGEMENT AND SECURITY (UEMS). Tato jedinečná technologie umožňuje fungovat bez výpadku, a to i v případě, že dochází k narušení bezpečnosti, které vždy ochromuje produktivitu a vystavuje organizaci finančním rizikům a poškození pověsti. Velká výhoda řešení Syxsense spočívá ve způsobu, jakým kombinuje sílu umělé inteligence s odbornými znalostmi v oboru a umožňuje spravovat a zabezpečovat koncové body tím, že včas zabrání zneužití hrozeb, nebo je alespoň ihned zneutralizuje.

Proč potřebuji chránit své koncové body?

Dnešní prostředí hrozeb je v důsledku COVID-19, následného přechodu na vzdálenou a hybridní práci a stále sofistikovanějších metod útoků kyberzločinců mnohem méně předvídatelné než kdykoli předtím. Vaše koncové body – notebooky, PC, servery, mobilní zařízení - jsou branou, kterou útočníci využívají k přístupu k firemním datům. Pokud své koncové body nechráníte vystavujete se riziku potenciálního útoku, a v konečném důsledku i finančním, reputačním a právním dopadům, které vám únik citlivých dat způsobí. Tyto dopady jsou navíc většinou nevratné a mohou vaši organizaci navždy zničit.



Řešení

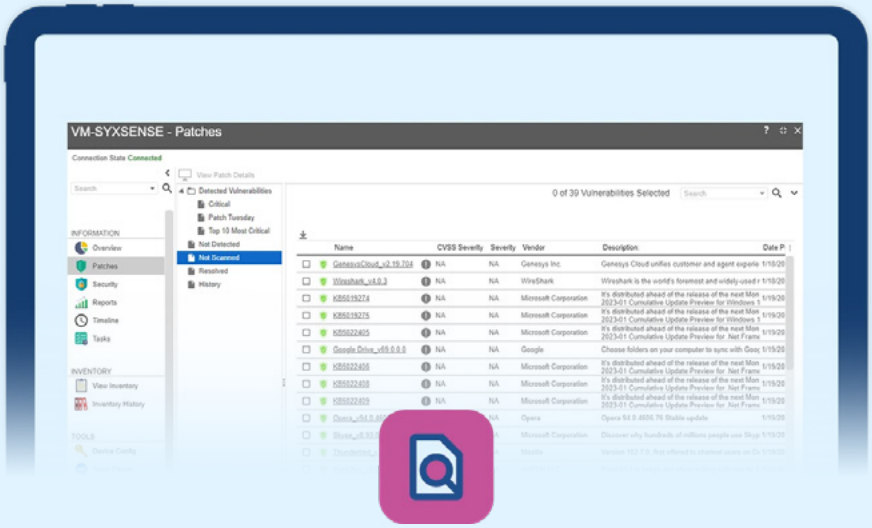
Pokročilý nástroj pro správu všech koncových bodů s širokou škálou využití na jakékoliv aplikace třetích stran. Odhalí zranitelnosti koncových stanic nebo serverů a vyřeší je z jediné konzole pomocí inteligentní automatizace a moderního přístupu Zero Trust.

Klíčové výhody

- Extrémně jednoduchý nástroj
- Komplexní řízení všech aplikací včetně třetích stran
- Automatizace formou patentované technologie Cortex
- Úspora lidských zdrojů / rychlá návratnost investice
- Razantní snížení bezpečnostních rizik
- Zajištění souladu s ISO 27001, HIPAA a samozřejmě ZoKB
- Aplikace NÚKIB doporučení v praxi

Portfolio řešení

Patch Management



Identifikujte své koncové body a pečujte o ně.

Vaše koncové body jsou branou, kterou útočníci využívají k přístupu k firemním datům. Pokud o ně dostatečně nepečujete, vystavujete se riziku potenciálního útoku a úniku dat, což může často vést k finančním, reputačním a právním důsledkům.

Minimalizujte plochu útoku!

Přesná detekce: Naše pokročilá logika detekce prohledá vaši síť a identifikuje zařízení s chybějícími aktualizacemi.

