filter:max

Scirge termékismertető

1118 Budapest, Muskotály utca 11. info@filtermax.hu www.filtermax.hu
tel.: +36 20 520 0967

Tartalom

Scirge

A Shadow IT fiókok és webalkalmazások kezeletlen támadási felületet, működési hatékonytalanságot és megfelelőségi fenyegetéseket hoznak létre. A Scirge segít az informatikai és biztonsági döntéshozóknak abban, hogy nagyobb rálátással rendelkezzenek a digitális ellátási láncokra, sikeresen védhessék a felügyelettel nem rendelkező fiókokat, felfedhessék a személyazonosságokat és kihasználhassák a megfelelőségi és műveleti kontextusokat.

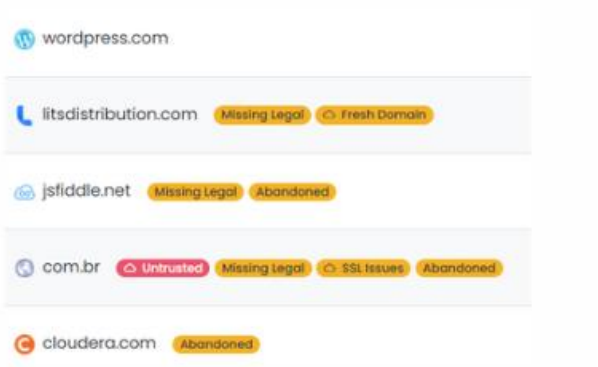
Shadow IT láthatóság

A Scirge egy felügyelt böngésző bővítményen keresztül azonosítja a SaaS és felhőalapú webszolgáltatásokat, webalkalmazásokat. Az észlelés azokon a vállalati e-mail domain-eken alapul, melyeket bejelentkezésre használnak, tekintet nélkül, bármely weboldalon.
Az alkalmazások URL-jeit a böngészőből gyűjtött metaadatok, valamint dinamikus adatok, például a domain regisztrációjától eltelt idő, a blacklist ellenőrzések és egyéb, ehhez kapcsolódó információk bővítik.
Ez lehetőséget biztosít a Scirge számára, hogy egy belső leltárt készítsen az összes harmadik feles alkalmazásokról az ismert alkalmazások adatbázisa nélkül.

Felhasználói fiókok és jelszóvédelem

A felhasználók által létrehozott új fiók minden vállalati környezet Achilles sarka. A Scirge minden egyes, a böngészőbe beírt jelszót figyel, hogy elejét vehesse a gyakori támadásoknak, mint az ATO, adathalászat, zsaroló programoktelepítése és csalás.

Egyedi összetettségű szabályok érhetőek el a szabályozási követelményeknek való megfeleléshez, míg az ipari szabványoknak megfelelő biztonságos kivonatolás a jelszavak újra felhasználásának, a jelszavak megosztásának és a kompromittálódott jelszavak észlelésére szolgál.

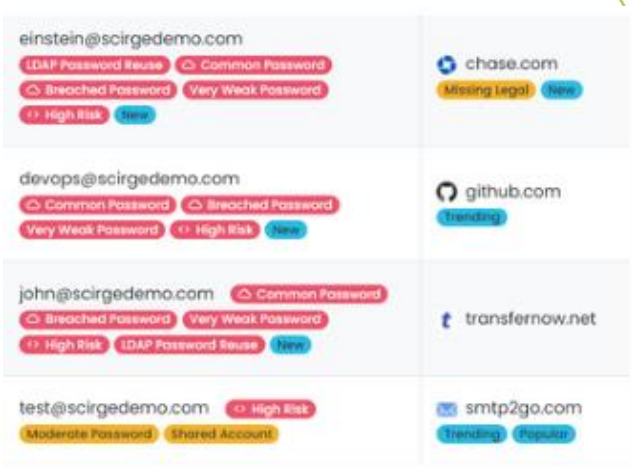


Applications Inventory

Active Directory jelszó higiénia

Active Directory vagy egyéb LDAP jelszavak ugyanazon a folyamaton mennek keresztül, mint bármely más fiók, lehetővé téve a megfelelőség és a védelem összetettségének ellenőrzését.

