Příloha č. 1 Zadávací dokumentace – Technická specifikace a popis nabízeného řešení, též Příloha č. 1 Kupní smlouvy

SYSTÉM PRO OCHRANU PROTI ŠKODLIVÉMU KÓDU VČETNĚ DETEKCE A REAKCE V KONCOVÝCH BODECH

POPIS STÁVAJÍCÍHO STAVU

Zadavatel provozuje antivirové řešení, které již nenaplňuje zvýšené potřeby kybernetické ochrany koncových bodů a ochrany provozu jeho informačních systémů.

Zadavatel má zájem implementovat nové funkcionality ochrany jeho infrastruktury a zejména zlepšit visibilitu aktivit uživatelů, které mohou vést k infikování koncových stanic.

Zadavatel chce v rámci projektu nasadit řešení, kterým jde jednoduše sledovat podezřelé chování uživatelů a zařízení, provést jejich rychlou analýzu příčiny problému a detekci zdroje infekce.

POŽADAVKY NA NOVÉ ŘEŠENÍ

Požadujeme zabezpečení ochrany koncových stanic a ochranu organizace před ztrátou informací pro 1600 koncových stanic, 100 serverů a 400 mobilních zařízení (mobilní telefony, tablety). Požadujeme plně funkční řešení po dobu 6 let.

Zadavatel považuje ochranu koncových zařízení za jednu z klíčových oblastí při boji proti kybernetickým hrozbám. Požadavky na ochranu koncových zařízení v segmentu zdravotnictví a pro organizace velikosti a významu Zadavatele se výrazně liší od požadavků menších firem či samozřejmě individuálních zákazníků. Zadavatel klade důraz na nepřetržité vyhledávání pokročilých hrozeb, identifikaci útoků v úvodních fázích a automatickou eliminaci hrozeb a rizik s využitím prvků umělé inteligence bez závislosti na využití známých signatur škodlivého kódu. Zadavatel v této oblasti fokusuje na dodávku technologicky nejvyspělejších řešení a preferuje nabídky na dodávky takových platforem/systémů, které jsou v době vypsání této veřejné zakázky umístěny (figurují) v kvadrantu Leaders v posledním hodnocení Gartner Magic Quadrant for Endpoint Protection Platforms.

TECHNICKÉ, FUNKČNÍ A INTEGRAČNÍ POŽADAVKY

Požadavky	Splňuje (Ano/Ne)	Stručný popis, jakým způsobem nabízené řešení splňuje daný požadavek (je možné doložit i konkrétním odkazem na

		přiloženou část nabídky, kde bude možné ověřit naplnění daného parametru)
Navrhované řešení musí podporovat: • Windows 10, • Windows 11 (64-bit), • Windows 2012 R2 (64-bit) a novější, • MAC OS, Linux distribuce Centos 7 a vyšší, • Debian 9 a vyšší.	ANO	Podpora Windows OS je rozdělena do 3 skupin: Group 1: • Windows 11 64-bit • Windows 10 64-bit • Windows 8.1 64-bit • Server/Storage Server/Server Core 2022 64-bit • Server/Server Core 2019 64-bit • Server/Storage Server/Server Core 2016 64-bit • Server/Storage Server 2012 R2 64-bit Group2: • Windows 10 32-bit • Windows 8.1 32-bit • Windows 8 32/64-bit • Windows 7 SP1 32/64-bit • Server/Storage Server/Server Core 2012 (not R2) 32/64-bit • Server 2008 R2 SP1 32/64-bit Group3: • Windows Vista SP2 32/64-bit • Windows XP SP3 32/64-bit • Windows XP SP2 64-bit (AMD64/EM64T) • Windows Embedded POSReady 2009 • Server 2008 SP2 (not R2) 32/64-bit • Server 2003 R2 SP2 32/64-bit • Server 2003 SP2 32/64-bit Podpora MacOS: • macOS Sonoma 14.0 – 14.6.1 • macOS Ventura 13.0 – 13.6.9

		• macOS Monterey 12.0 -12.7.6 Podpora Linux: • Azure Linux • CentOS 8.4 - 8.0, 7.9 - 7.0, 6.10 - 6.4, Strem v9 • Red Hat Enterprise Linux (RHEL) 9.3.- 9.0, 8.9- 8.0, 7.9 - 7.0, 6.10 - 6.4 • Ubuntu 22.04.6, 22.04, 20.04, 18.04, 16.04, 14.04 • Amazon Linux 2023.3, 2023.1, 2023,2 , AMI 2018, AMI 2017 • SUSE Linux Enterprise Server 15 sp5, 15.x, 12.x, 11 sp4 • Debian 12.4, 12.2, 12.1, 12, 11.9, 11.8, 11.7, 11, 10, 9, 8 • Virtuozzo 7 • Scientific Linux 7, 6 • AlmaLinux 9.3, 9.2, 9.1, 9.0, 8.8, 8.7, 8.6, 8.5, 8.4 • Rocky Linux 9.3, 9.2, 9.1, 9.0, 8.8, 8.7, 8.6, 8.5, 8.4 • Oracle 9.3, 9.2, 9.1, 9.0, 8.8 - 8.0, 7.9 - 7.0, 6.10, 6.9 • Fedora 39, 38, 37, 36, 35 • CloudLinux Shared v8, v6
Veškerá komunikace přenášená mezi management serverem a pracovní stanicí (agent) musí být během přenosu šifrována.	ANO	Podporovány jsou verze TLS 1.2 a 1.3, verze TLS 1.1 a nižší není podporována
Řešení musí zajišťovat funkce EPP (Endpoint Protection Platform) nové generace a EDR (Endpoint Detection and Response) v rámci jednoho samostatného agenta, který ke své funkci nepotřebuje připojení ke cloudu nebo konzoli pro správu.	ANO	Integruje funkce EPP i EDR a nabízí komplexní ochranu od prevence po detekci a reakci. Využívá jak statickou umělou inteligenci pro detekci před spuštěním, tak behaviorální umělou inteligenci pro monitorování a reakci v reálném čase. Agent SentinelOne pracuje nezávisle a poskytuje ochranu i v režimu offline. Tím je zajištěna nepřetržité zabezpečení bez závislosti na připojení k internetu.