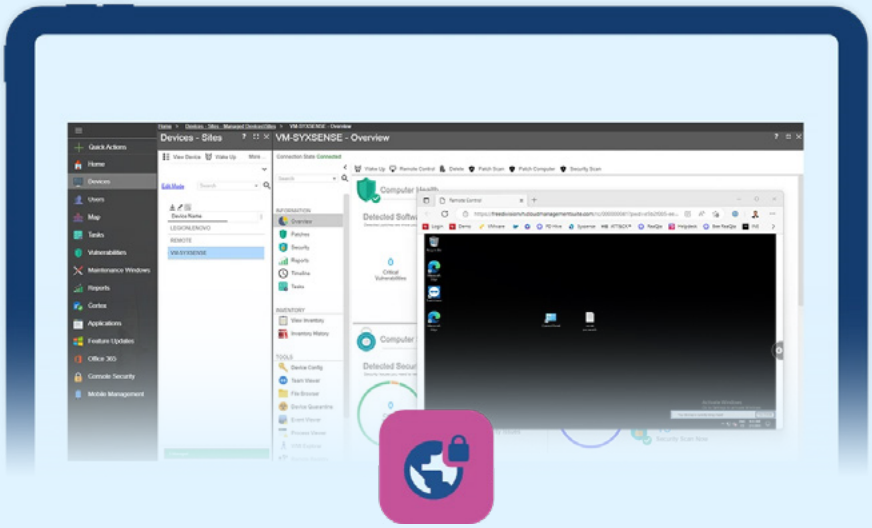
Rychlé nasazení: Zkraťte dobu mezi identifikací a lokalizací. Odhalte včas místo kritické hrozby a okamžitě nasaďte řešení.

Operační systém a třetí strany: Obsah našich záplat je každý večer upravován pomocí synchronizace s databází NIST a automatizovaného webového vyhledávače.

O nahrazování záplat, aktualizacích a Syxscore se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Remote Control



Přístup a kontrola odkudkoli a kdykoli

Sdílejte odkudkoli: Přistupujte k zařízení vašich zaměstnanců z libovolné vzdálenosti, ať jste kdekoli.

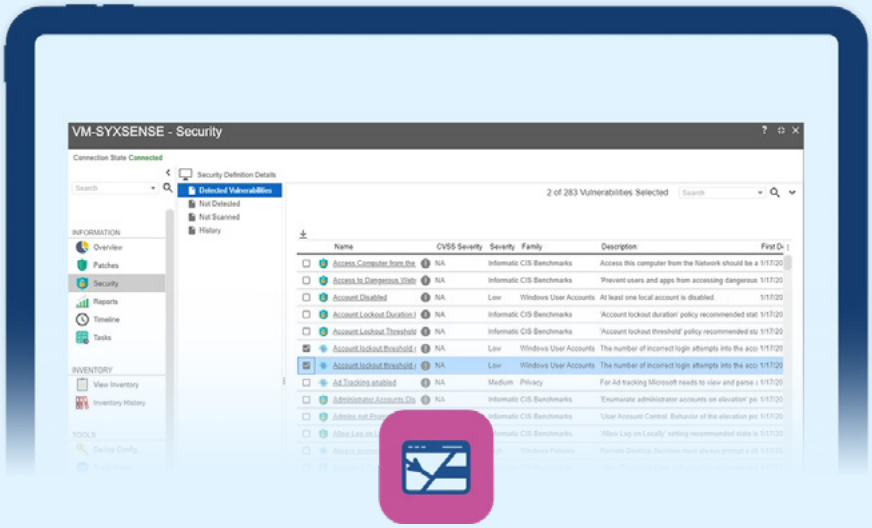
Vzdálené řešení problémů: Vyřešte jakýkoli problém, velký i malý. Sdílejte pracovní plochu, rychle identifikujte problémy a najděte řešení během několika minut.

Cloudová platforma: Zabezpečené cloudové připojení, které vám umožní vzdálený přístup k libovolnému zařízení.

O ovládání pomocí prohlížeče, přenosu souborů a skriptů nebo integraci s TeamViewer se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Skener zranitelností



Konfigurační omyly už pro vás nebudou kritické.

Náš sken vyhledá zranitelnosti ve vašem prostředí a pomůže vám určit jejich prioritu k nápravě. Neposkytujeme jen viditelnost, ale především velmi rychlé sjednání nápravy na 2 až 3 kliky.

Odhalte zranitelnosti: Najděte slabá místa a chyby v konfiguraci, kvůli kterým hrozí odcizení vašich citlivých dat nebo nežádoucí změna jejich stavu.

