Sectona Security Platform

Přehledný, integrovaný přístup k managementu oprávnění

Sectona Security Platform pomáhá podnikům snižovat riziko cílených útoků na privilegované účty, umístěné v datových centrech a cloudu. Sectona přináší integrované komponenty pro správu oprávnění, které řeší problémy s přístupem současné dynamické pracovní síly a komunikace mezi zařízeními pro moderní IT infrastrukturu a koncové body, umístěné v rámci lokálních prostředí, virtuálních prostředí nebo cloudu.

Sectona se svým integrovaným přístupem poskytuje jedinou konzoli pro zabezpečení hesel a důvěrných informací ve vestavěném úložišti, zabezpečení přístupu pomocí technologie pro přístup napříč platformami a správu oprávnění nad koncovými body.

Správa oprávnění kdekoli

Zabezpečte hesla a důvěrné informace pomocí integrované platformy napříč koncovými body, aplikacemi a pracovními úlohami.

Škálovatelná správa relací

Využijte technologii pro správu relací napříč platformami a spravujte tak relace na koncových bodech, v prohlížeči nebo na terminálovém serveru.

Vytvořeno s ohledem na škálování a bezpečnost

Implementujte a spravujte platformu se zabudovanými funkcemi vysoké dostupnosti, modulárními komponentami a podporou distribuované architektury.

Případy použití

Zabezpečený vzdálený privilegovaný přístup
Izoluje privilegované relace, spravuje komplexní politiky přístupu pomocí dynamického seskupování, podporuje uživatele přistupující z neznámé sítě.

Odebrání práv administrátora
Zablokování oprávnění na koncových bodech, zvýšení oprávnění na vyžádání, zamezení spouštění neznámých aplikací.

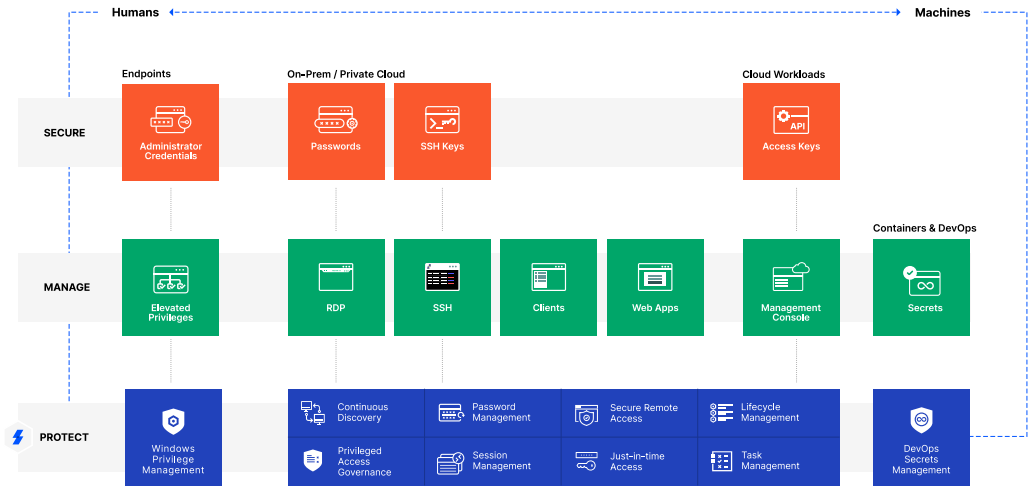
Zabezpečená cloudová prostředí
Správa identit a autentifikace, urychlený On-Boarding, umožnění vzdáleného přístupu bez VPN.

Automatické vyhodnocení oprávnění
Centralizované monitorování přidělení a používání oprávněného přístupu, nastavení vlastnictví kritických účtů

Zjednodušení privilegovaného přístupu
Automatizované poskytování privilegovaných účtů, flexibilní operace správy účtů.

