SILVERFORT

Единая платформа защиты учетных данных

Без агентов, без прокси и без ограничений

ДиалогНаука

Повестка

- Актуальность защиты УЗ
- Традиционные решения МФА
- Silverfort. Архитектура и ключевые отличия
- Демо
- Вопросы и ответы

О компании Silverfort

Заказчики

- Банки
- Здравоохранение
- Ритейл
- Нефтегаз
- Телеком
- Медиа
- ИТ
- Промышленность

Статистика

- Основана в 2016
- Инвестиции $41.5M
- Крупнейшие инвесторы (Сити)
- Глобальная поддержка 24x7, русскоязычный TAM

451 Research FIRESTARTER
CNBC UPSTART100 2018
CYBER SECURITY EXCELLENCE AWARDS WINNER 2018
THE CHANNEL CO. CRN EMERGING VENDORS 2019
INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019
Gartner COOL VENDOR 2019

Microsoft paloalto NETWORKS CYBERARK okta
Check Point SOFTWARE TECHNOLOGIES LTD. cisco FORTINET RSA yubico

SILVERFORT

Типичные задачи и проблемы

Незащищаемые критические системы

Миграция МФА в облака

Латеральное движение не смотря на все купленные СЗИ

Незащищенные сервисные УЗ

Существующая система МФА мешает бизнесу

Атаки с использованием УЗ растут

Более 80% всех взломов и 77% взломов облаков использовали украденные аккаунты

Отчет о расследовании взломов Verizon (DBIR), 2020

verizon

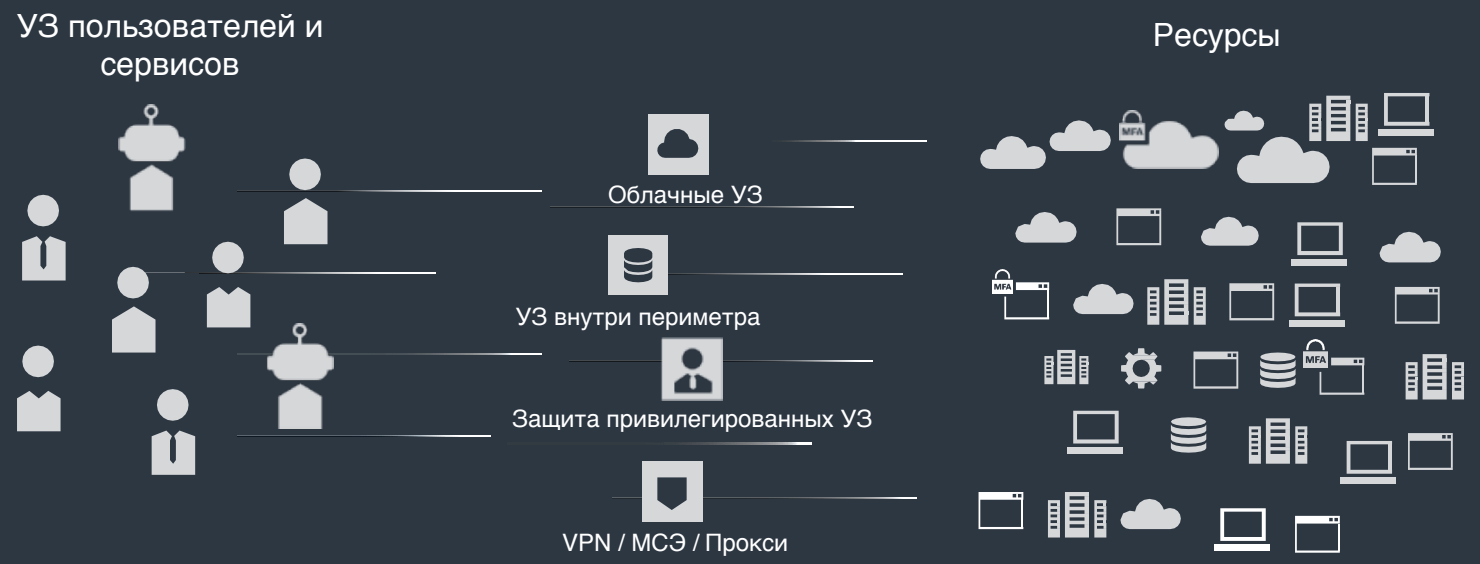
Вероятность взлома вашего аккаунта ниже на 99,9%, если вы используете МФА