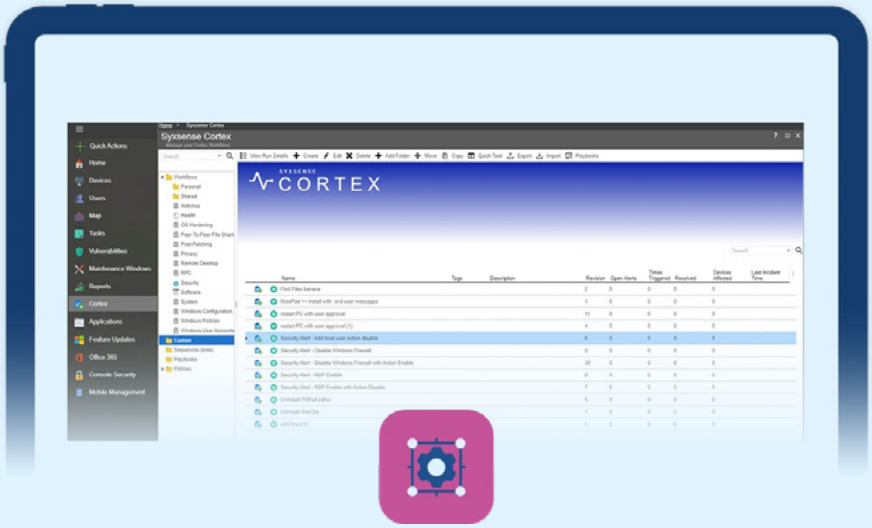
Snižte rizika: Převezměte zpět kontrolu nad dodržováním bezpečnostních předpisů na každém jednotlivém zařízení, které lidé ve vaší organizaci používají k práci.

Posílení detekce hrozeb: Zachytíme více než jen zranitelnosti operačního systému a třetích stran. Prohledejte konfigurace zabezpečení, jako jsou otevřené porty, stav antivirového programu, vypnuté brány firewall a další.

O databázii zranitelsnotí a možnostech upozornění na zranitelnosti se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Cortex – Workflows



Deployment aplikací nebyl nikdy snazší a bezpečnější.

Správně nastavená automatizace procesů přináší vždy více bezpečnosti do každé organizace. Je příjemné, aby vaši zaměstnanci pracovali s aktuálními nástroji a využívali je naplno.

Inteligentní koncové body: Cortex předává data o změnách chování a stavu koncových bodů v reálném čase, 24 hodin denně, 7 dní v týdnu, 365 dní v roce.

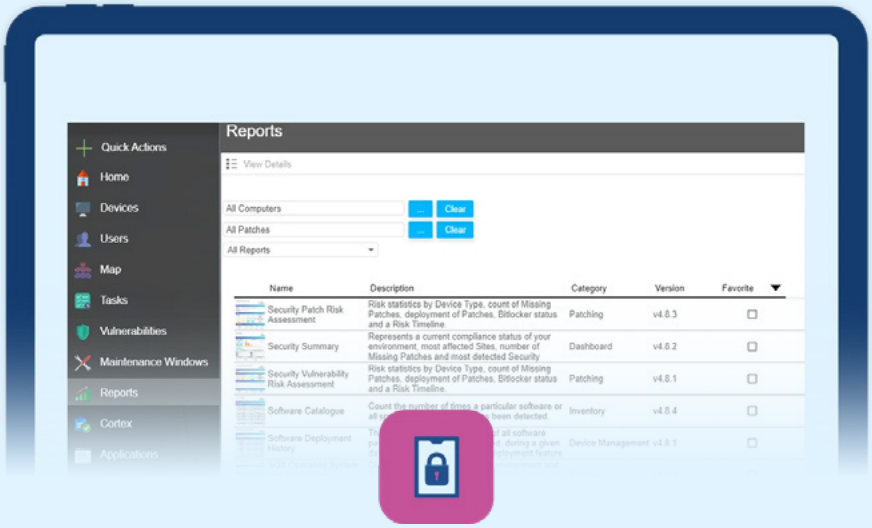
Využijte automatizaci: Vytvářejte pracovní postupy, které propojují procesy od začátku do konce, od detekce hrozeb až po jejich řešení.

Reakce na jedno kliknutí: Udělali jsme těžkou práci za vás. Získejte plný přístup k naší rozsáhlé knihovně předpřipravených pracovních postupů vedoucích k nápravě.

O reaktivních receptorech nebo o knihovně hotových pracovních postupů a jejich vizualizaci se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Soulad s předpisy – Compliance Reporting



Buďte v souladu s předpisy a prokažte shodu.

Chraňte citlivá data: Zajistěte, aby data zákazníků a společnosti byla získávána, ukládána, distribuována a zabezpečena v souladu s regulačními požadavky.