A harmadik fél web-alkalmazásaiban újra felhasznált Active Directory jelszavak azonosítása fontos pont, mivel az ellopott hitelesítő adatok hozzájárulnak a sikeres támadások közel 80%-ához, beleértve a zsarolóprogramok telepítését is.

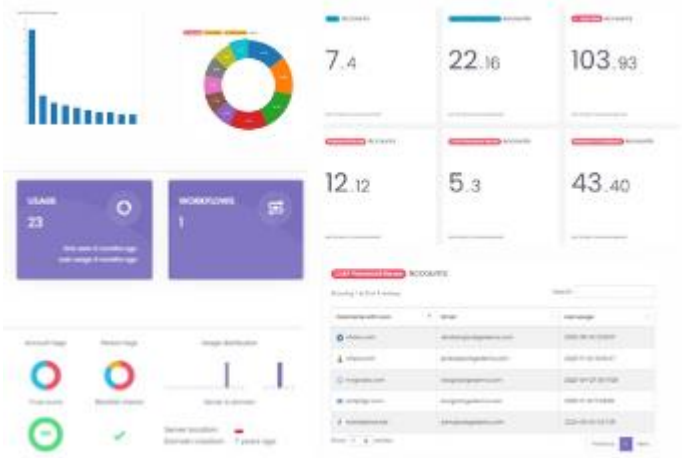


Azonnali felderítés

A Scirge felderítési metódusa egy könnyű funkció, amely segít a szervezeteknek azonnal felmérni történelmi Shadow IT lábnyomukat a böngészőelőzmények és a böngésző által mentett fiókok elemzésével. Ez lehetővé teszi a Shadow IT auditálását és értékelését termékintegráció nélkül. A jelentések megmutatják a felfedezett alkalmazások számát, a mentett fiókok pedig pontosan megmutatják, hogy mely alkalmazások és jelszavak lehetnek sebezhetőek.

Megfelelés és kockázat

A nem kezelt, harmadik féltől származó Általános Szerződési Feltételek és irányelvek a földrajzi és bizalmi adatokkal együtt felsorolásra kerülnek, hogy kontextust biztosítsanak a kockázatértékelésekhez és auditokhoz. Az automatizált figyelmeztetések és jelentések lehetővé teszik az érintettek számára, hogy naprakészek maradjanak a szervezeten belüli Shadow IT eszközökről. A fiókmegosztási és használati trendek láthatósága lehetővé teszi a visszaélések vagy belső csalások korai felismerését. Az offboard folyamatokat kiterjesztik a nem engedélyezett szolgáltatásokra és identitásokra is.



Felhasználói oktatás

Az eltérő osztályok, tapasztalat és szakmai háttér más megközelítést igényel az oktatásban. A Scirge lehetővé teszi az oktatási üzenetek testreszabását a triggerek és a közönség alapján.

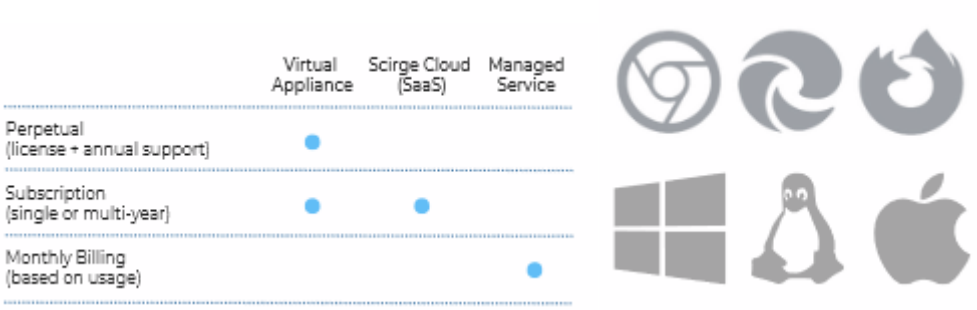
Az informatikai osztály rossz jelszó higiéniájára vonatkozó figyelmeztetések további hangsúlyt igényelhetnek, míg a nem informatikai szakemberekre vonatkozó összetettségi követelményeknek rendkívül világosnak és egyszerűnek kell lenniük.

