

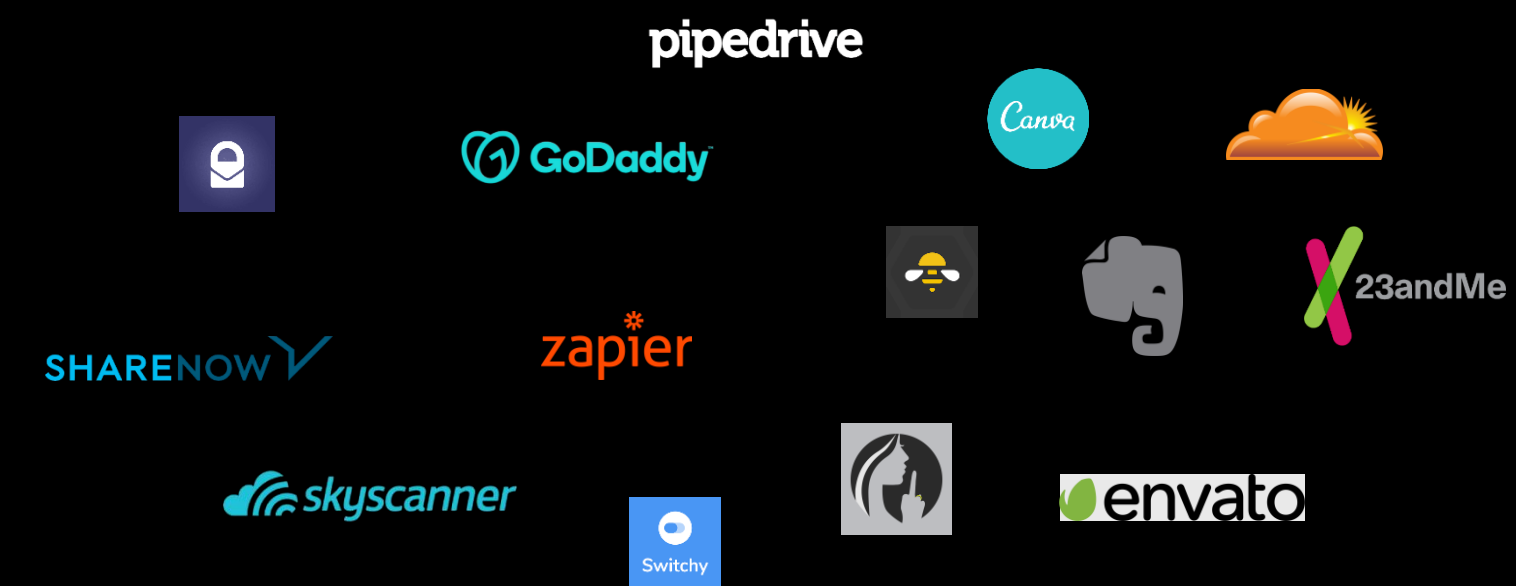


SCIRGE

UNVEIL + CONTROL ALL BUSINESS WEB APP REGS & LOGINS

СЕРЬЕЗНЫЕ СЕРВИСЫ

И... ВСЕ ОСТАЛЬНЫЕ



Ведут журнал действий
Интегрируются с IDM/PAM
Есть защита от утечек
Ролевая модель доступа
Парольная политика и 2FA

Введите ваш E-mail
Введите ваш пароль

СПЕЦИАЛИСТЫ ИБ
НЕДООЦЕНИВАЮТ КОЛИЧЕСТВО
УЧЕТНЫХ ЗАПИСЕЙ НА
СОТРУДНИКА В 15-22Х

CISCO

191

Среднее количество учеток на сотрудника
(2020 Digital Shadows)

А ЧЕГО В ЭТОМ ПЛОХОГО?

Риски, связанные с учетками

„80% ВЗЛОМОВ
КОРПОРАТИВНЫХ СЕТЕЙ
СВЯЗАНЫ С УТЕКШИМИ ИЛИ
ПОДОБРАННЫМИ ПАРОЛЯМИ”