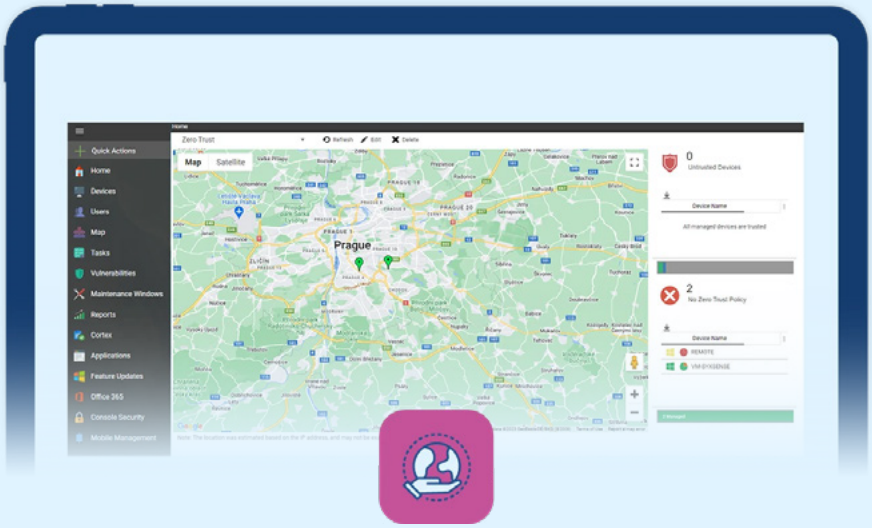
Prokažte shodu s předpisy: Vytvářejte vždy aktuální zprávy o shodě pro audity regulačních orgánů,protože normy se mění a vyvíjejí.

Předcházejte incidentům: Předcházejte finančním postihům, ztrátě reputace nebo dokonce zákazníků a drahým soudním sporům pomocí automatizovaných procesů a hlášení.

O strategii dodržování předpisů a průmyslových regulacích se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Nulová důvěra - Zero Trust



Odstraňte hrozby dříve, než budou zneužity.

Odhalte zranitelnosti koncových stanic nebo serverů co nejdříve pomocí aplikace principů nulové důvěry. Snadno je pak vyřešíte z jediné konzole pomocí inteligentní automatizace.

Nemůžete důvěřovat žádnému koncovému bodu!

Odborné vzdělávání a výcvik: Předpokládejte, že v síti existují útočníci.

Ověřovna: Zkontrolujte stav zabezpečení uživatelů i zařízení.

Důvěřuj, ale prověřuj: Přehodnocujte důvěryhodnost při každém pokusu o přihlášení a přístup.

O přístupu nulové důvěry a vynucování hodnocení důvěryhodnosti se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Automatizace nápravných opatření

Rychleji odstraňte více hrozeb.

Pohodlně automatizujte veškerá nápravná opatření v okamžiku, kdy jsou hrozby zjištěny. Později bez stresu jen zkontrolujte, k čemu došlo během vaší nepřítomnosti.

Eliminujte hrozby: Nedovolte útočníkům získat kontrolu nad vašim prostředím díky automatizaci správy zranitelností.

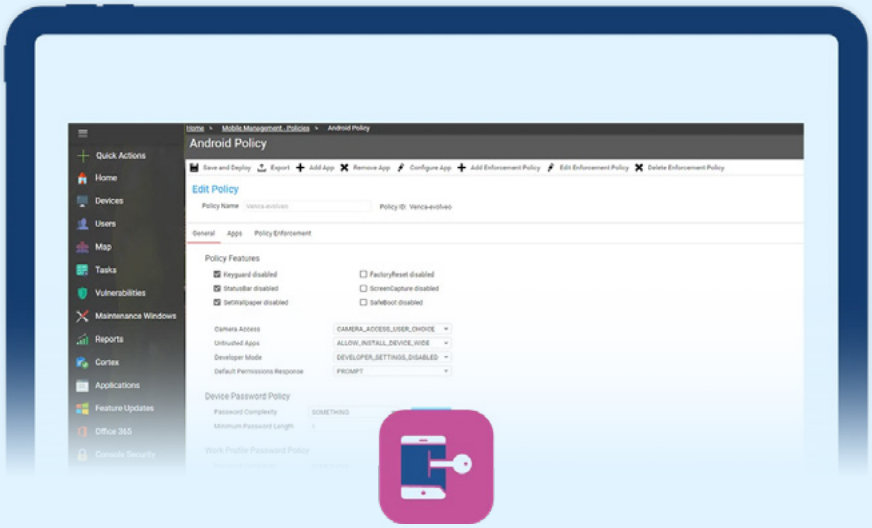
Rychlejší náprava: Zkraťte lhůty pro nápravu kritických bezpečnostních zranitelností a aplikujte záplaty v řádu hodin od jejich vydání.