Алекс Вейнерт, Менеджер программы, Защита УЗ

Microsoft

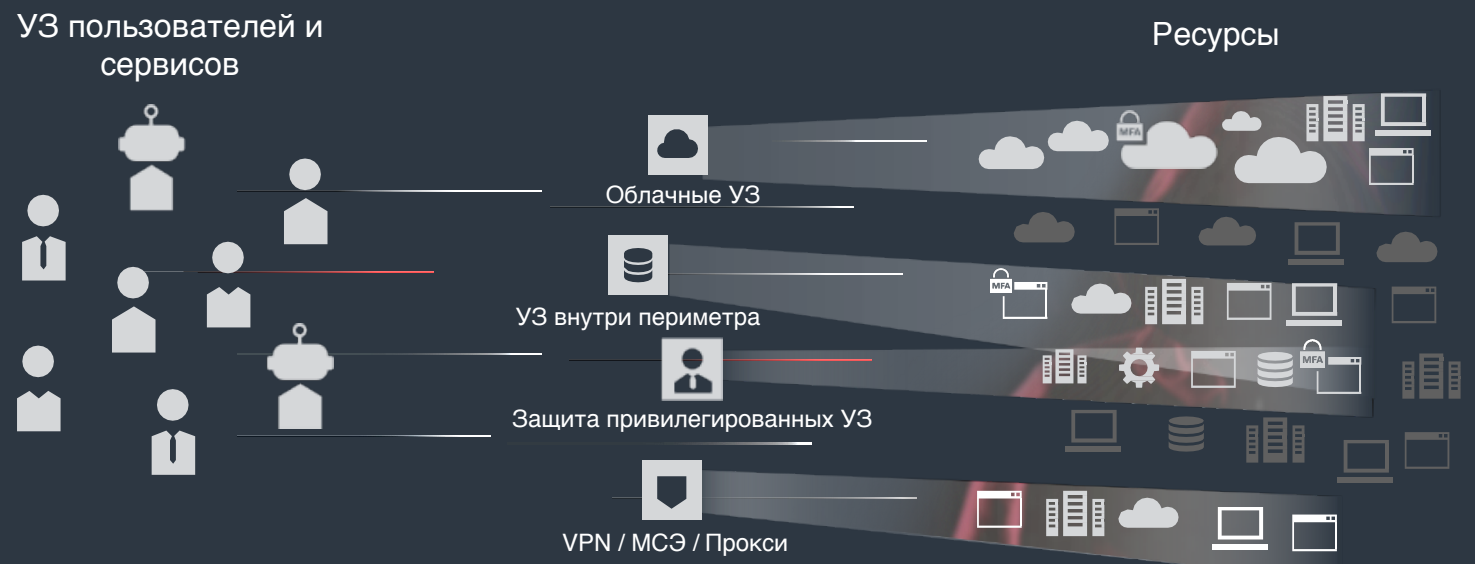
Большинство компаний уже используют МФА и аналогичные СЗИ.
Так почему же атаки на УЗ остаются проблемой?