Agent musí být plně autonomní, což znamená, že jeho provoz a funkčnost nesmí záviset na serveru pro správu, cloudu nebo JAKÝCHKOLIV externích zdrojích agenta. Detekce a reakce na pokročilé hrozby (0-day, fileless, RAM-based, 0-Day Exploits, ransomware, cryptominers, laterální pohyb, APT) musí být možná v reálném čase, nesmí záviset na stavu sítě stanice (agent musí provádět stejnou funkcionalitu online i offline) a nesmí vyžadovat žádný jiný typ externích zdrojů.	Ano	V případě útoku může agent automaticky provést nápravu hrozby a vrátit systém do stavu před útokem. Poskytuje úplný přehled o prostředí koncového bodu pomocí forenzních dat v reálném čase a údajů o celém kontextu. Kombinace statické AI pro detekci před spuštěním a behaviorální AI pro monitoring v reálném čase zajišťuje, že SentinelOne agent dokáže účinně chránit koncové body i v izolovaných nebo odpojených prostředích.
Řešení musí podporovat ověřování SSO – SAMLv2.	ANO	SentinelOne podporuje ověřování pomocí Single Sign-On (SSO) a protokolu SAML v2.0. Toto řešení umožňuje integraci s různými poskytovateli identity (IdP), což zjednodušuje správu přístupu a zvyšuje bezpečnost. IdP-initiated SSO: Uživatelé se mohou přihlásit prostřednictvím svého poskytovatele identity a následně získat přístup k SentinelOne konzoli. SP-initiated SSO: Uživatelé mohou začít přihlašovací proces přímo na SentinelOne konzoli a být přesměrováni na svého poskytovatele identity pro ověření. Podpora různých IdP: SentinelOne lze integrovat s různými poskytovateli identity.
Řešení musí podporovat dvoufaktorovou autentizaci (2FA) pro přístup správce pomocí Google Authenticator nebo Microsoft Authenticator.	ANO	SentinelOne podporuje dvoufaktorovou autentizaci (2FA) pro přístup správce a lze ji konfigurovat pomocí aplikací Google Authenticator nebo Microsoft Authenticator.
Úložiště EDR musí umožňovat uchovávat data alespoň 14 dní v cloudovém modelu SaaS a musí být prodloužitelné na 365 dní.	ANO	Standardní doba uchovávání dat je 14 dní. Je možné prodloužení doby uchovávání dat až na 365 dní. Data jsou ukládána v cloudovém prostředí, což zajišťuje flexibilitu a škálovatelnost.
Informace o incidentech a související události musí být uchovávány v centrální konzoli alespoň po dobu 1 roku.	ANO	Je možné prodloužení doby uchovávání dat na 365 dní i více.

Řešení musí být schopno identifikovat pokročilé hrozby, jako jsou fileless útoky, 0-day malware nebo zneužití zranitelností ve vlastněném softwaru/hardwaru bez použití reputačních enginů nebo detekčních modulů založených na signaturách. Reputačním enginem je myšlena identifikace hrozeb pomocí následujících reputačních prvků: • IP Adresy, • DNS, • URL, • zkratky/hashe.	ANO	Behaviorální AI: SentinelOne využívá behaviorální analýzu a strojové učení k detekci anomálií a podezřelého chování v reálném čase, což umožňuje identifikaci hrozeb bez nutnosti signatur nebo reputačních dat. Fileless útoky: SentinelOne dokáže detekovat fileless útoky, které nevyužívají tradiční soubory, ale místo toho injektují škodlivý kód přímo do paměti nebo využívají legitimní systémové procesy, jako je PowerShell. 0-day malware: Díky pokročilým algoritmům strojového učení a behaviorální analýze je SentinelOne schopen identifikovat a blokovat 0-day malware, který využívá dosud neznámé zranitelnosti. Exploity zranitelností: SentinelOne monitoruje a analyzuje chování aplikací a systémových procesů, což umožňuje detekci a blokování exploitů zranitelností ve vlastním softwaru nebo hardwaru.
Řešení musí využívat statické a dynamické algoritmy založené na umělé inteligenci k identifikaci hrozeb, včetně těch, které dosud nebyly známy.	ANO	SentinelOne využívá kombinaci statických a dynamických algoritmů založených na umělé inteligenci (AI) k identifikaci hrozeb. Statická AI se využívá k analýze souborů před jejich spuštěním. Tyto algoritmy zkoumají strukturu souborů a hledají vzory, které jsou typické pro škodlivý kód. Dynamická AI sleduje chování aplikací a procesů v reálném čase. Tato behaviorální analýza umožňuje detekci anomálií a podezřelého chování, které může naznačovat přítomnost škodlivého kódu nebo útoku. Dynamická analýza je obzvláště účinná při detekci fileless útoků a 0-day malware, které se vyhýbají tradičním metodám detekce založeným na signaturách.
Moduly EPP / EDR nabízené v řešení musí automaticky reagovat na vznikající hrozby a zmírňovat jejich dopady v reálném čase, autonomním způsobem s následujícími	ANO	SentinelOne nabízí pokročilé moduly EPP (Endpoint Protection Platform) a EDR (Endpoint Detection and Response), které automaticky reagují na vznikající hrozby

možnostmi reakce na hrozby definovanými bezpečnostní politikou: • **Upozornění** • **Ukončení procesu** • **Karanténa** • **Odpojení od sítě** • **Náprava** • **Obnovení**		eliminují jejich dopady v reálném čase. Tyto moduly fungují autonomně a umožňují různé možnosti reakce na hrozby, které lze definovat v bezpečnostní politice. Možnosti reakce na hrozby: Upozornění: Automatické upozornění administrátorů na detekované hrozby prostřednictvím notifikací. Ukončení procesu: Automatické ukončení škodlivých procesů, aby se zabránilo dalšímu šíření hrozby. Karanténa: Izolace infikovaných souborů nebo aplikací, aby se zabránilo jejich spuštění nebo šíření. Odpojení od sítě: Automatické odpojení infikovaného zařízení od sítě, aby se zabránilo šíření hrozby na další zařízení. Náprava: Automatická remediace hrozeb, která zahrnuje odstranění škodlivého kódu a opravu zasažených systémových komponent. Obnovení: Funkce rollback, která umožňuje vrátit systém do původního stavu před útokem.
Řešení musí umožnit obnovit stav koncové stanice do stavu v době vytvoření záznamu Volume Shadow Copy (VSS) a vrátit zpět změny provedené škodlivým procesem a jeho přidruženými prostředky. Agent musí autonomně a téměř v reálném čase obnovovat data z chráněného hostitele v případě útoku ransomwaru.	ANO	Obnova v SentinelOne: SentinelOne využívá technologii VSS, která je nativně integrována do všech podnikových verzí operačního systému Windows. Tato technologie umožňuje vytváření záloh systémových stavů a souborů. Autonomní obnova - v případě detekce ransomwaru nebo jiného škodlivého útoku může SentinelOne autonomně obnovit systém do předchozího stavu pomocí VSS, aniž by to ovlivnilo jiné benigní aktivity na koncovém bodu. SentinelOne také chrání VSS před škodlivými aktivitami, aby zajistil, že zálohy zůstanou nedotčené a použitelné pro obnovu.