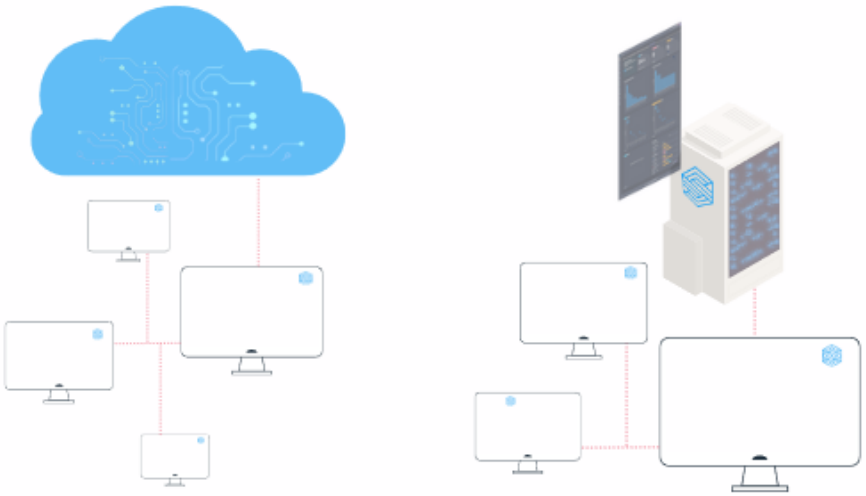
Implementációs lehetőségek

A Scirge egy könnyű végpont-összetevővel rendelkezik böngészőbővítmény formájában. Feladata a fiók- és alkalmazáshasználat figyelése vállalati e-mail-címeken és hitelesítő adatokon keresztül, valamint központilag felügyelt házirendek alapján végzett műveletek végrehajtása.

A kezelés és a konfiguráció natív felhőszolgáltatásként vagy helyszíni telepítésként (on-premise) érhető el. A menedzselt szolgáltatás opció is elérhető a régiótól függően. A Horizon Cloud Intelligence szolgáltatások minden esetben elérhetőek az adatok bővítéséhez.

A Chrome, Edge és Firefox böngészőket minden fő végpont operációs rendszer támogatja.





Biztonság és adatvédelem

A végpontok a kezelt házirendek által szabályozott adatok korlátozott körét gyűjtik. A cleartext jelszavakat soha nem tárolják, a végpontokon, az átvitel során és a szerveren végzett kivonatolás és titkosítás biztosítja a legmagasabb szintű adatvédelmi és adatvédelmi szabványokat.

Az adatvédelmi lehetőségek kapcsán bővebb információ a gyártó honlapján érhető el.

Összefoglaló

A Shadow IT Discovery segít feltárni a szervezet informatikai lábnyomának és ellátási láncának legkevésbé ismert sarkait. A Scirge olyan oktatást kínál, amely a viselkedést célozza meg, és korai figyelmeztetéseket a felmerülő fenyegetésekre.

IT vezetés

Az agilitás és a digitalizáció nem valósulhat meg egyéni kezdeményezés nélkül. Az üzleti osztályok nem oszthatják meg a tudást, miközben az informatikának láthatóságra van szüksége ahhoz, hogy támogassa a nem informatikai részlegek innovációját.

A Shadow IT Discovery segít feltárni a feltörekvő trendeket és az örökölt vagy elhagyott szolgáltatásokat, amelyek támogatási, biztonsági vagy pénzügyi szempontból figyelmet igényelnek.

Koczkázat és megfelelőség

A szabályozások és biztonsági keretrendszerek az Ön eszközeinek leltárán és azok kockázat-érték profilján alapulnak. A Shadow IT teljesen elérhetetlen a kockázatelemzés számára anélkül, hogy konkrét, célzott erőfeszítéseket tenne a láthatóság megteremtésére.

A Scirge felsorolja a nem felügyelt alkalmazásokat és fiókokat, és kontextust ad a használatukhoz és a kockázatokhoz. A személyre szabott, figyelemfelkeltő üzenetek segítenek javítani a különböző műszaki ismeretekkel és háttérrel rendelkező alkalmazottak biztonsági szokásait.

Biztonsági osztályok

A hitelesítő adatok újrafelhasználása és visszaélése a zsarolóvírusok telepítésének és a sikeres jogsértéseknek az első számú tényezője. A legtöbb nem kezelt jelszó és azonosító a Shadow IT-ből származik, ahol a modern hitelesítési módszerek nem kényszeríthetők ki.