Множество разных МФА-решений



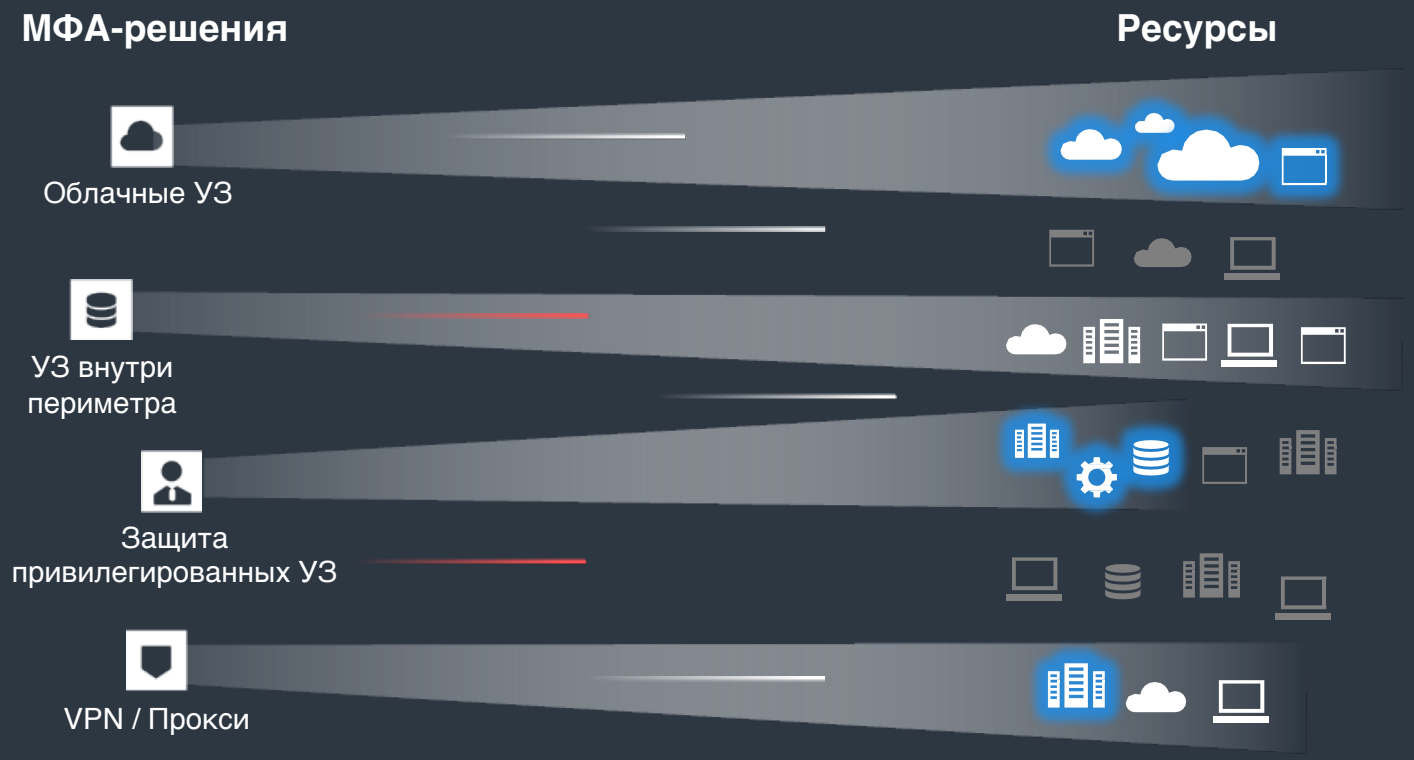
SILVERFORT

Мониторинг и защита – точечные и неполные



SILVERFORT

99% систем используют незащищаемые протоколы



SILVERFORT

1. alerter/tgr-dc1
2. alerter/tgr-dc1.tgr.local
3. alerter/tgr-dc1.tgr.local/tgr
4. alerter/tgr-dc1.tgr.local/tgr.local
5. alerter/tgr-dc1/tgr
6. appmgmt/tgr-dc1
7. appmgmt/tgr-dc1.tgr.local
8. appmgmt/tgr-dc1.tgr.local/tgr
9. appmgmt/tgr-dc1.tgr.local/tgr.local
10. appmgmt/tgr-dc1/tgr
11. browser/tgr-dc1
12. browser/tgr-dc1.tgr.local
13. browser/tgr-dc1.tgr.local/tgr
14. browser/tgr-dc1.tgr.local/tgr.local
15. browser/tgr-dc1/tgr
16. cifs/tgr-dc1
17. cifs/tgr-dc1.tgr.local
18. cifs/tgr-dc1.tgr.local/tgr
19. cifs/tgr-dc1.tgr.local/tgr.local
20. cifs/tgr-dc1/tgr
21. cisvc/tgr-dc1
22. cisvc/tgr-dc1.tgr.local
23. cisvc/tgr-dc1.tgr.local/tgr
24. cisvc/tgr-dc1.tgr.local/tgr.local
25. cisvc/tgr-dc1/tgr
26. clipsrv/tgr-dc1
27. clipsrv/tgr-dc1.tgr.local
28. clipsrv/tgr-dc1.tgr.local/tgr
29. clipsrv/tgr-dc1.tgr.local/tgr.local
30. clipsrv/tgr-dc1/tgr
31. dcom/tgr-dc1
32. dcom/tgr-dc1.tgr.local
33. dcom/tgr-dc1.tgr.local/tgr
34. dcom/tgr-dc1.tgr.local/tgr.local
35. dcom/tgr-dc1/tgr
36. dfsr-12f9a27c-bf97-4787-9364-d31b6c55eb04/tgr-dc1.tgr.local
37. dhcp/tgr-dc1
38. dhcp/tgr-dc1.tgr.local
39. dhcp/tgr-dc1.tgr.local/tgr
40. dhcp/tgr-dc1.tgr.local/tgr.local
41. dhcp/tgr-dc1/tgr
42. dmserver/tgr-dc1
43. dmserver/tgr-dc1.tgr.local
44. dmserver/tgr-dc1.tgr.local/tgr
45. dmserver/tgr-dc1.tgr.local/tgr.local
46. dmserver/tgr-dc1/tgr
47. dns/tgr-dc1
48. dns/tgr-dc1.tgr.local
49. dns/tgr-dc1.tgr.local/tgr
50. dns/tgr-dc1.tgr.local/tgr.local
51. dns/tgr-dc1/tgr
52. dnscache/tgr-dc1
53. dnscache/tgr-dc1.tgr.local
54. dnscache/tgr-dc1.tgr.local/tgr
55. dnscache/tgr-dc1.tgr.local/tgr.local
56. dnscache/tgr-dc1/tgr
57. e3514235-4b06-11d1-ab04-00c04fc2dcd2/aa967939-03f5-4d49-8592-3e0acc3c23fa/tgr.local
58. eventlog/tgr-dc1
59. eventlog/tgr-dc1.tgr.local
60. eventlog/tgr-dc1.tgr.local/tgr
61. eventlog/tgr-dc1.tgr.local/tgr.local
62. eventlog/tgr-dc1/tgr
63. eventsystem/tgr-dc1
64. eventsystem/tgr-dc1.tgr.local
65. eventsystem/tgr-dc1.tgr.local/tgr
66. eventsystem/tgr-dc1.tgr.local/tgr.local
67. eventsystem/tgr-dc1/tgr
68. exchangeab/tgr-dc1
69. exchangeab/tgr-dc1.tgr.local
70. fax/tgr-dc1
71. fax/tgr-dc1.tgr.local
72. fax/tgr-dc1.tgr.local/tgr
73. fax/tgr-dc1.tgr.local/tgr.local
74. fax/tgr-dc1/tgr
75. gc/tgr-dc1.tgr.local/tgr.local
76. host/tgr-dc1
77. host/tgr-dc1.tgr.local
78. host/tgr-dc1.tgr.local/tgr
79. host/tgr-dc1.tgr.local/tgr.local
80. host/tgr-dc1/tgr
81. http/tgr-dc1
82. http/tgr-dc1.tgr.local
83. http/tgr-dc1.tgr.local/tgr
84. http/tgr-dc1.tgr.local/tgr.local
85. http/tgr-dc1/tgr
86. ias/tgr-dc1
87. ias/tgr-dc1.tgr.local
88. ias/tgr-dc1.tgr.local/tgr
89. ias/tgr-dc1.tgr.local/tgr.local
90. ias/tgr-dc1/tgr
91. iisadmin/tgr-dc1
92. iisadmin/tgr-dc1.tgr.local
93. iisadmin/tgr-dc1.tgr.local/tgr
94. iisadmin/tgr-dc1.tgr.local/tgr.local
95. iisadmin/tgr-dc1/tgr