		Obnova dat probíhá téměř v reálném čase, což minimalizuje dopad útoku a zajišťuje rychlé obnovení provozu. Jak to funguje: 1. Detekce útoku: SentinelOne detekuje škodlivý proces nebo ransomware útok. 2. Izolace a analýza: Infikované zařízení je izolováno a útok je analyzován. 3. Obnova pomocí VSS: Systém je obnoven do stavu před útokem pomocí záloh vytvořených technologií VSS.
Řešení musí podporovat následující mechanismy detekce malwaru: • **Pre-Execution** – identifikace malwaru na základě souborů pomocí reputation engine. Tato funkce ke svým úkolům nevyžaduje aktualizace databáze signatur ani aktualizace signatur souborů • **Před spuštěním** – řešení musí být schopno identifikovat neznámý souborový malware na základě statické analýzy pomocí algoritmů strojového učení. Taková analýza musí probíhat autonomně na koncové stanici, bez externích závislostí nebo externího zpracování. Aby funkce fungovala, nesmí vyžadovat zahrnutí známých IoC (DNS, IP, URL, HASH) a taková detekce musí fungovat v reálném čase, když se přistupuje k danému operačnímu systému nebo souboru. • **Run-Time** – Agent musí identifikovat útoky a reagovat na ně pomocí sofistikovaných hackerských technik (útoky bez souborů, 0denní zranitelnosti a malware, škodlivé skriptování, laterální pohyb, ransomware, trojské koně, APT atd.)	ANO	SentinelOne podporuje pokročilé mechanismy detekce malwaru: Reputation engine: zajišťuje ochranu proti uložení nebo spuštění známých škodlivých souborů. Statická analýza pomocí AI: SentinelOne využívá statické algoritmy strojového učení k analýze souborů před jejich spuštěním. Tato analýza probíhá autonomně na koncové stanici a nevyžaduje externí závislosti nebo externí zpracování. Detekce funguje v reálném čase a nevyžaduje známé IoC (DNS, IP, URL, HASH). Behaviorální A identifikuje a reaguje na útoky pomocí behaviorální analýzy a algoritmů umělé inteligence. Tento přístup umožňuje detekci sofistikovaných hackerských technik, jako jsou fileless útoky, 0-day zranitelnosti, škodlivé skriptování, laterální pohyb, ransomware, trojské koně a APT3. Detekce probíhá téměř v reálném čase a nevyžaduje externí závislosti ani lidský zásah. Výhody těchto mechanismů: Autonomní detekce: Všechny detekční mechanismy fungují autonomně, což minimalizuje potřebu manuálního zásahu.

Identifikace těchto hrozeb nesmí vyžadovat externí závislosti, lidský zásah nebo analýzu dat mimo chráněnou koncovou stanici. Funkčnost musí být implementována téměř v reálném čase pomocí algoritmů umělé inteligence		Reálný čas: Detekce a reakce probíhají téměř v reálném čase, což zajišťuje rychlou ochranu proti hrozbám. Detekční mechanismy nevyžadují externí závislosti, což zvyšuje spolehlivost a efektivitu ochrany.
Známý IoC (DNS, IP, URL, HASH) nesmí být vyžadován jako prostředek identifikace hrozby.	ANO	SentinelOne využívá statické algoritmy strojového učení k analýze souborů před jejich spuštěním. Tato analýza probíhá autonomně na koncové stanici a nevyžaduje externí závislosti nebo externí zpracování. Detekce funguje v reálném čase a nevyžaduje známé IoC (DNS, IP, URL, HASH).
Řešení musí poskytovat silný mechanismus "Anti-Tamper", tj. mechanismy na ochranu před manipulací se softwarem malwarem nebo koncovým uživatelem. Tento mechanismus musí být chráněn jedinečným heslem pro každý koncový počítač. • **Stav zapnuto/vypnuto.** Ochrana před neoprávněnou manipulací je konfigurovatelnou možností v bezpečnostních politikách.	ANO	Pokud je povolena tamper protection budou tyto akce znemožněny kromě autorizovaných uživatelských účtů a uživatelů s přístupovým klíčem: Službu SentinelOne Agent nelze zastavit. Uživatelé nemohou odinstalovat službu SentinelOne Agent v interaktivní relaci (tj. pomocí příkazového řádku nebo prostředí Windows PowerShell). Klíče registru související s agentem nelze měnit ani odstraňovat. Složka, ve které je nainstalován agent, je chráněna proti zápisu. Softwarové ovladače nainstalované s agentem jsou chráněny proti změnám.
Bezpečnostní politika musí poskytovat možnost povolit nebo zakázat jednotlivé detekční moduly nebo podle typu modulu (moduly před spuštěním a moduly za běhu). Tato volba není vyžadována pro reputation engine.	ANO	SentinelOne používá následující detekční moduly: • Reputation - Tento modul je vždy povolený a nelze ho zakázat. • Static AI • Static AI – Suspicious • Behavioral AI – Executables • Documents, Scripts • Lateral Movement • Anti Exploitation / Fileless

		• Potentially Unwanted Applications • Application Control • Identity Detection & Response • Detect Interactive Threat
Řešení musí poskytovat možnost odesílat textové zprávy uživateli koncové stanice přímo z konzoly pro správu, a to i v případě, že agent běžící na stanici je v režimu izolace sítě / karantény sítě.	ANO	I když je zařízení izolováno od sítě, stále může komunikovat se SentinelOne management konzolí. To umožňuje administrátorům zasílat zprávy a instrukce přímo uživateli.
Řešení musí obsahovat řídicí panel zobrazující všechny počítače a možnost filtrovat je na základě atributů, jako je operační systém, typ koncové stanice, verze agenta, přítomné zranitelnosti, atributy AD, telemetrické informace, IP adresování, hardwarové vlastnosti, počty procesorů, adresy Mac, rozhraní, název hostitele, název skupiny, doména). Seznam musí být k dispozici pro zobrazení hostitelům inventáře, použití akcí na podmnožinu koncových stanic nebo mapování koncových stanic na skupiny. Musí poskytovat možnost zobrazení podrobností o stanici, jako jsou aspekty telemetrie, stav stanice, aplikace, a poskytnout následující možnosti akcí: • Odpojit/Připojit od sítě (karanténa sítě), • Restartovat OS, • Vypnout systém, • Odeslat zprávu uživateli, • Odinstalovat agenta, • Zobrazit hrozby	ANO	Administrátorská konzole umožňuje zobrazit všechny počítače a filtrovat je na základě různých atributů. Filtrování a zobrazení: • Operační systém: Filtrování podle různých operačních systémů. • Typ koncové stanice: Možnost filtrovat podle typu zařízení (např. PC, server). • Verze agenta: Zobrazení a filtrování podle verzí nainstalovaného agenta. • Přítomné zranitelnosti: Identifikace a filtrování zařízení podle zranitelností. • Atributy AD: Filtrování na základě atributů Active Directory. • Telemetrické informace: Zobrazení telemetrických dat z koncových bodů. • IP adresování: Filtrování podle IP adres. • Hardwarové vlastnosti: Zobrazení a filtrování podle hardwarových specifikací, jako jsou počty procesorů, adresy MAC, rozhraní, název hostitele, název skupiny a doména.