IBM, Verizon, DBIR 2018- 2020

ВЗЛАМЫВАЮТ ВСЕХ

```

247253 gcolejhon@yahoo "h!5
247254 gcolejrl3@bel irtboy
247255 gcolejrl@vericole2
247256 gcolejrl6@gmail
247257 gcolejrl@comca 2000
247258 gcolejrl@msn.c
247259 gcolejrl@opton gcole
247260 gcolejrl@wow
247261 gcolekiwiboy@ 822949 cyrax0007@ma
247262 gcolekk3@hotmail 822950 butamuh11111
247263 gcolel@hotmail 822951 skhavelin@ma
247264 gcolel@hotmail 822952 sanya_gostev
247265 gcolela@yahoo 822953 s.lilz3000@m
247266 gcoleline@yah 822954 danila.curov
247267 gcolell@hotmail 822955 pavelastor@m
247268 gcolell@yahoo 822956 vitalik.voro
247269 gcolella01@sn 822957 ivan.filatov
247270 gcolella12@yal 822958 slepik@mail.
247271 gcolella1@ver 822959 Artem Bystro
247272 gcolella33@yal 822960 dan3994@yand
247273 gcolella44@ao 822961 mcherunet@bk
247274 gcolella78@ho 822962 s.druzhik@ya
247275 gcolella@bell 822963 vowa.ziberov
247276 gcolella@cisco 822964 tat-chupina@
247277 gcolella@cisco 822965 pohuist228@m
247278 gcolella@cisco 822966 kirille11111
247279 gcolella@cisco 822967 bagzhan@mail
247280 gcolella@cisco 822968 starshinina.j
247281 gcolella@cisco 822969 dsvinukhov20
247282 gcolella@cisco 822970 Zevson123@ya
247283 gcolella@cisco 822971 eduard.urazi
247284 gcolella@cisco 822972 cafeterio@ma
247285 gcolella@cisco 822973 pepelev1999@
247286 gcolella@cisco 822974 VAKARCHYK909
247287 gcolella@cisco 822975 spokky_196@m
247288 gcolella@cisco 822976 erlan.kaipov
247289 gcolella@cisco 822977 resid@mail.
247290 gcolella@cisco 822978 ershov-al-vl
247291 gcolella@cisco 822979 tuz21021997@
247292 gcolella@cisco 822980 www.nikita.2
247293 gcolella@cisco 822981 biberoff2017

```

Database Name ↓
myspace.com
linkedin.com
adobe.com
vk.com
tumblr.com
twitter.com
neopets.com
dropbox.com
gmail.com
imesh.com

Database Name	Date Indexed	Record Count
melco-resorts.com	2021-09-30	34,067,773
hootvpn.com	2021-09-30	121
weleakinfo.com	2021-09-30	23,881
harborvpnapp.com	2021-09-30	88
nomer.io	2021-09-30	3,751,654
androidlista.com	2021-09-30	6,592,434
hideandseek.online	2021-09-30	230
lyf.app	2021-09-30	227,124
realgm.com	2021-09-30	116,949
cpfl.com.br	2021-09-30	92,669
sofascore.com	2021-09-30	262,390
lolhentai.net	2021-09-23	84,446
fenlink.net	2021-09-23	51,845
couple.uk	2021-09-23	29,698
dood.com	2021-09-23	18,395
habibs.com.br	2021-09-23	3,934,847
hiphopforum.sk	2021-09-23	109,462
indiamart.com	2021-09-14	6,161,866
temeoo.com	2021-09-14	62,520
gemplex.tv	2021-09-14	4,624,555

РИСКИ ДЛЯ БИЗНЕСА

Получение доступа к сети

Кража данных

Потеря денег и удар по репутации

Юридические риски

Атака на клиентов

Остановка бизнеса

1.2. In summary, between 22 June and 5 September 2018, a malicious actor ("the **Attacker**") gained access to an internal BA application through the use of compromised credentials for a Citrix remote access gateway ("**CAG**"). [REDACTED]
[REDACTED]
[REDACTED] After gaining access to the wider network,

British Airways оштрафованы на £20.000.000

(<https://ico.org.uk/action-weve-taken/enforcement/british-airways/>)

ТЕНЕВОЕ IT: НЕКОНТРОЛИРУЕМЫЕ УЧЕТКИ

Используемые сервисы не согласовываются

Учетные записи не контролируются ИТ/ИБ

Сотрудники сохраняют доступ после увольнения

Менеджеры паролей не решают проблему

СУТЬ РЕШЕНИЯ ОТ SCIRGE

Целевым сотрудникам на корпоративных рабочих станциях устанавливается специальное расширение для браузера, которое:

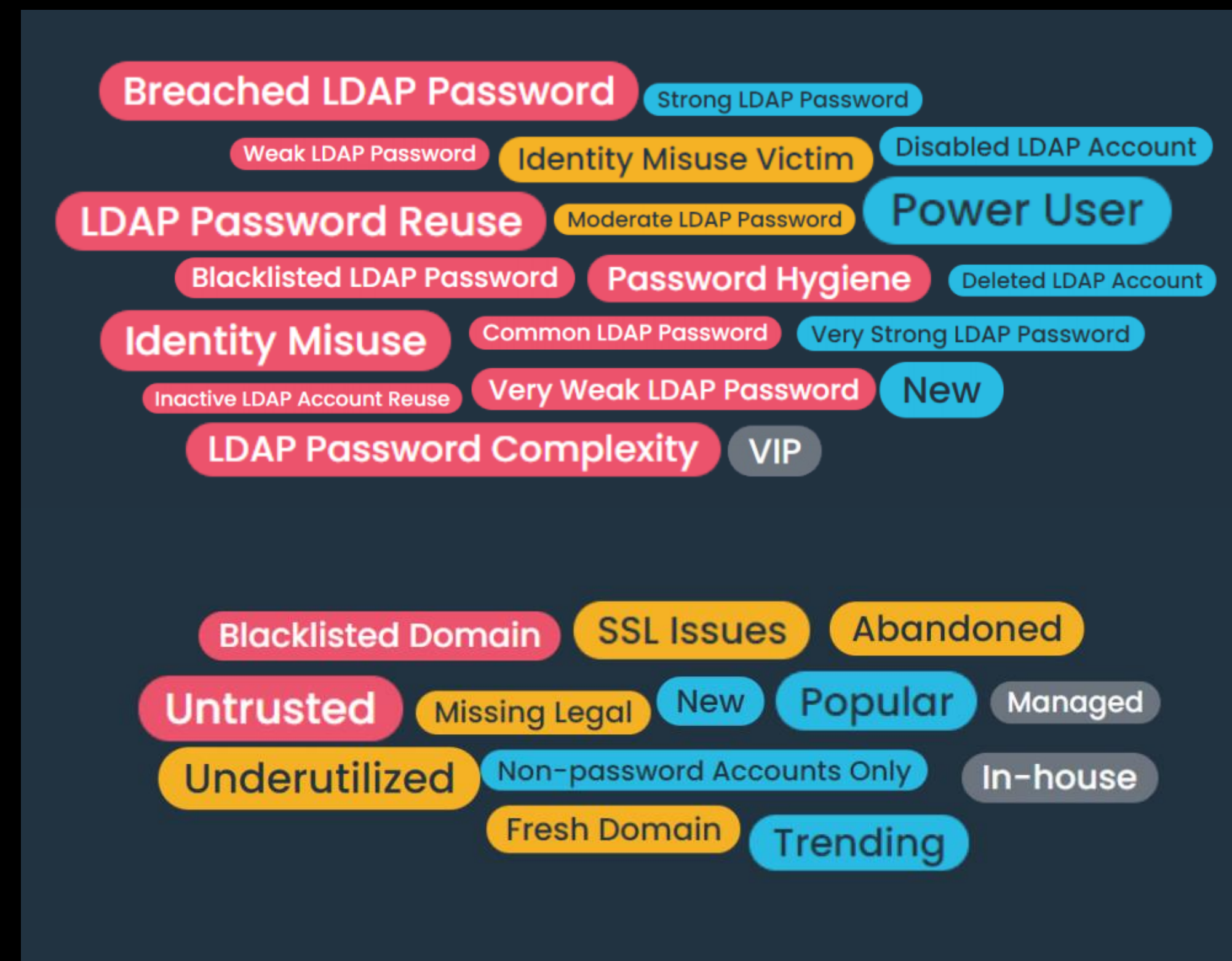
- Обнаруживает использование корпоративных учетных записей на внешних веб-сайтах
- Предупреждает о вводе слишком простого или уже использованного пароля
- Не дает ввести пароль на фишинговых веб-сайтах
- Обучает сотрудников через баннеры на посещаемых веб-сайтах

App	Accounts	People	Usage
komus.ru Underutilized	2	3	28
afi-d.ru Underutilized Missing Legal Abandoned	2	2	17
lancloud.ru Underutilized Missing Legal Abandoned	1	1	4
10.10.13.122 Underutilized Abandoned	2	1	10
gfi.com Underutilized Abandoned	4	2	8
altaro.com Underutilized Abandoned	2	1	2
ivi.ru Underutilized Abandoned	2	1	2
live.com Missing Legal Underutilized Abandoned	2	1	3
invicti.com Missing Legal Underutilized Abandoned	1	1	1
office365.com Non-password Accounts Only	1	1	2
yandex.ru Underutilized Abandoned	3	1	3
habr.com Underutilized Missing Legal Abandoned Popular	12	2	31

СУТЬ РЕШЕНИЯ ОТ SCIRGE

Анализирует полученные данные и сообщает о случаях, когда:

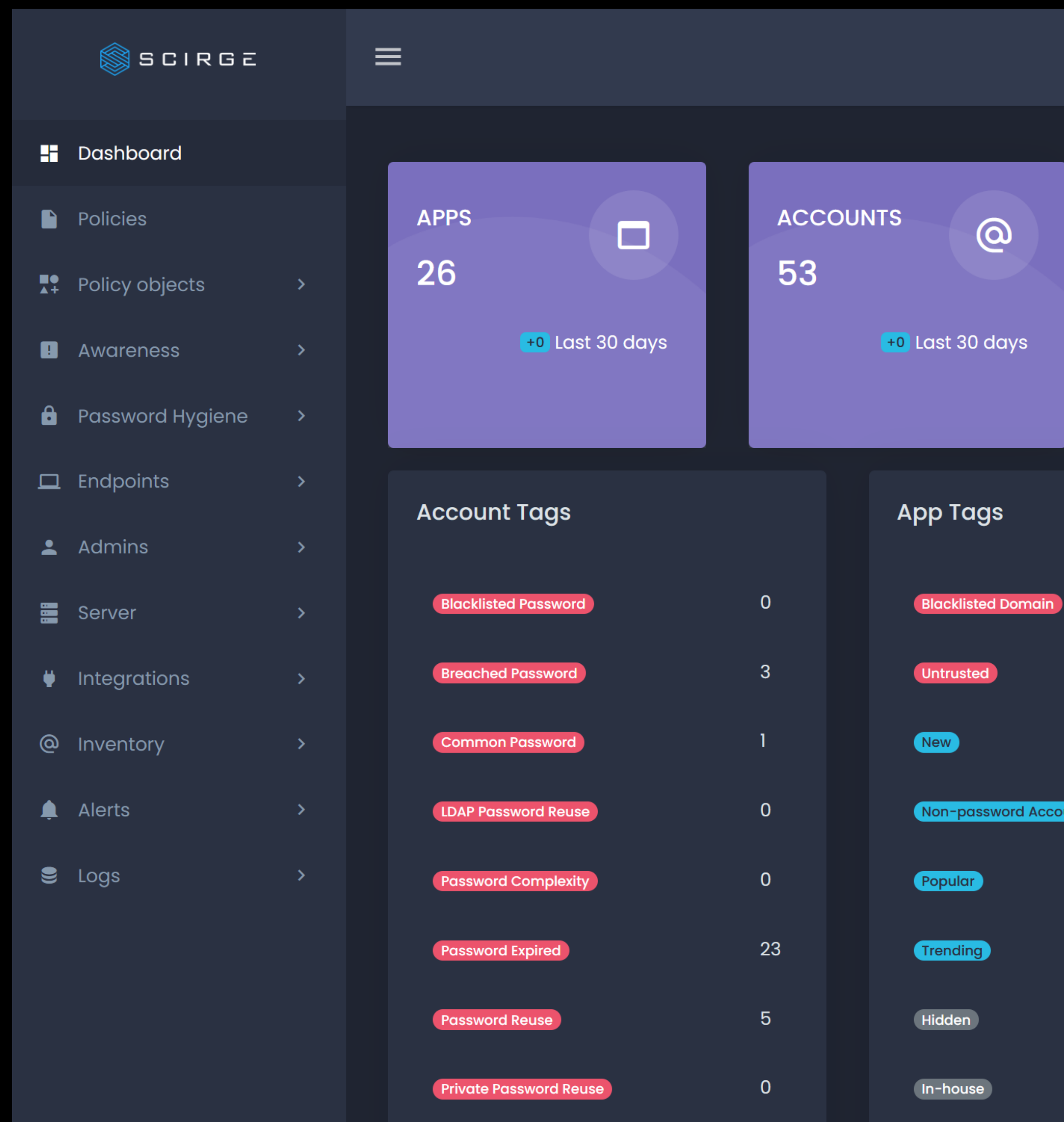
- пароль не соответствует уровню сложности
- такой же пароль используется другим сотрудником или от другой учетки
- выполнен вход (попытка входа) на веб-сайте с низким уровнем доверия
- пользователь использовал чужую учетную запись
- учетная запись давно не использовалась
- и так далее



СУТЬ РЕШЕНИЯ ОТ SCIRGE

Решение создано для корпоративного использования:

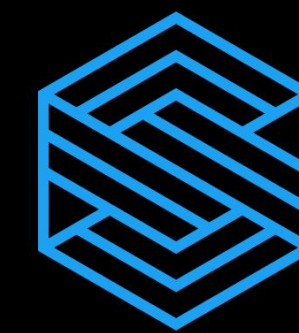
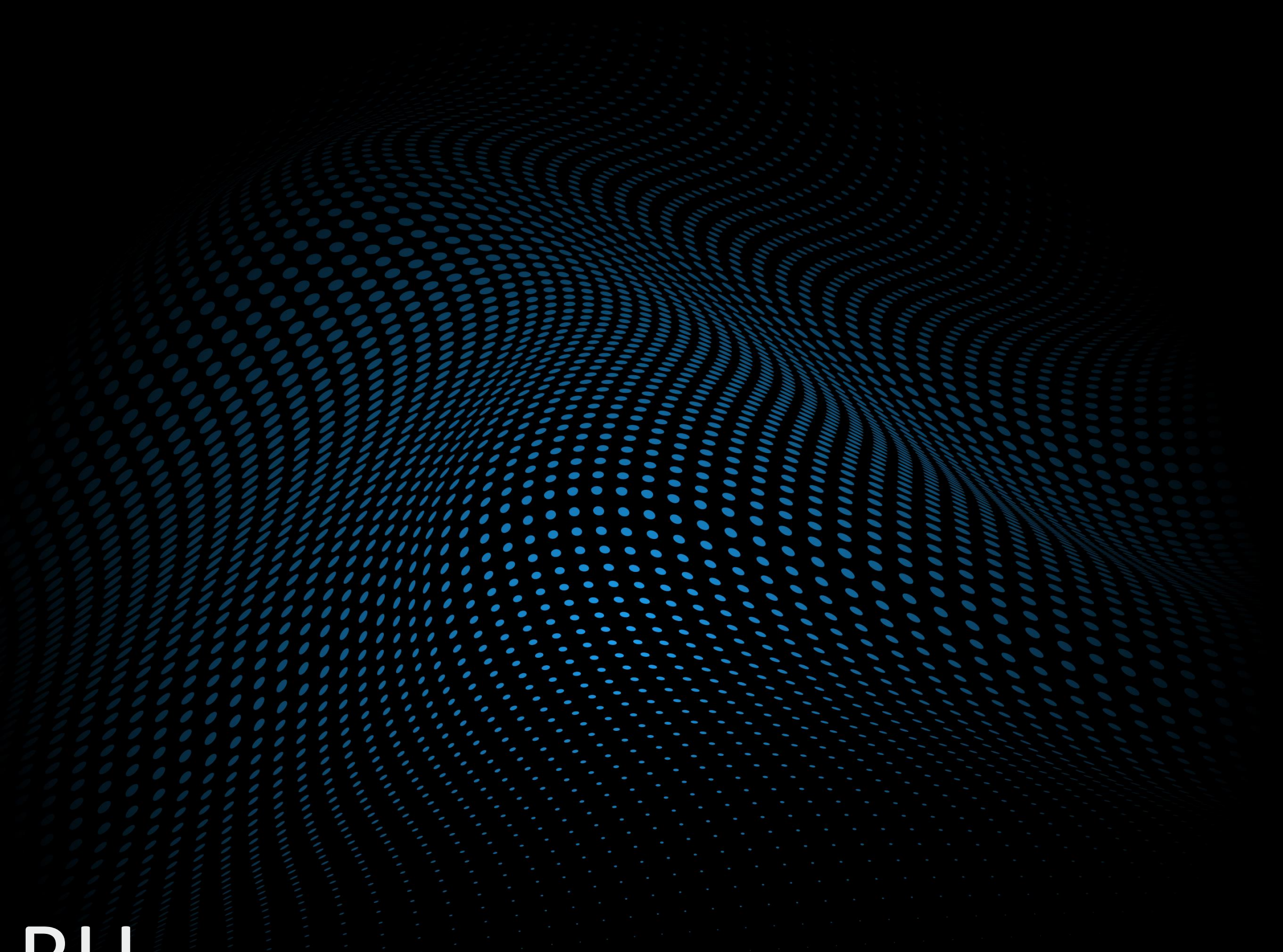
- Релевая модель доступа и анонимизации данных
- Интеграция с LDAP и SIEM
- Оповещения и отчетность
- Инвентаризация учеток, подключенных браузеров
- Тонкая настройка меток для быстрого поиска
- Установка корпоративных сертификатов доверия
- Установка расширения через групповые политики



SCIRGE ПОДХОДИТ ДЛЯ СЕТЕЙ ЛЮБЫХ РАЗМЕРОВ

Для уязвимого SMB с 10-100 сотрудниками

Для крупных компаний до 10.000 сотрудников



SCIRGE
UNVEIL + CONTROL ALL BUSINESS WEB APP REGS & LOGINS

SCIRGE.RU

INFO@SCIRGE.RU