Omezte škody: Vyhněte se narušení provozu, poškození pověsti a rostoucím nákladům, které jsou způsobené únikem dat.

O dynamickém dotazování, karanténě, úkolech, údržbě a odstávkách systému se více dozvíte na našem

CHCI VĚDĚT VÍCE

Mobile Device Management



Správa, konfigurace a zabezpečení mobilních zařízení

Pracujte kdekoli: Umožněte zaměstnancům bezpečně pracovat s firemními zdroji z jakéhokoli zařízení, včetně jejich vlastního.

Zabezpečení na dálku: Uzamykejte, resetujte a vymazávejte mobilní zařízení z konzole Syxsense bez ohledu na jejich umístění.

iOS a Android: Podpora správy mobilních zařízení pro zařízení iPhone, iPad a Android. firewall a další.

O zabezpečení mobilních zařízení a kontejnerizaci dat se dozvíte více na našem webu.

CHCI VĚDĚT VÍCE

Závěr

Řešení UEMS od výrobce Syxsense poskytuje 100% přehled o vašem prostředí, možnost detekovat hrozby v reálném čase a spravovat a zabezpečit každé zařízení z jediné konzole. Díky Syxsense máte k dispozici kompletní informace o koncových bodech a nápravu hrozeb bez ohledu na operační systém nebo umístění, včetně lokálních, vzdálených, roamingových a cloudových zařízení.

Licencování

Syxsense Manage

- Cloud-Based Architecture
- Discovery Agent
- Device Management
- Inventory History & Audit Logs
- Patch Scan
- Patch Management (OS & Third-Party)
- Software Distribution
- Office 365 App Provisioning
- Active Directory Integration
- Remote Control
- Maintenance Windows & Blackout Hours
- Dynamic Patch Tuesday Windows
- Reboot Management
- Windows 10 Feature Update Management
- SyxScore
- Ansible Workflows
- Device Location Maps
- Custom Data Fields
- Supercedence by Default
- Custom Data Fields
- Wake-on-LAN
- Reporting
- Customizable Dashboards
- User Management & Scoping
- Troubleshooting Tools
- Add On: MDM

Syxsense Secure

Vše z Syxsense Manage a navíc:

- Cortex Drag & Drop Workflow Builder
- Policies
- Security Vulnerability Scan
- Security Vulnerability & Content Management
- Configuration Management
- Quarantine
- Threat Alerts
- Real-Time Views & Actions
- Network Map with Device Health
- IoT Discovery
- Device Timeline
- nMap
- Proof of Compliance (HIPAA, PCI, SOX)
- Add On: MDM

Syxsense Enterprise

Vše z Syxsense Secure a navíc:

- Zero Trust
- 24/7 Intelligent Automation
- Security Remediation
- Cortex Workflow Script Library
- MDM
- Open API
- Data export for SIEM

O společnosti Syxsense

Společnost Syxsense Inc. založena v roce 2012 se sídlem v Newport Beach v Kalifornii je celosvětový lídr v oblasti jednotné správy koncových bodů a jejich zabezpečení.
Výrobce je předním poskytovatelem inovativní cloudové technologie, která poskytuje hlubokou viditelnost s detaily o každém koncovém zařízení, na každém místě, všude uvnitř i vně sítě a také v cloudu.
Nyní již s více než 500 dlouhodobými enterprise zákazníky s počtem koncových bodů od 100 do 100 000 poskytuje různá řešení pro organizace všech velikostí i pro poskytovatele služeb (MSP). Značka Syxsense je synonymem prvního poskytovatele bezpečnostních IT řešení na světě, který nabízí správu záplat, skenování zranitelností a zabezpečení koncových bodů včetně mobilních zařízení v jediné konzoli.

O společnosti FreeDivision

IT bezpečnosti se věnujeme více než 17 let a stále je naším koníčkem. Vyhledáváme to nejlepší z oblasti bezpečnosti a ochrany dat. Zastupujeme několik celosvětově renomovaných výrobců a jejich řešení vám exkluzivně přinášíme spolu s týmem proškolených profesionálů a konzultačními službami.

FREEDIVISION
for safety reasons

FREEDIVISION S.R.O.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

OBCHOD
assistant@freedivision.com
+420 220 972 426

TECHNICKÝ KONTAKT
ngsoc@freedivision.com
+support.freedivision.com

FREEDIVISION.COM

THE FUTURE OF ENDPOINT SECURITY