		Akce na podmnožinu koncových stanic: • Odpojit/Připojit od sítě (karanténa sítě): Možnost izolovat zařízení od sítě nebo je znovu připojit. • Restartovat OS: Možnost vzdáleně restartovat operační systém na koncovém bodu. • Vypnout systém: Možnost vzdáleně vypnout zařízení. • Odeslat zprávu uživateli: Odesílání textových zpráv uživatelům přímo z konzoly, i když je zařízení v režimu izolace. • Odinstalovat agenta: Možnost vzdáleně odinstalovat SentinelOne agenta z koncového bodu. • Zobrazit hrozby: Zobrazení všech detekovaných hrozeb na konkrétním zařízení.
Zásady ochrany stanice musí umožňovat volbu reakce (např. výstraha nebo aktivní reakce) na detekovanou hrozbu na základě kvalifikace události. Aktivní reakce na hrozby musí být prováděna autonomním agentem, a to i v případě, že chráněná stanice není připojena k síti.	ANO	Administrátoři mohou nastavit různé reakce na detekované hrozby, jako jsou výstrahy nebo aktivní reakce (např. izolace zařízení, ukončení procesu, karanténa souboru) na základě závažnosti a typu hrozby. SentinelOne agent funguje autonomně a je schopen provádět aktivní reakce na hrozby bez nutnosti připojení k síti. To zahrnuje izolaci zařízení, odstranění škodlivého kódu a obnovení systému do původního stavu. Reakce jsou prováděny téměř v reálném čase, což minimalizuje dopad hrozeb a zajišťuje rychlou obnovu.
Řešení EPP/EDR musí být vyžadováno pro zajištění funkčnosti lokálního firewallu pro chráněnou koncovou stanici. Ochrana bránou firewall musí umožňovat jedinečné	ANO	SentinelOne umožňuje definovat jedinečné firewallové zásady pro každou chráněnou skupinu koncových bodů. To

zásady pro každou chráněnou skupinu hostitelů. Pravidla brány firewall musí být schopná brát v úvahu následující parametry: • FQDN, • IP, • CIDR. Funkce musí být podporovány pro následující operační systémy: • Windows, • Linux a • macOS.		zajišťuje, že různé skupiny zařízení mohou mít specifické bezpečnostní politiky. Parametry pravidel firewallu: FQDN (Fully Qualified Domain Name): Pravidla mohou být nastavena na základě plně kvalifikovaných doménových jmen. IP adresy: Pravidla mohou být definována na základě konkrétních IP adres. CIDR (Classless Inter-Domain Routing): Pravidla mohou zahrnovat rozsahy IP adres pomocí CIDR notace. Podporován je agent na Windows, Linux i MacOS. V definici FW pravidla lze omezit, na který typ OS bude aplikováno.
Řešení EPP/EDR musí mít funkcionalitu pro ovládání zařízení, která se pokoušejí o přístup k chráněné stanici. Řízení zařízení musí umožňovat jedinečné zásady pro každou chráněnou skupinu hostitelů. Podpora ovládání zařízení je vyžadována pro následující rozhraní: • USB a • Bluetooth. Funkce musí být podporovány pro následující operační systémy: • Windows a • macOS.	ANO	Podpora rozhraní: USB: Možnost řídit přístup USB zařízení na základě atributů jako Vendor ID, Product ID, Serial Number a Class. Bluetooth: Možnost řídit přístup Bluetooth zařízení podle verze protokolu a typu zařízení. Administrátoři mohou definovat specifické zásady pro různé skupiny hostitelů, což umožňuje granularitu a flexibilitu při správě zařízení. Podpora pro definování a aplikaci zásad ovládání zařízení na Windows a macOS zařízeních.
Řešení EPP / EDR musí spravovat zranitelnosti aplikací nainstalovaných na chráněném hostiteli a poskytovat informace CVE spojené s detekovanou zranitelností.	ANO	Řešení umožňuje identifikaci a správu zranitelností, automaticky detekuje zranitelnosti v aplikacích a poskytuje podrobné informace o CVE. Nabízí nástroje pro opravu zranitelností a zajištění bezpečnosti systémů. Umožňuje integraci s dalšími nástroji pro komplexní zabezpečení.
Funkce EDR musí mít schopnost automaticky a autonomně provádět předběžné indexování a předběžnou korelaci událostí, ke kterým dochází v chráněném prostředí. Indexování musí probíhat v reálném čase a proces musí probíhat na chráněné stanici, nikoli v cloudu. Související	ANO	SentinelOne využívá technologii Singularity Storyline, která automaticky monitoruje, sleduje a kontextualizuje data událostí v reálném čase. Tento proces probíhá přímo na chráněné stanici, nikoli v cloudu. Každá událost je opatřena

události musí mít jedinečný identifikátor, který pomůže identifikovat skupinu událostí, které spolu souvisí. Dotaz obsahující tento typ identifikátoru musí vracet informace o všech událostech (IP, DNS, SOUBORY, REGISTRY, PROCESY, ADRESY URL atd.), které tvoří danou situaci, bez ohledu na to, zda souvisí s malwarem či nikoli. Kromě toho by řídicí panel EDR měl obsahovat průzkumníka "stromu procesů", který by graficky vizualizoval a analyzoval procesy, které tvořily událost.		jedinečným identifikátorem, což umožňuje snadnou identifikaci a korelaci souvisejících událostí. Pomocí těchto identifikátorů se lze dotazovat na informace o všech souvisejících událostech, včetně IP adres, DNS záznamů, souborů, registrů, procesů a URL adres. Konzole obsahuje nástroj pro grafickou vizualizaci a analýzu procesů, které tvoří událost.
EDR musí podporovat možnost vytvářet vlastní pravidla detekce pomocí transformace dotazů (EDR / XDR) na pravidla automatické detekce.	ANO	SentinelOne EDR podporuje vytváření vlastních pravidel detekce pomocí technologie Storyline Active Response (STAR). Tato technologie umožňuje bezpečnostním transformovat dotazy z mechanismu sběru a dotazování dat EDR (Deep Visibility) na automatizovaná pravidla detekce. Klíčové funkce STAR: • Vytváření vlastních pravidel detekce: Lze psát vlastní dotazy a přeměnit je na pravidla, která automaticky spouštějí upozornění a reakce při detekci. • Automatizované reakce: Pravidla mohou být nastavena tak, aby automaticky reagovala na hrozby, například karanténou koncových bodů nebo zastavením procesů. • Reálný čas: Všechna pravidla a reakce jsou aplikována v reálném čase na celou síť nebo na vybranou část.
EDR musí poskytovat prohlížeč stromu procesů.	ANO	SentinelOne konzole obsahuje nástroj pro grafickou vizualizaci a analýzu procesů, které tvoří událost.
EDR musí automaticky indexovat a korelovat události pod jedinečným identifikátorem,	ANO	Každá událost je opatřena jedinečným identifikátorem, což umožňuje snadnou

