SCIRGE

SHEDDING LIGHT ON SHADOW IT

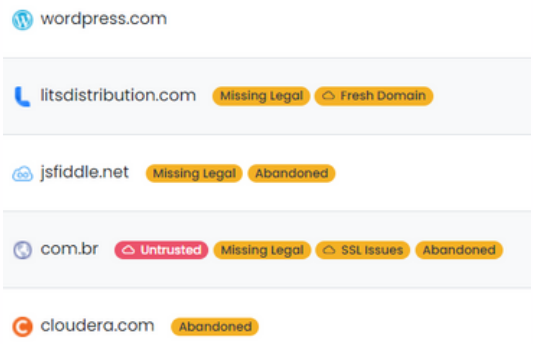
A felügyelet nélküli Shadow IT-fiókok és webes alkalmazások támadási felületet, hatékonysági és megfelelőségi kockázatokat hoznak létre.

A Scirge az informatikai és biztonsági döntéshozóknak segít abban, hogy átláthatóvá tegyék a digitális ellátási láncokat, valamint megvédjék a felhasználói fiókokat és azonosítókat.

Shadow IT Láthatóság

A Scirge a SaaS és a felhőalapú webes alkalmazásokat egy menedzselt böngésző-kiterjesztésen keresztül azonosítja. A detekció a bejelentkezéskor használt vállalati e-mail domain alapján történik, így a rendszer előre definiált adatbázis nélkül képes bármely webes szolgáltatás felismerésére.

A központi leltárokban az alkalmazások URL-címeit a böngészőből gyűjtött metaadatokkal, valamint dinamikus adatokkal, például a domain életkorával, feketelista-ellenőrzésekkel és egyéb kapcsolódó információkkal gazdagítjuk.

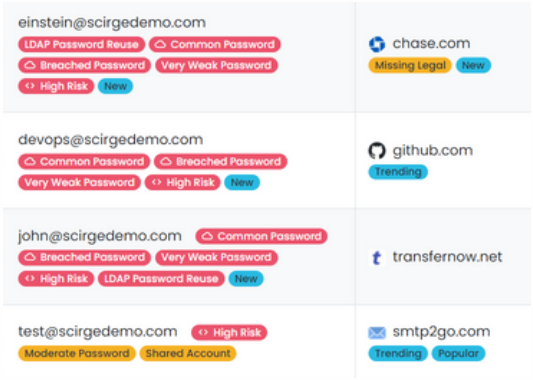


Alkalmazás leltár

Account és Jelszó Védelem

Az alkalmazottak által létrehozott fiókok a vállalatok Achilles-sarka. A Scirge minden egyes, a böngészőbe bevitt jelszót felügyel, hogy megelőzze az olyan gyakori támadási vektorokat, mint például a fiókátvétel, az adathalászat, a zsarolóprogramok telepítése és a belső visszaélések.

A szabályozási követelményeknek való megfelelés érdekében egyedi jelszó komplexitási szabályokat definiálhatunk. A jelszavak újrafelhasználását, megosztását, valamint korábban ellopott jelszavak használatát a szabványoknak megfelelő hashelés segítségével detektáljuk.



Hozzáférés leltár

Active Directory Jelszó Védelem

Az AD/LDAP jelszavak ugyanolyan folyamaton mennek keresztül, mint bármely más fiók, így a szabályozói elvárások és biztonsági ellenőrzések a lokális fiókokra is érvényesíthetőek.

A harmadik féltől származó webes alkalmazásokban újra felhasznált AD-jelszavak azonosítása kritikus indikátor, mivel az ellopott hitelesítő adatok a sikeres támadások 80%-ához járulnak hozzá, beleértve a zsarolóprogramok telepítését is.

Azonnali Felderítés

A Scirge Discovery egy könnyített funkció, amely a böngésző előzmények és a böngésző által mentett fiókok elemzésével segít a szervezeteknek azonnal felmérni a Shadow IT lábnyomukat.

A jelentések megmutatják a felfedezett alkalmazások számát, a mentett fiókok pedig pontosan megmutatják, hogy mely alkalmazások és jelszavak lehetnek sebezhetőek.

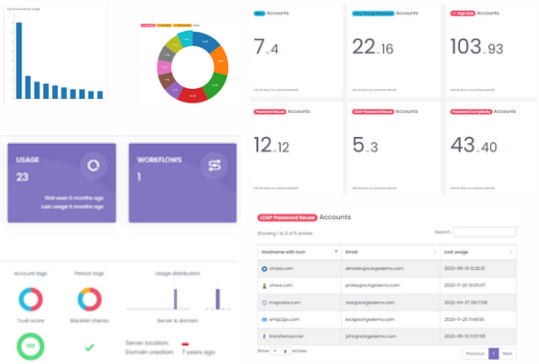
Felhasználási Területek

Megfelelőség

A beszállítók által kiadott ÁSZF-ek és irányelvek a földrajzi és bizalmi adatokkal együtt begyűjtésre kerülnek, hogy a kockázatértékelés és az auditok számára kontextust biztosítsanak.

Az automatikus figyelmeztetések és jelentések lehetővé teszik az érdekeltek és a GRC szakemberek számára, hogy naprakészek maradjanak a szervezeten belül megjelenő Shadow IT szolgáltatásokkal kapcsolatban.

A fiókmegosztási és használati trendek láthatósága lehetővé teszi a szabálytalanságok vagy belső csalások korai felismerését. A kiléptetési folyamatok során a kezeletlen identitások átadása vagy törlése is lehetővé válik.