96. ldap/aa967939-03f5-4d49-8592-3e0acc3c23fa._msdcs.tgr.local
97. ldap/tgr-dc1
98. ldap/tgr-dc1.tgr.local
99. ldap/tgr-dc1.tgr.local/domaindnszones.tgr.local
100. ldap/tgr-dc1.tgr.local/forestdnszones.tgr.local
101. ldap/tgr-dc1.tgr.local/tgr
102. ldap/tgr-dc1.tgr.local/tgr.local
103. ldap/tgr-dc1/tgr
104. mcsvc/tgr-dc1
105. mcsvc/tgr-dc1.tgr.local
106. mcsvc/tgr-dc1.tgr.local/tgr
107. mcsvc/tgr-dc1.tgr.local/tgr.local
108. mcsvc/tgr-dc1/tgr
109. messenger/tgr-dc1
110. messenger/tgr-dc1.tgr.local
111. messenger/tgr-dc1.tgr.local/tgr
112. messenger/tgr-dc1.tgr.local/tgr.local
113. messenger/tgr-dc1/tgr
114. msdtc/tgr-dc1
115. msdtc/tgr-dc1.tgr.local
116. msdtc/tgr-dc1.tgr.local/tgr
117. msdtc/tgr-dc1.tgr.local/tgr.local
118. msdtc/tgr-dc1/tgr
119. msiserver/tgr-dc1
120. msiserver/tgr-dc1.tgr.local
121. msiserver/tgr-dc1.tgr.local/tgr
122. msiserver/tgr-dc1.tgr.local/tgr.local
123. msiserver/tgr-dc1/tgr
124. netdde/tgr-dc1
125. netdde/tgr-dc1.tgr.local
126. netdde/tgr-dc1.tgr.local/tgr
127. netdde/tgr-dc1.tgr.local/tgr.local
128. netdde/tgr-dc1/tgr
129. netddedsm/tgr-dc1
130. netddedsm/tgr-dc1.tgr.local
131. netddedsm/tgr-dc1.tgr.local/tgr
132. netddedsm/tgr-dc1.tgr.local/tgr.local
133. netddedsm/tgr-dc1/tgr
134. netlogon/tgr-dc1
135. netlogon/tgr-dc1.tgr.local
136. netlogon/tgr-dc1.tgr.local/tgr
137. netlogon/tgr-dc1.tgr.local/tgr.local
138. netlogon/tgr-dc1/tgr
139. netman/tgr-dc1
140. netman/tgr-dc1.tgr.local
141. netman/tgr-dc1.tgr.local/tgr
142. netman/tgr-dc1.tgr.local/tgr.local
143. netman/tgr-dc1/tgr
144. nmagent/tgr-dc1
145. nmagent/tgr-dc1.tgr.local
146. nmagent/tgr-dc1.tgr.local/tgr
147. nmagent/tgr-dc1.tgr.local/tgr.local
148. nmagent/tgr-dc1/tgr
149. oakley/tgr-dc1
150. oakley/tgr-dc1.tgr.local
151. oakley/tgr-dc1.tgr.local/tgr
152. oakley/tgr-dc1.tgr.local/tgr.local
153. oakley/tgr-dc1/tgr
154. plugplay/tgr-dc1
155. plugplay/tgr-dc1.tgr.local
156. plugplay/tgr-dc1.tgr.local/tgr
157. plugplay/tgr-dc1.tgr.local/tgr.local
158. plugplay/tgr-dc1/tgr
159. policyagent/tgr-dc1
160. policyagent/tgr-dc1.tgr.local
161. policyagent/tgr-dc1.tgr.local/tgr
162. policyagent/tgr-dc1.tgr.local/tgr.local
163. policyagent/tgr-dc1/tgr
164. protectedstorage/tgr-dc1
165. protectedstorage/tgr-dc1.tgr.local
166. protectedstorage/tgr-dc1.tgr.local/tgr
167. protectedstorage/tgr-dc1.tgr.local/tgr.local
168. protectedstorage/tgr-dc1/tgr
169. rasman/tgr-dc1
170. rasman/tgr-dc1.tgr.local
171. rasman/tgr-dc1.tgr.local/tgr
172. rasman/tgr-dc1.tgr.local/tgr.local
173. rasman/tgr-dc1/tgr
174. remoteaccess/tgr-dc1
175. remoteaccess/tgr-dc1.tgr.local
176. remoteaccess/tgr-dc1.tgr.local/tgr
177. remoteaccess/tgr-dc1.tgr.local/tgr.local
178. remoteaccess/tgr-dc1/tgr
179. replicator/tgr-dc1
180. replicator/tgr-dc1.tgr.local
181. replicator/tgr-dc1.tgr.local/tgr
182. replicator/tgr-dc1.tgr.local/tgr.local
183. replicator/tgr-dc1/tgr
184. restrictedkrbhost/tgr-dc1
185. restrictedkrbhost/tgr-dc1.tgr.local
186. rpc/tgr-dc1
187. rpc/tgr-dc1.tgr.local