který jednoznačně identifikuje konkrétní strom procesu.		identifikaci a korelaci souvisejících událostí.
Řešení EPP / EDR musí poskytovat funkci Full Remote Shell, aby správce mohl provádět příkazy na koncové stanici, i když je v izolovaném stavu sítě. Kromě toho musí řešení uložit přepis zkompilované relace a chránit jej min. heslem.	ANO	SentinelOne konzole obsahuje funkci Full Remote Shell, která umožňuje správcům provádět příkazy na koncových stanicích i když jsou v izolovaném stavu sítě. Tato funkce poskytuje bezpečný přístup k chráněným koncovým bodům přímo, což umožňuje rychlé řešení problémů a sběr forenzních dat
Navržené řešení musí mít schopnosti překládat přirozený jazyk do strukturovaných dotazů a automaticky je spouštět proti shromážděné telemetrii EDR/XDR.	ANO	SentinelOne nabízí technologii Purple AI: Překlad přirozeného jazyka: Purple AI dokáže převést dotazy v přirozeném jazyce na sofistikované strukturované dotazy (PowerQueries). Automatické spouštění dotazů: Tyto dotazy jsou automaticky spouštěny proti shromážděné telemetrii, což zjednodušuje a urychluje proces vyhledávání hrozeb a vyšetřování. Inteligentní sumarizace výsledků: Výsledky jsou inteligentně sumarizovány a jsou navrhovány další dotazy v přirozeném jazyce. Kolaborativní nástroje: Purple AI umožňuje snadnou spolupráci prostřednictvím sdílených, exportovatelných vyšetřovacích poznámek a automaticky generovaných e-mailů.
Navrhované řešení musí mít zabudovaný ochranný mechanismus, který zabrání uživatelům v nevhodném použití řešení a je odolný vůči útokům LLM.	ANO	SentinelOne zahrnuje několik ochranných mechanismů, které zabraňují nevhodnému použití řešení a poskytují odolnost vůči útokům na Large Language Models (LLM): Vícefaktorová autentizace (MFA): Zajišťuje, že přístup k systému je omezen pouze na autorizované uživatele. Role-based Access Control (RBAC): Umožňuje správcům definovat a omezit přístupová práva uživatelů na základě jejich rolí, čímž se minimalizuje riziko zneužití.

		Šifrování dat: Všechna data jsou šifrována jak při přenosu, tak při uložení, což zajišťuje jejich ochranu před neoprávněným přístupem. Detekce a prevence útoků: SentinelOne využívá pokročilé algoritmy a strojové učení k detekci a prevenci útoků, včetně těch, které jsou zaměřeny na zneužití LLM. Auditní logy a monitorování: Systém zaznamenává všechny akce uživatelů a poskytuje podrobné auditní logy, které mohou být použity k monitorování a vyšetřování podezřelých aktivit. Tyto mechanismy společně zajišťují, že SentinelOne je robustní a bezpečné řešení, které chrání před útoky na LLM modely.
Navrhované řešení musí mít konverzační koncept, který by nám měl umožnit klást otázky a dostávat odpovědi v konkrétním kontextu (tj. časový rozsah poslední tři dny).	ANO	SentinelOne nabízí konverzační koncept prostřednictvím technologie Purple AI, která umožňuje klást otázky v přirozeném jazyce a získávat odpovědi na základě shromážděné telemetrie. Dotazy mohou být specifikovány pro konkrétní časový rozsah, což umožňuje přesnější a relevantnější odpovědi.
Navrhované řešení musí mít schopnosti sumarizovat protokoly událostí a indikátory pomocí přirozeného jazyka.	ANO	Technologie Purple AI umožňuje automatické shrnutí protokolů událostí a indikátorů do přirozeného jazyka, což usnadňuje analýzu a pochopení dat.
Navrhované řešení musí mít schopnost sdílet výsledky šetření s ostatními členy týmu.	ANO	SentinelOne umožňuje sdílení výsledků šetření s ostatními členy týmu prostřednictvím několika funkcí: • Kolaborativní nástroje: SentinelOne poskytuje nástroje pro spolupráci, které umožňují sdílení vyšetřovacích poznámek a výsledků s ostatními členy týmu. • Automatické generování e-mailů: Výsledky šetření mohou být automaticky shrnuty a odeslány e-mailem příslušným členům týmu. • Export a sdílení dat: Uživatelé mohou exportovat data a zprávy z

		vyšetřování a sdílet je s ostatními členy týmu.
Navrhované řešení by nemělo být trénováno pomocí telemetrie zákazníků, dotazů a výsledků dotazů.	ANO	SentinelOne nevyužívá data zákazníků pro trénování svých modelů, čímž zajišťuje, že citlivé informace zůstávají chráněny. Veškerá telemetrie a data jsou zpracovávána a uchovávána s důrazem na bezpečnost a soukromí.
Řešení musí podporovat integraci se SIEM systémy třetích stran. *Integrace do SIEM systému Zadavatele (RSA Netwitness) není požadována jako součást implementace.*	ANO	SentinelOne podporuje integraci se SIEM systémy třetích stran, což umožňuje rozšířenou viditelnost a efektivnější správu bezpečnostních incidentů. SentinelOne se lze integrovat s různými SIEM platformami.
Řešení musí podporovat alespoň jeden z následujících formátů syslogu: • CEF, • CEF2, • RFC-5424, • STIX a • IOC.	ANO	SentinelOne podporuje integraci se systémy třetích stran pomocí Syslog formátů: CEF, CEF2, RFC-5424, STIX, IOC
Software nebo agenti nainstalovaní na uživatelských stanicích nesmí vyžadovat lokální Administrátorská práva ke spuštění.	ANO	SentinelOne agent nevyžaduje lokální administrátorská práva ke spuštění na uživatelských stanicích. Administrátorská práva jsou potřebná pouze pro instalaci a správu softwaru. Po instalaci může agent běžet bez nutnosti dalších administrátorských oprávnění.
Řešení musí být schopné integrace se službou Active Directory, aby bylo možné agenty automaticky přiřadit ke skupinám, které se mají přidružit k zásadám AD. Konzola pro správu by se NEMĚLA připojovat ke službě Active Directory přímo prostřednictvím služby ADFS ani žádnou jinou metodou k získání atributů služby AD zařízení a uživatele. Server pro správu řešení by neměl mít žádné závislosti na stavu služby AD.	ANO	SentinelOne podporuje integraci se službou Active Directory (AD) bez nutnosti přímého připojení ke službě AD prostřednictvím ADFS. Agent je nainstalován přímo na koncových stanicích, což umožňuje získávání informací o členství v AD přímo z koncového bodu. Informace o členství v AD jsou odesílány do cloudu přes zabezpečené připojení SSL, což eliminuje potřebu přímého připojení ke službě AD. Agenti mohou být automaticky přiřazeni ke skupinám na základě jejich členství v AD, což umožňuje snadnou správu zásad.

EDR musí být nativně integrován s komponentou EPP v jediném autonomním agentovi.	ANO	SentinelOne nativně integruje EDR (Endpoint Detection and Response) a EPP (Endpoint Protection Platform) do jediného autonomního agenta. Tento agent kombinuje pokročilé funkce prevence, detekce a reakce v reálném čase.

LICENCOVÁNÍ

- Řešení EPP/EDR musí podporovat následující modely nasazení:
  - SaaS (agent-> cloudová SaaS služba) nebo
  - lokální on-premise nasazení (virtuální zařízení).