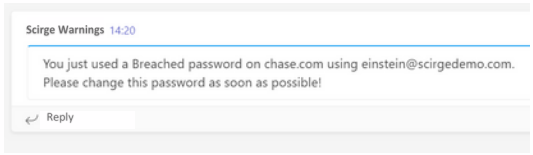
Egyedi riportok

Oktatás

A különböző üzleti területeken eltérő tapasztalattal és szakmai hátterel dolgozó munkatársak egyedi megközelítést igényelnek az oktatásban.

A Scirge lehetővé teszi, hogy testre szabjuk az oktatási üzeneteket a kiváltó okok, valamint a célközönség alapján.

Az informatikai részlegeknél a rossz jelszóhigiéniára vonatkozó figyelmeztetések nagyobb hangsúlyt igényelhetnek, míg a nem technikai szakemberek számára a komplexitási követelményeknek rendkívül világosnak és egyszerűnek kell lenniük.



Több csatornás üzenetküldés

Olvasnivalók

Implementációs Lehetőségek

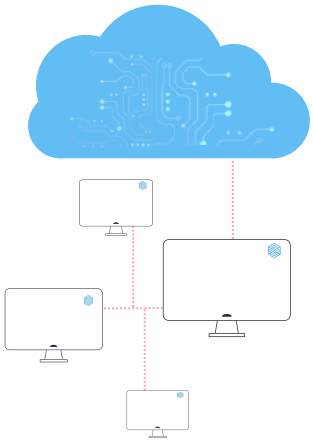
A Scirge egy könnyen telepíthető böngésző bővítmény formájában hajtja végre a központi szabályokat a végpontokon. Az alkalmazásokat és fiókokat a vállalati e-mail címek alapján azonosítja és a szerveren rendezi leltárokba.

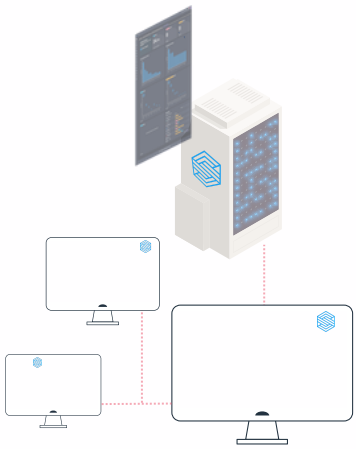
A management és konfiguráció natív felhő-szolgáltatásként, helyben telepíthető appliance verzióban, valamint managelt szolgáltatásként is elérhető. A Horizon Cloud Intelligence szolgáltatásai minden esetben elérhetőek az adatok gazdagítására.

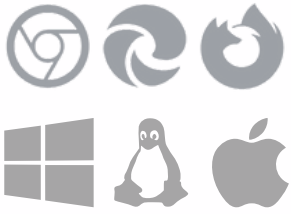
A rendszer a Chrome, Edge és Firefox böngészőket támogatja a főbb végponti operációs rendszereken.

	Virtuális Applianc	Scirge Cloud (SaaS)	Managelt Szolgáltatás
Örökös licensz (licensz + éves követés)	●		
Előfizetés (Egy vagy több éves)	●	●	
Havi számlázás (felhasználás alapú)			●

Implementációs és licensz mátrix







Biztonság és Adatvédelem

A végpontok a házirendek által szabályozott módon, az adatok korlátozott körét gyűjtik össze. Cleartext jelszavak soha nem kerülnek tárolásra. A végpontokon, a hálózati forgalomban és a kiszolgálón is hashelés és titkosítás biztosítja az adatok bizalmasságát és integritását.

További információ az adatvédelemről és a biztonságról.

Ingyenes Próba

Cégvezetés

A Shadow IT felderítése segít feltárni a szervezet informatikai lábnyomának és beszállítói láncainak legkevésbé ismert szegleteit. A Scirge olyan oktatást nyújt, amely a viselkedést célozza meg, és korai figyelmeztetést ad a felmerülő kockázatokra.

IT Döntéshozók

Az agilitás és a digitalizáció nem valósulhat meg egyéni kezdeményezések nélkül. Az üzleti egységeken belüli silók nem tudják megosztani a tudást, míg az IT-nek átláthatóságra van szüksége ahhoz, hogy támogassa a nem IT-részlegek innovációját.

Az Shadow IT felderítése segít feltárni az újonnan megjelenő trendeket és a régebbi vagy elhagyott szolgáltatásokat, amelyek figyelmet igényelnek a támogatás, a biztonság vagy a költségek szempontjából.

Kockázatkezelés és Megfelelés

A szabályozások és biztonsági keretrendszerek az eszköz leltárakon és kockázati besorolásokon alapulnak. A Shadow IT teljesen elérhetetlen a kockázatelemzés számára a láthatóság megteremtésére irányuló konkrét, célzott erőfeszítések nélkül.

A Scirge létrehozza a felügyelet nélküli alkalmazások és fiókok leltárát, és kontextusba helyezi használatukat és kockázataikat. A személyre szabott, figyelemfelkeltő üzenetek segítenek javítani az eltérő technikai készségekkel és háttérrel rendelkező alkalmazottak biztonsági szokásait.

Biztonság

A hitelesítő adatok újrafelhasználása a zsarolóvírusok elterjedésének és a sikeres betöréseknek az első számú okozója. A legtöbb kezeletlen jelszó és azonosító Shadow IT szolgáltatásokból származik, ahol a modern hitelesítési módszerek nem érvényesíthetők.

30 Perces Online Konzultáció