188. rpc/tgr-dc1.tgr.local/tgr
189. rpc/tgr-dc1.tgr.local/tgr.local
190. rpc/tgr-dc1/tgr
191. rpclocator/tgr-dc1
192. rpclocator/tgr-dc1.tgr.local
193. rpclocator/tgr-dc1.tgr.local/tgr
194. rpclocator/tgr-dc1.tgr.local/tgr.local
195. rpclocator/tgr-dc1/tgr
196. rpcss/tgr-dc1
197. rpcss/tgr-dc1.tgr.local
198. rpcss/tgr-dc1.tgr.local/tgr
199. rpcss/tgr-dc1.tgr.local/tgr.local
200. rpcss/tgr-dc1/tgr
201. rsvp/tgr-dc1
202. rsvp/tgr-dc1.tgr.local
203. rsvp/tgr-dc1.tgr.local/tgr
204. rsvp/tgr-dc1.tgr.local/tgr.local
205. rsvp/tgr-dc1/tgr
206. samss/tgr-dc1
207. samss/tgr-dc1.tgr.local
208. samss/tgr-dc1.tgr.local/tgr
209. samss/tgr-dc1.tgr.local/tgr.local
210. samss/tgr-dc1/tgr
211. scardsvr/tgr-dc1
212. scardsvr/tgr-dc1.tgr.local
213. scardsvr/tgr-dc1.tgr.local/tgr
214. scardsvr/tgr-dc1.tgr.local/tgr.local
215. scardsvr/tgr-dc1/tgr
216. scesrv/tgr-dc1
217. scesrv/tgr-dc1.tgr.local
218. scesrv/tgr-dc1.tgr.local/tgr
219. scesrv/tgr-dc1.tgr.local/tgr.local
220. scesrv/tgr-dc1/tgr
221. schedule/tgr-dc1
222. schedule/tgr-dc1.tgr.local
223. schedule/tgr-dc1.tgr.local/tgr
224. schedule/tgr-dc1.tgr.local/tgr.local
225. schedule/tgr-dc1/tgr
226. scm/tgr-dc1
227. scm/tgr-dc1.tgr.local
228. scm/tgr-dc1.tgr.local/tgr
229. scm/tgr-dc1.tgr.local/tgr.local
230. scm/tgr-dc1/tgr
231. seclogon/tgr-dc1
232. seclogon/tgr-dc1.tgr.local
233. seclogon/tgr-dc1.tgr.local/tgr
234. seclogon/tgr-dc1.tgr.local/tgr.local
235. seclogon/tgr-dc1/tgr
236. snmp/tgr-dc1
237. snmp/tgr-dc1.tgr.local
238. snmp/tgr-dc1.tgr.local/tgr
239. snmp/tgr-dc1.tgr.local/tgr.local
240. snmp/tgr-dc1/tgr
241. spooler/tgr-dc1
242. spooler/tgr-dc1.tgr.local
243. spooler/tgr-dc1.tgr.local/tgr
244. spooler/tgr-dc1.tgr.local/tgr.local
245. spooler/tgr-dc1/tgr
246. tapisrv/tgr-dc1
247. tapisrv/tgr-dc1.tgr.local
248. tapisrv/tgr-dc1.tgr.local/tgr
249. tapisrv/tgr-dc1.tgr.local/tgr.local
250. tapisrv/tgr-dc1/tgr
251. termsrv/tgr-dc1
252. termsrv/tgr-dc1.tgr.local
253. tgr-dc1
254. tgr-dc1$
255. time/tgr-dc1
256. time/tgr-dc1.tgr.local
257. time/tgr-dc1.tgr.local/tgr
258. time/tgr-dc1.tgr.local/tgr.local
259. time/tgr-dc1/tgr
260. trksvr/tgr-dc1
261. trksvr/tgr-dc1.tgr.local
262. trksvr/tgr-dc1.tgr.local/tgr
263. trksvr/tgr-dc1.tgr.local/tgr.local
264. trksvr/tgr-dc1/tgr
265. trkwks/tgr-dc1
266. trkwks/tgr-dc1.tgr.local
267. trkwks/tgr-dc1.tgr.local/tgr
268. trkwks/tgr-dc1.tgr.local/tgr.local
269. trkwks/tgr-dc1/tgr
270. ups/tgr-dc1
271. ups/tgr-dc1.tgr.local
272. ups/tgr-dc1.tgr.local/tgr
273. ups/tgr-dc1.tgr.local/tgr.local
274. ups/tgr-dc1/tgr
275. w3svc/tgr-dc1
276. w3svc/tgr-dc1.tgr.local
277. w3svc/tgr-dc1.tgr.local/tgr
278. w3svc/tgr-dc1.tgr.local/tgr.local
279. w3svc/tgr-dc1/tgr
280. wins/tgr-dc1
281. wins/tgr-dc1.tgr.local
282. wins/tgr-dc1.tgr.local/tgr
283. wins/tgr-dc1.tgr.local/tgr.local
284. wins/tgr-dc1/tgr
285. wsman/tgr-dc1
286. wsman/tgr-dc1.tgr.local
287. www/tgr-dc1
288. www/tgr-dc1.tgr.local
289. www/tgr-dc1.tgr.local/tgr
290. www/tgr-dc1.tgr.local/tgr.local
291. www/tgr-dc1/tgr