IMPLEMENTAČNÍ POŽADAVKY

- Zpracování prováděcího projektu
- Pilotní implementace do infrastruktury Zadavatele na reprezentativní vzorek min. 50 zařízení
- Následná implementace na zbytek zařízení
- Zaškolení tří administrátorů
- Dokumentace skutečného stavu

Popis nabízeného řešení:

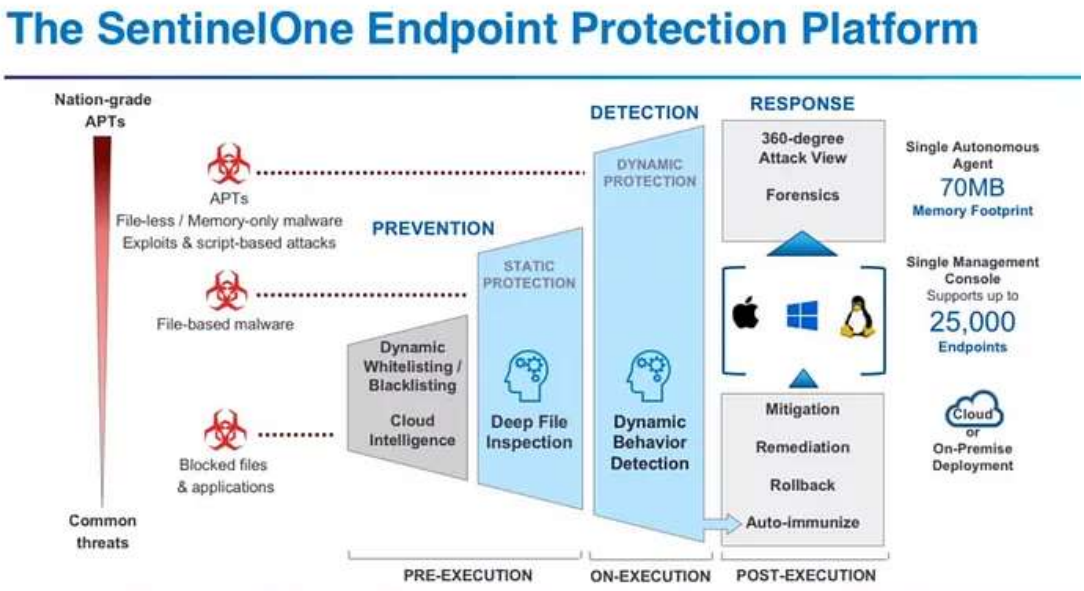
(dodavatel uvede popis nabízeného řešení v rozsahu max. 8 normostran, který bude zahrnovat minimálně – základní popis nabízeného řešení / konkrétní specifikace, formulace nebo deklarace dokládající splnění jednotlivých požadavků definovaných výše v části "Technické, funkční a integrační požadavky" / popis způsobu napojení na AD / popis způsobu distribuce/instalace agenta / seznam činností, které je možné provádět lokálně na agentovi, a které činnosti je možné provádět pouze z konzole / schéma architektury řešení včetně komunikace mezi klientem a centrální částí / další skutečnosti dle uvážení dodavatele)

1. Základní popis nabízeného řešení

SentinelOne Singularity Complete je pokročilé řešení pro ochranu koncových bodů, které kombinuje několik technologií k detekci a prevenci kybernetických hrozeb.

Základní architektura řešení SentinelOne:

- Agent na koncovém bodu: SentinelOne agent je nainstalován na koncových zařízeních (PC, servery, mobilní zařízení). Tento agent monitoruje a analyzuje chování systému v reálném čase.
- Cloudová platforma: Data shromážděná agenty jsou odesílána do cloudové platformy SentinelOne, kde jsou analyzována pomocí pokročilých algoritmů a strojového učení.
- Centrální správa: Administrátoři mohou spravovat a monitorovat všechny koncové body z jednoho centrálního dashboardu, což umožňuje rychlou reakci na incidenty a snadnou správu politik.



Klíčové funkce

- Pokročilá statická detekce: Analýza souborů před jejich spuštěním pomocí statických metod a dotazování na databázi vzorků.

- Detekce za běhu: Monitorování a analýza chování procesů v reálném čase, což umožňuje detekci a blokování podezřelých aktivit.
- Remediace a rollback: Po detekci hrozby umožňuje SentinelOne detailní analýzu útoku a vrácení systému do původního stavu pomocí funkce rollback.
- Auto-imunizace: Informuje ostatní koncové body v síti o detekované hrozbě a zabraňuje jejímu dalšímu šíření.

Agent využívá umělou inteligencí a je autonomní. Detekuje a reaguje na škodlivé aktivity v reálném čase, bez lidského zásahu. Pokud je koncový bod offline, jeho agent jej nadále chrání pomocí autonomních funkcí.

Local Agent Blocklist – Agent má svůj vlastní seznam signatur malwaru založený na Threat Intelligence . Detekuje každý soubor, který je zkopírován do koncového bodu a když je proces spuštěn nebo vytvořen.

Static AI – detekuje škodlivé chování z podezřelých atributů souborů, kódu a ze vztahů v souborových systémech, registrech, vlastnostech sítě, paměti a procesech. Statická umělá inteligence detekuje a zabraňuje typickým manipulacím útoky a událostem z MITRE ATT&CK.

Behavioral AI – Monitoruje objekty a události koncového bodu a detekuje útoky bez souborů, nové útoky, lateral movement, sběr dat, exploity v paměti, eskalaci oprávnění a další.

Storyline – Agent seskupuje všechny události a objekty související s hrozbou. To poskytuje úplnou viditelnost hrozby a všech jejích částí pro kompletní remediaci problému.

Politiky – Politika „Protect“ aplikuje automatickou mitigaci hrozeb a všech objektů hrozby ze Storyline. Politika „Detect“ umožňuje zobrazit data, která agent odesílá do management konzole, nastavit vlastní škodlivý nebo neškodný verdikt a spustit one-click mitigaci.

Purple AI - pokročilý AI bezpečnostní analytik navržený k zjednodušení a urychlení detekce hrozeb, vyšetřování a reakce. Umožňuje bezpečnostním týmům klást otázky v přirozeném jazyce, které jsou přeloženy do složitých dotazů PowerQuery. Zrychluje lov hrozeb a vyšetřování díky AI-powered analýzám, automatickým souhrnům a navrhovaným dotazům. Purple AI není trénován na zákaznických datech a je navržen s nejvyšší úrovní ochrany dat. Podporuje Open Cybersecurity Schema Framework (OCSF) pro okamžité dotazování nativních a partnerských dat v normalizovaném pohledu.