Představení řešení

Sectona Security Platform spojuje prvky pro zabezpečení oprávnění při rostoucích úrovních útoků na organizace. Úzká integrace napříč platformou umožňuje týmům provozu, řízení a zabezpečení IT konzistentní správu a řízení bezpečnostních oprávnění napříč cloudem, virtuálními a koncovými body. Kompletní platforma byla vyvinuta od základu jako plně integrovaná pro zajištění velmi snadného používání, pro jednodušší správu a provoz.



Možnosti platformy

Řešte požadavky a problémy dynamického světa IT jednoduše a ve vhodnou chvíli díky integrované Sectona Security Platform a jejím možnostem.Sectona Security Platform byla vyvinuta pro zajištění Základních funkcí, které řeší správu hesel, správu relací pro IT provoz a bezpečnostní týmy. Pokročilé funkce jsou zaměřené na správu platformy, řízení oprávnění na koncových bodech a snadné a škálovatelné řízení oprávnění správcem s dělením na jednotlivé týmy nebo části IT prostředí, pro omezení rizika útoku.

Základní

Průběžná kontrola

Zabezpečení a kontrola nově přidaných zařízení a skrytých privilegovaných účtů.

Správa hesel

Robustní úložiště hesel pro zabezpečení privilegovaných identit a klíčů SSH.

Zabezpečený vzdálený přístup

Umožnění vzdáleného přístupu bez VPN.

Nahrávání relací a analýza hrozeb

Pokročilé monitorování relací pro všechny privilegované aktivity s profilováním rizik a analýzou chování.

Vícefaktorová autentifikace

Neutralizace rizik, spojených s kompromitací pověření, pomocí široké sady MFA mechanismů.

Přístup Just-In-Time

Odstranění stávajících oprávnění a využívání kombinace přístupů k zavedení J-I-T politik.

Správa privilegovaných úloh

Automatizace využívání přiřazených práv

Správa životního cyklu účtu

Zjednodušuje správu životního cyklu privilegovaných účtů a skupin v heterogenní infrastruktuře.

Pokročilé

Správa privilegovaných přístupů

Správa privilegovaných oprávnění a přístupu k platformě pro privilegovaný přístup, soupis účtů pro zabezpečení a dodržování právních norem.

Správa oprávnění oken

Kontrola a zabezpečení používání účtu správce v systému Windows, kontrola zvýšených oprávnění pro uživatele pracovní plochy systému Windows.

DevOps Secrets Management

Zabezpečení důvěrných přístupů, využívajících přístupy DevOps k aplikacím a službám, eliminace vestavěných nebo pevně zakódovaných pověření ,a protokolování všech privilegovaných relací.

Funkce platformy

- Integrujte víc než jen RDP a SSH, integrujte specializované programy a nástroje pomocí sady DIY Plugin Development Kit
- Využívá technologie správy relací napříč platformami k zabezpečení každé relace díky izolování této privilegované relace na konkrétní koncový bod.
- Integrovaná správa privilegovaných přístupů.
- Zabezpečení hesel, ssh klíčů a důvěrných informací v speciálně vytvořeném trezoru, který podporuje pouze autorizovaný přístup prostřednictvím PAM a API.
- Zabudovaná podpora vysoké dostupnost a horizontální i vertikální škálovatelnosti na úrovni modulů vám pomůže navrhnout optimální prostředí, které bude pružně reagovat na poptávku po zdrojích.
- Sectona MFA poskytuje silnější zabezpečení nastavení PAM tím, že vyžaduje druhý verifikační krok, generovaný prostřednictvím aplikace Sectona nebo SMS.
- Snadné nasazení PAM v různých regionech nebo lokalitách, ať už v cloudu nebo lokálně, díky flexibilním a odděleným komponentám, vytvořeným pro cloudová prostředí.
- Zabezpečení hesel a tajných informací v pasivní, šifrované a ověřené aplikaci odolné proti Break Glass scénářům.

sectona

Sectona se svým lehkým, integrovaným konceptem poskytuje jedinou konzoli pro zabezpečení hesel a důvěrných informací v zabudovaném trezoru, zabezpečení přístupu pomocí technologie pro přístup napříč platformami, a správu oprávnění nad koncovými body.

Pro více informací navštivte www.sectona.cz