Проблемы традиционных МФА

Характеристика	Традиционные МФА
Архитектура	Требует установки агента, прокси или интеграции с **каждой отдельной** защищаемой машиной. **Если агент удален – защиты нет**
Защита протоколов интерактивного входа (RDP и аналоги)	**Да, если существует агент или интеграция**
Защита всех других протоколов (более 100 для Windows, в том числе протоколы командной строки psexec / smb, wmi, powershell, которые обычно и используют злоумышленники)	**Нет**
Защита систем и устройств, на которые нельзя установить агент (IoT / OT, гипервизоры, legacy, file shares, самописное ПО и пр.)	**Нет**
Защита сервисных УЗ	**Нет**
Мониторинг и анализ всех попыток аутентификации и доступа ко всем ресурсам во всех средах организации	**Нет**
Адаптивная политика МФА на основе AI, уровня риска , без закидывания пользователей постоянными запросами на второй фактор	**Нет**
Выявление и блокирование атак на УЗ (аномалии, брутфорс по множеству ПК, криптолокеры, нацеленные хакеры и пр.)	**Нет**
Единая система аутентификации для всех кейсов (VPN, Windows, Linux, облака, веб и пр.)	**Нет**
Простота лицензирования, отсутствие множества модулей для разных протоколов	**Нет**