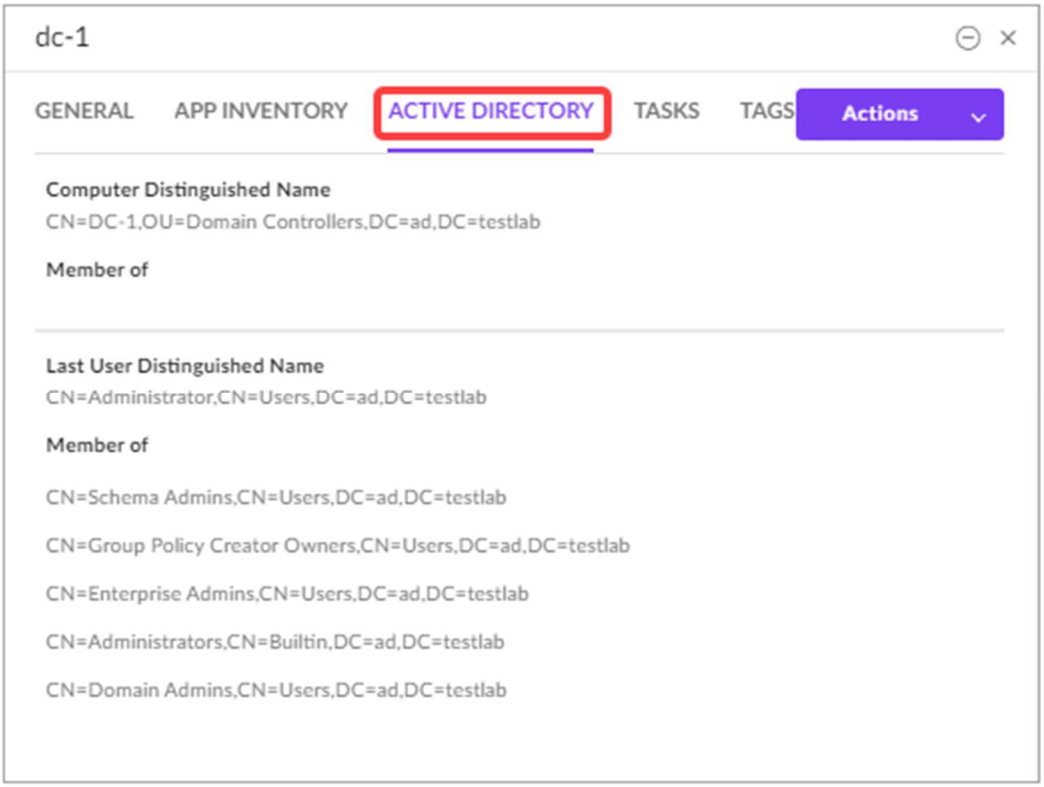
2. Konkrétní specifikace, formulace nebo deklarace dokládající splnění jednotlivých požadavků definovaných výše v části "Technické, funkční a integrační požadavky"

Uvedeno přímo u jednotlivých bodů v tabulce „Technické, funkční a integrační požadavky“

3. Popis způsobu napojení na AD

Integrace se službou Active Directory (AD) probíhá automaticky (není nutné konfigurovat AD server), když se agent, který je instalován na stanici v AD doméně, zaregistruje do managementu. Když se uživatel na této stanici přihlásí nebo odhlásí, agent odešle informace o AD do Management Console.

Když je koncový bod součástí AD domény, v „Endpoint Details“ je zobrazena karta „ACTIVE DIRECTORY“, která obsahuje informace o stanici a uživateli načtené z AD.



Karta „ACTIVE DIRECTORY“ zobrazuje doménu, skupiny, ve kterých je koncový bod, posledního přihlášeného uživatele a skupiny, ve kterých se uživatel nachází.

Na základě informací z AD je možné vytvářet tyto dynamické skupiny:

Device AD Membership – Skupiny podle fyzického umístění pracovní stanice nebo jiných relevantních detailů kolem samotné pracovní stanice.

User AD Membership – používá informace o aktuálním uživateli z AD, nezávisle na fyzické pracovní stanici. To je možné využít v prostředí VDI a také pro sdílené pracovní stanice nebo kiosky.

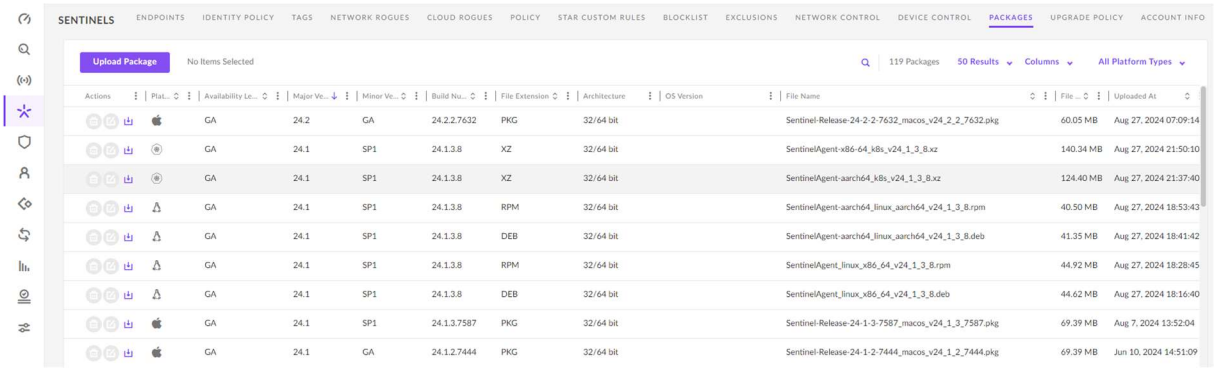
Agenti se dotazují na data z AD a odesílají aktualizace do konzoly pro správu v těchto případech:

- Načítá se agent
- Uživatel se přihlásí
- Uživatel se odhlásí
- Pravidelně (ve výchozím nastavení 180 minut. Toto lze změnit v parametrech agenta)

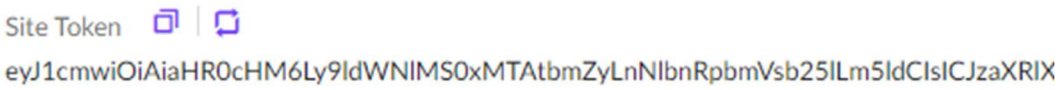
AD a LDAP nejsou podporovány pro ověřování přihlášení do Management Console.

4. Popis způsobu distribuce/instalace agenta

V management konzoli SentinelOne v menu Sentinels - Packages je k dispozici seznam dostupných verzí agentů pro všechny podporované OS. Seznam je možné filtrovat podle různých kritérií a následně stáhnout zvolený balíček.



Pro spárování agenta s managementem slouží „Site token“, který je se zobrazuje v management konzoli a který se použije při instalaci instalačního balíčku.



Windows:

Instalaci je možné provádět ručně spuštěním .exe balíčku, případně pomocí GPO, MS Intune nebo jiných nástrojů s využitím .msi balíčku. V konfiguraci balíčku se použije parametr -t k zadání site tokenu, např:

```
SentinelOneInstaller_windows_64bit_v22_2_1_200.exe -t a1b2c3d4e5f6g7h8i9a1b2c3d4e5f6g7h8i9
```

Po instalaci není nezbytně nutné provádět restart, většina funkcí je dostupná s výjimkou Behavioral AI budou, která je dispozici až po restartu.

macOS:

Po stažení a spuštění balíčku .pkg je nutné zadat „Site token“ a také povolit „Full Disk Access“ a „Network Extension“. Instalaci je možné provádět také pomocí příkazového řádku.