Silverfort

Анализ всех событий аутентификации и доступа, во всех средах

SILVERFORT

Silverfort

Комплексная защита УЗ, консолидация МФА, без агентов и прокси

Стратегия Silverfort

Повышение защищенности

Анализ доступа во ВСЕХ средах

Предотвращение атак на УЗ в реальном времени

Защита всех систем и интерфейсов

Уменьшение неудобства

Избежание усталости от МФА

Единый подход к МФА для разных систем

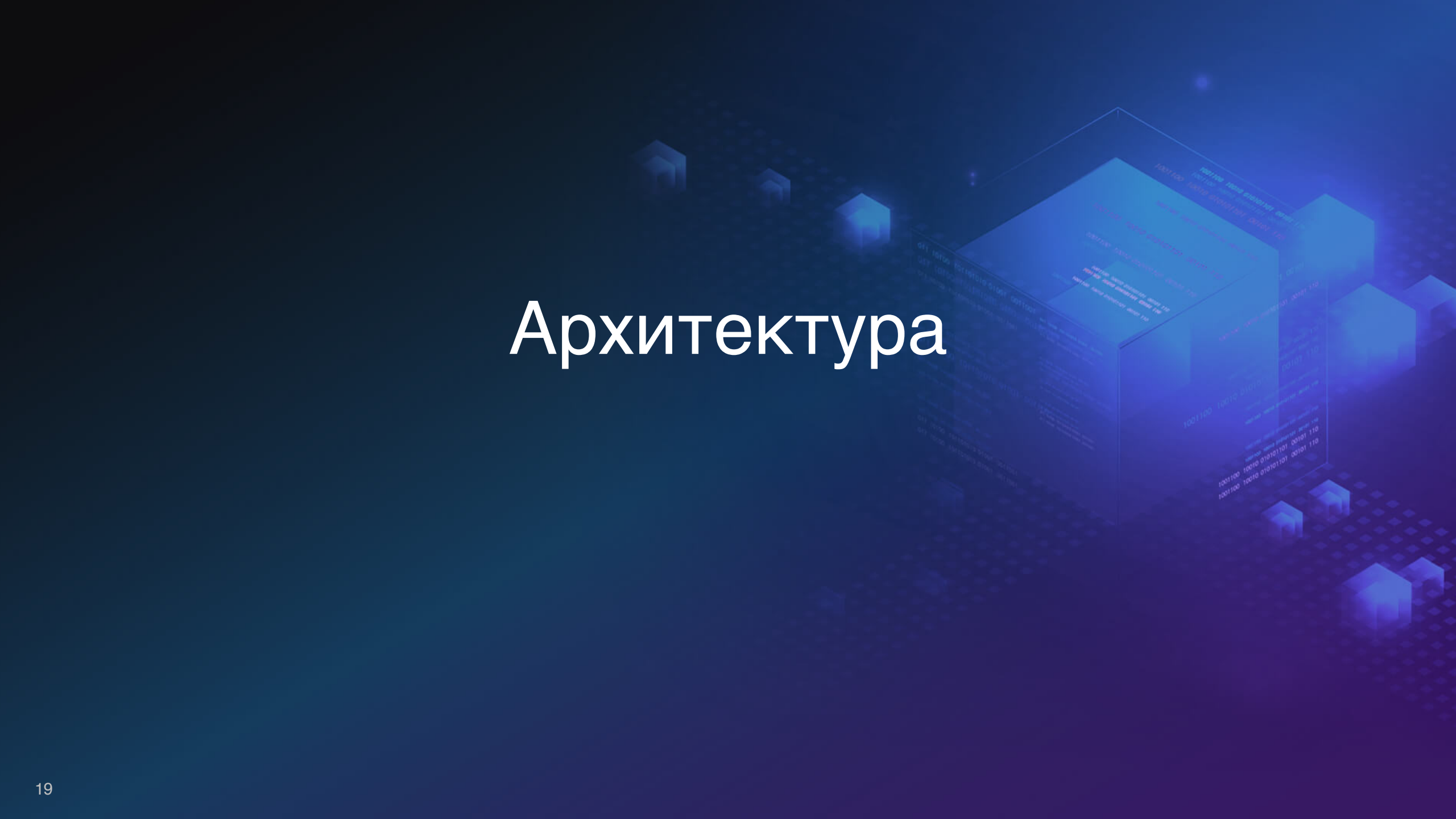
Снижение расходов

Консолидация систем защиты УЗ

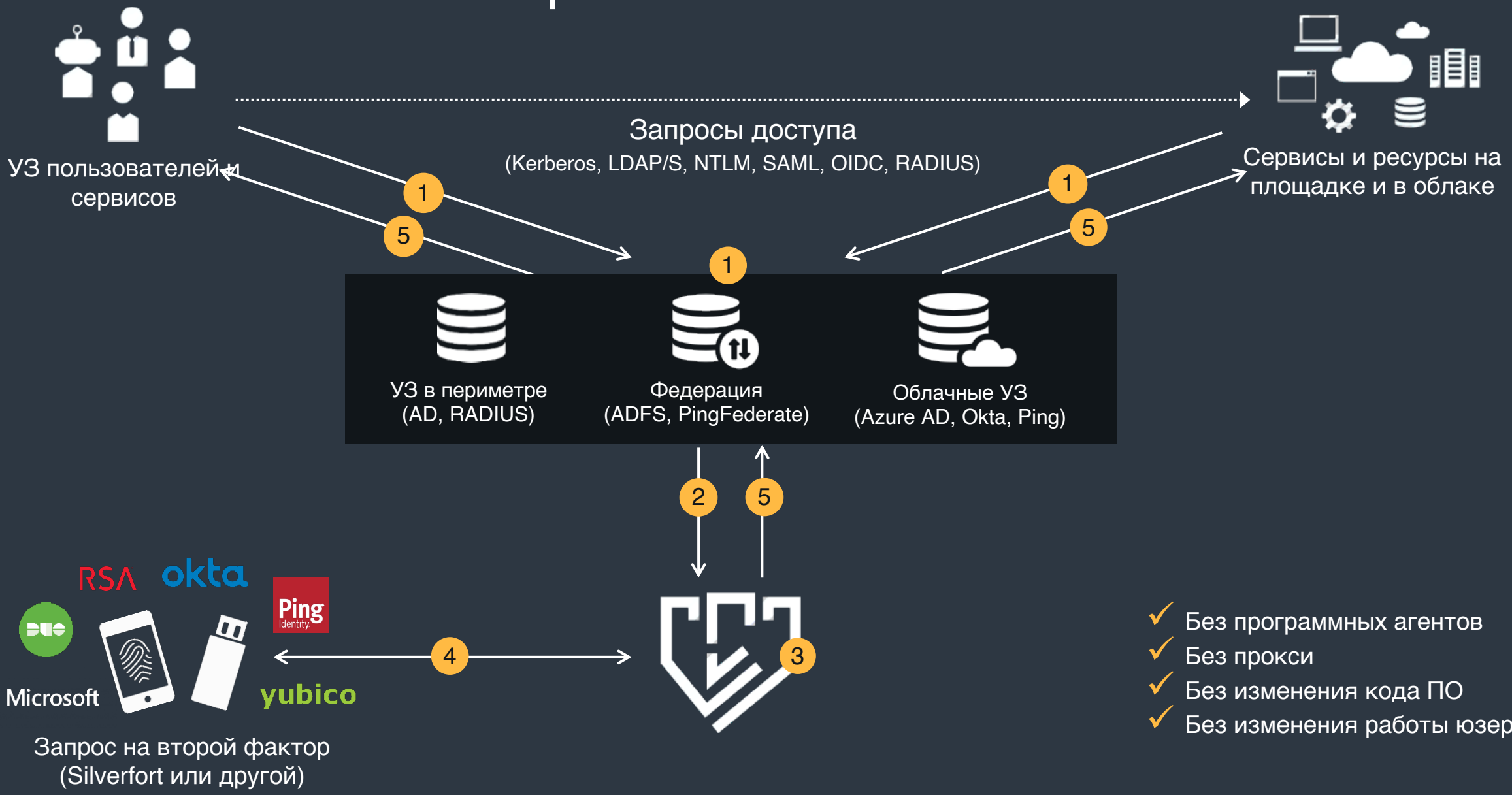
Декомиссия устаревших МФА

Избежание бесконечных проектов по интеграции отдельных систем

Архитектура



Как работает Silverfort?

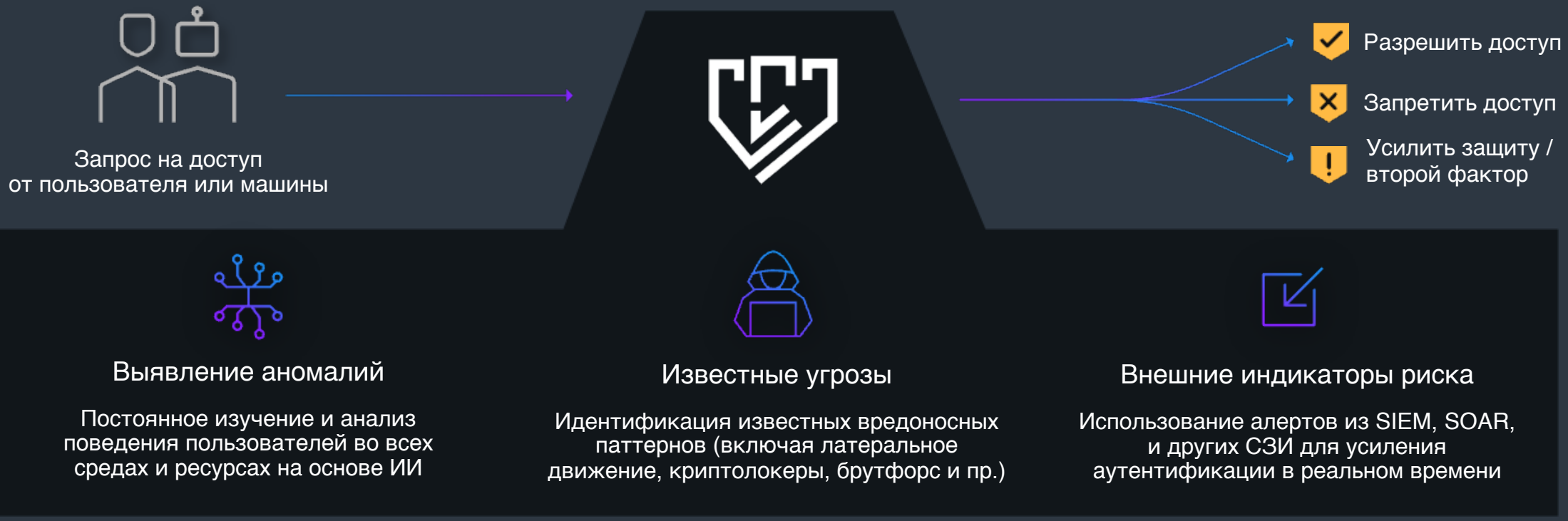


- ✓ Без программных агентов
- ✓ Без прокси
- ✓ Без изменения кода ПО
- ✓ Без изменения работы юзеров

SILVERFORT

Алгоритм Silverfort по выявлению рисков УЗ

Благодаря уникальной архитектуре без агентов и прокси Silverfort осуществляет мониторинг и анализ в 100-200 раз больше данных, чем другие решения для аутентификации на основе уровня риска



Индикаторы риска – примеры

- Аномальный пользователь
- Аномальный сервер
- Аномальный сервис
- Аномальный день
- Аномальный час
- Аномальный сайт AD
- Брутфорс
- Слабое шифрование
- Новое устройство
- Итерация по SMB
- Всплеск аутентификации
- Вредоносный IP-адрес
- Чрезмерная активность
- Невозможное путешествие
- Аутентификатор далеко от устройства
- Вход в сервисный аккаунт в интерактивном режиме
- Использование устаревшей учетной записи
- Использование устаревшего устройства
- Доступ к устаревшему ресурсу
- Общее устройство
- Привилегированный пользователь
- Зараженное устройство
- Админ с SPN (Kerberoasting)
- Общая учетная запись
- Заблокированная учетная запись
- Широко используемый аккаунт
- Старый пароль / никогда не истекает
- Атака с распылением паролей
- Отказ на МФА
- Старая ОС
- Сервисный аккаунт действует как человек
- Человек действует как машина
- Теневой администратор
- Пользователь сообщил, что "это был не я"
- Неограниченное делегирование
- Анонимизированный IP-адрес
- Подозрительный IP-адрес
- IP-адрес, зараженный ВПО
- Незнакомый вход
- Утекщие учетные данные
- Pass the Ticket
- Неправильная конфигурация управления УЗ пользователей
- Латеральное движение
- Атака программ-вымогателей