Linux:

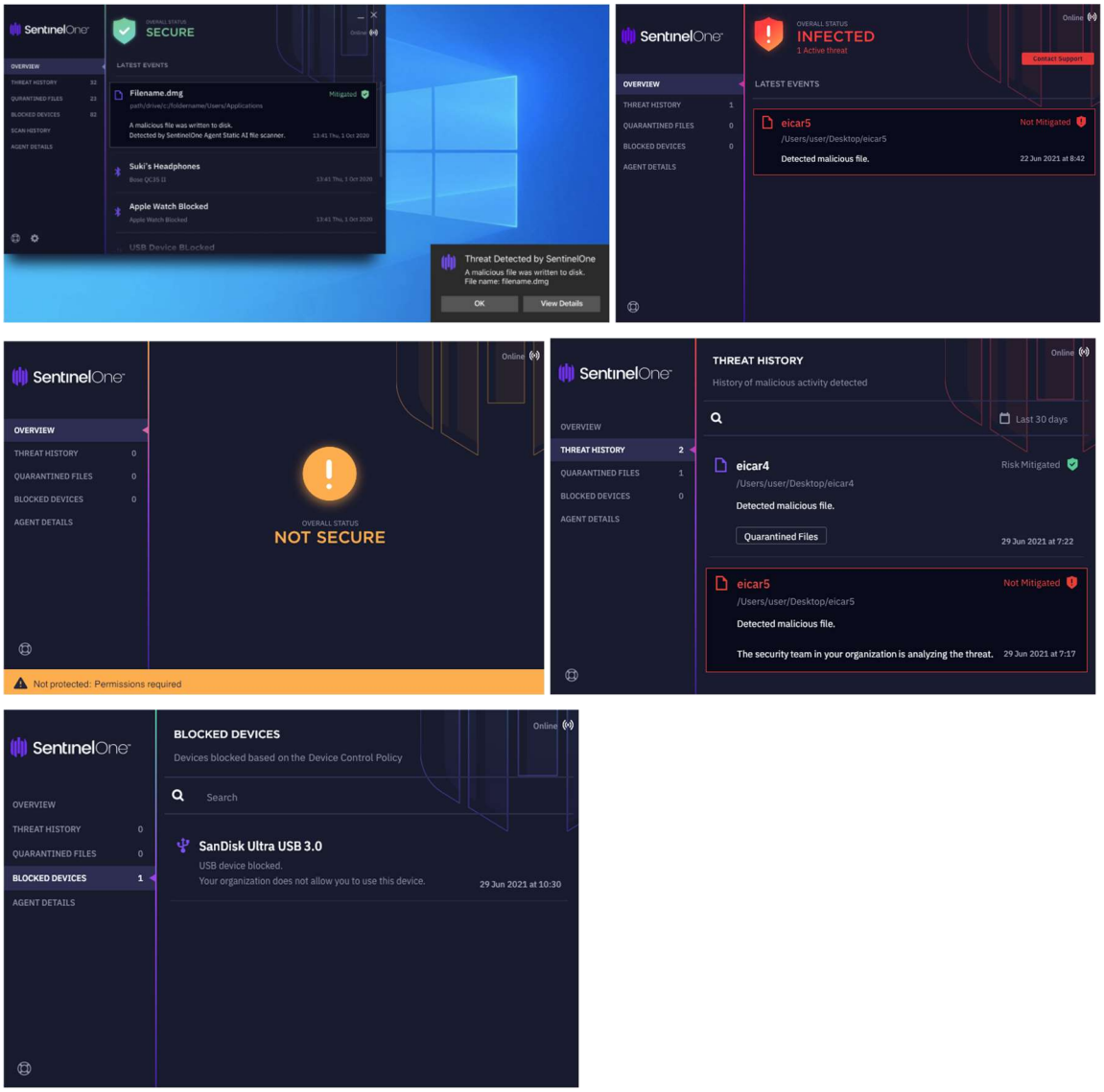
Po stažení a spuštění balíčku (RPM nebo DEB) je nutné zadat „Site token“ případně je možné vytvořit konfigurační soubor, který obsahuje nastavení agenta. Instalaci je pak možné provést spuštěním skriptu.

5. Seznam činností, které je možné provádět lokálně na agentovi, a které činnosti je možné provádět pouze z konzole

Činnosti na agentovi:

- Celkový přehled o stavu zabezpečení koncového bodu, stav připojení k managementu

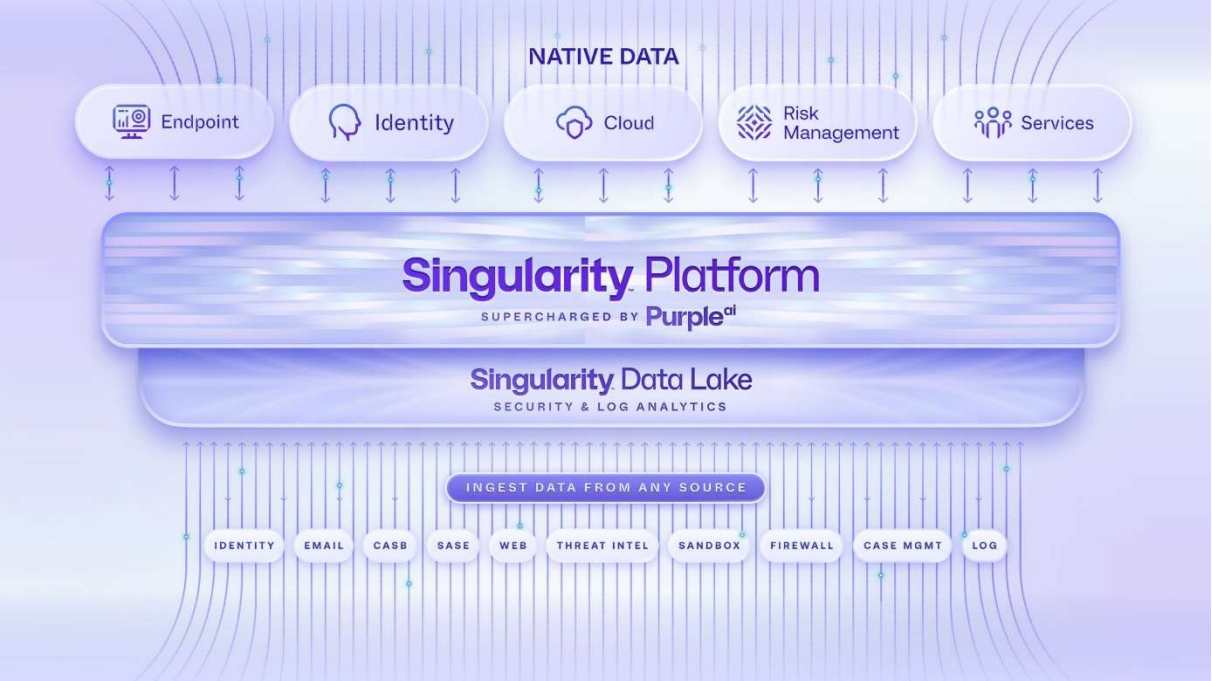
- Zobrazení historie detekovaných hrozeb, informace o stavu řešení hrozby
- Zobrazení karantény
- Zobrazení blokovaných zařízení



Veškerá změna konfigurace, spuštění skenování disku, zastavení agenta atd. se provádí z management konzole.

6. Schéma architektury řešení včetně komunikace mezi klientem a centrální částí

Cloudová webová management konzole je přístupná pomocí protokolu HTTPS. Komunikace mezi agentem na koncovém bodu a managementem probíhá na TCP 443.



Používané porty jsou uvedeny v následující tabulce:

Služba	**Zdroj**	**Cíl**	**Port**
SMTP	Management	SMTP server	TCP-25
SMTP SSL/TLS	Management	SMTP server	TCP-465 / TCP-587
Syslog	Management	Syslog server	UDP-514
Syslog over SSL	Management	Syslog server	TCP-6514
WebSocket	Windows endpoints s Agentem	Datová centra AWS podle regionu	TCP-443