Традиционные МФА и Silverfort

Характеристика	Традиционные МФА	Silverfort
Архитектура	Требует установки агента, прокси или интеграции с **каждой отдельной** защищаемой машиной. **Если агент удален – защиты нет**	Легкое внедрение без агентов и прокси. Постоянная непрерывная защита, которую нельзя обойти
Защита протоколов интерактивного входа (RDP и аналоги)	**Да, если существует агент или интеграция**	**Да**
Защита всех других протоколов (более 100 для Windows, в том числе протоколы командной строки psexec / smb, wmi, powershell, которые обычно и используют злоумышленники)	**Нет**	**Да**
Защита систем и устройств, на которые нельзя установить агент (IoT / OT, гипервизоры, legacy, file shares, самописное ПО и пр.)	**Нет**	**Да**
Защита сервисных УЗ	**Нет**	**Да**
Мониторинг и анализ всех попыток аутентификации и доступа ко всем ресурсам во всех средах организации	**Нет**	**Да**
Адаптивная политика МФА на основе AI, уровня риска , без закидывания пользователей постоянными запросами на второй фактор	**Нет**	**Да**
Выявление и блокирование атак на УЗ (аномалии, брутфорс по множеству ПК, криптолокеры, нацеленные хакеры и пр.)	**Нет**	**Да**
Единая система аутентификации для всех кейсов (VPN, Windows, Linux, облака, веб и пр.)	**Нет**	**Да**
Простота лицензирования, отсутствие множества модулей для разных протоколов	**Нет**	**Да**

Какова ваша цель?

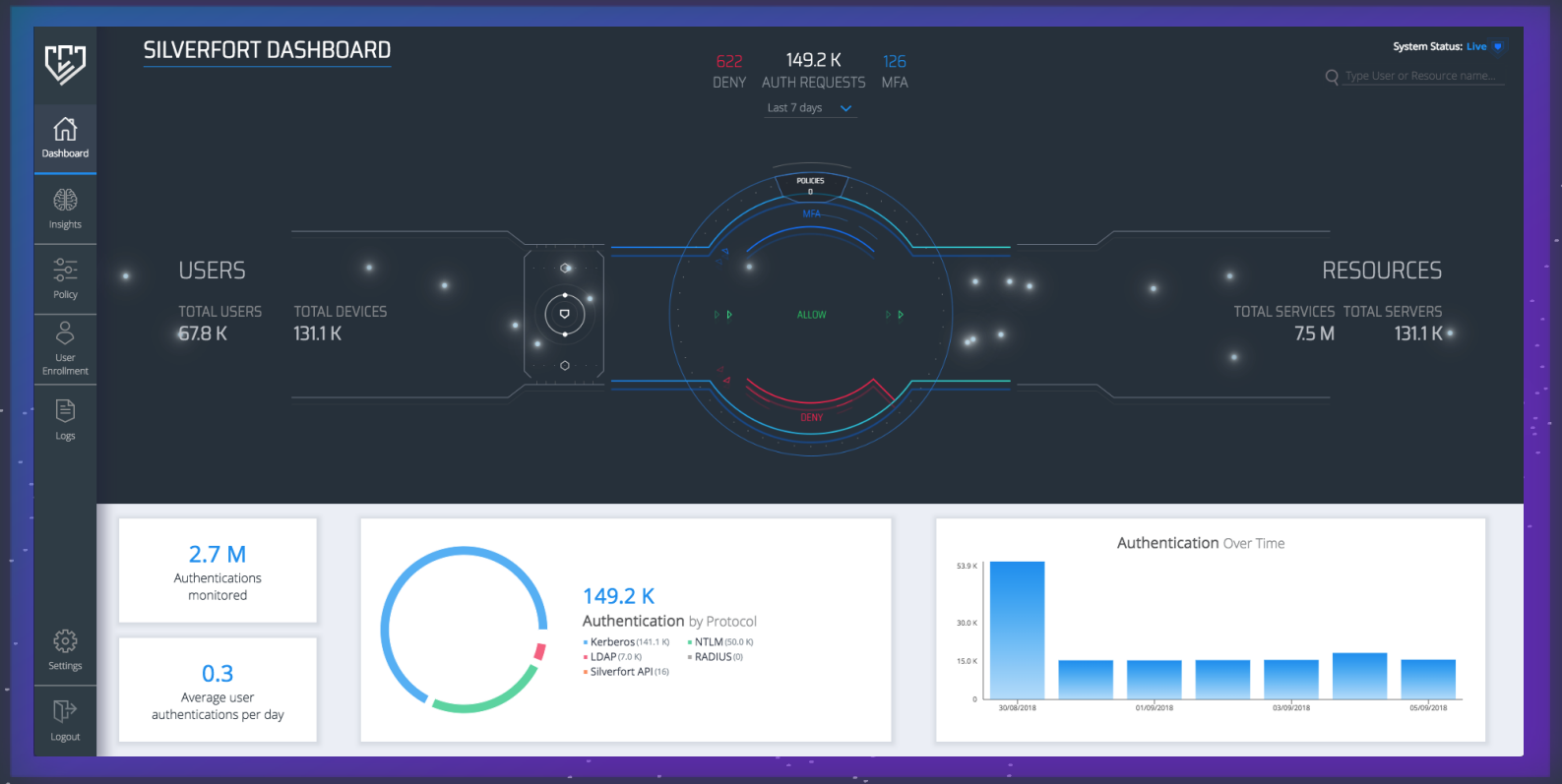
Иллюзия защиты

Реальная защита сотрудников и ресурсов от взлома

Классические решения МФА

Silverfort

Демонстрация



SILVERFORT

SILVERFORT

Спасибо!

Вопросы и отзывы: sales@tiger-optics.ru