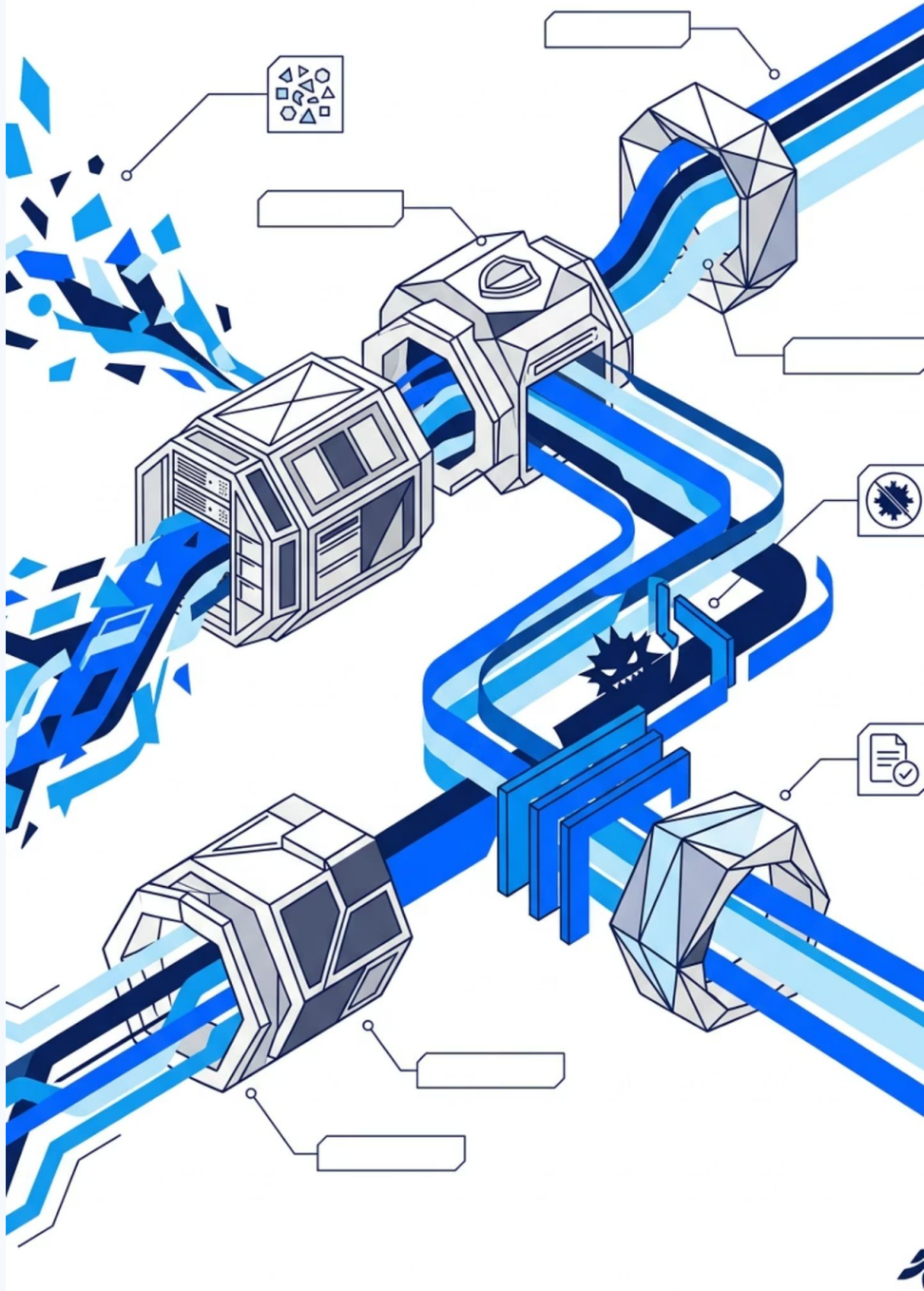
NXLog, BlueCat, Stellar Cyber, Seclore

Архитектура видимости: четыре вендора — одна стратегия

Профессиональный обзор решений для сбора телеметрии, управления сетью, обнаружения угроз и защиты данных. Каждый продукт — отдельный слой зрелой кибербезопасности.

CYBERSECURITY BRIEFING

ENTERPRISE ИБ



SOFTPROM

Softprom — Value Added IT Distributor

ВЕНДОР 1

NXLog — Швейцарский нож для телеметрии

Проблема

SIEM-системы захлёбываются от «мусорных» логов. Splunk, Elastic, QRadar берут огромные деньги за объём входящих данных (EPS или ГБ). До 50% событий — это информационный шум: дубликаты, пустые строки, рутинные операции.

Решение

Единый конвейер (pipeline) для сбора, фильтрации и маршрутизации данных перед отправкой в SIEM.

Результат

100% видимость IT-среды без перегрузки аналитиков. NXLog работает как умный фильтр и универсальный маршрутизатор: собирает данные со всех источников и отправляет в SIEM только то, что действительно важно.

Принцип: «Garbage in, garbage out» — мусор на входе означает мусор на выходе. NXLog устраняет проблему у самого источника.

NXLOG — ПРЕИМУЩЕСТВА

Ключевые преимущества NXLog

Агностичность

Работает с любыми источниками данных (Windows, Linux, базы данных, облака) и любыми SIEM-платформами без привязки к вендору.

Сверхлёгкий агент

Написан на C/C++, потребляет минимум RAM и CPU. Подходит даже для IoT-устройств и устаревших серверов — в отличие от Logstash на Java.

Мощный парсинг

Конвертация форматов (JSON, XML, CSV, Syslog) на лету, маскирование чувствительных полей, сжатие и шифрование логов перед отправкой.

Справедливая лицензия

Оплата за источник данных (ноду), а не за объём. Даже если трафик вырастет в 10 раз из-за атаки — счёт не изменится ни на цент.

NXLOG — КЕЙСЫ

Кейсы использования NXLog

1

Снижение затрат на SIEM

Отсекая ненужные события на уровне агента, компании экономят **до 25–50%** на лицензиях тяжёлых SIEM-систем. Фильтрация происходит до попадания данных в платформу.

2

Комплаенс: GDPR, PCI-DSS

NXLog шифрует данные «в полёте» и параллельно отправляет их в SIEM (быстрый анализ) и в холодное хранилище AWS S3 (долгосрочный аудит) в неизменном виде.

3

Мониторинг SCADA/ICS

У многих конкурентов нет агентов для специфических ОС или старых Windows на заводах. NXLog поддерживает промышленные объекты там, где другие пасуют.

4

Миграция SIEM

Пересылка логов одновременно в старую и новую систему позволяет проводить бесшовную миграцию без потери данных и без остановки мониторинга.

NXLOG — ДОВЕРИЕ

Кто доверяет NXLog?

15+

Лет на рынке

Глобальный стандарт лог-менеджмента

600+

Enterprise-клиентов

В 62 странах мира, включая Fortune 500

Отрасли применения

Финансовый сектор

Топ-игроки, которым нужен предсказуемый бюджет без скачков лицензионных затрат

Правительственные учреждения

Строгие требования к хранению и неизменности логов для государственного аудита

Телеком и производство

Гетерогенные среды с тысячами разнородных источников событий

> «Мы никогда не знаем, какой источник данных придётся подключить завтра, но с NXLog у нас в руках швейцарский нож, который справится с чем угодно.»

ВЕНДОР 2

BlueCat — Интеллектуальное управление сетью

Проблема

Хаос в сетях из-за ручного управления DNS, DHCP и IP-адресами. Экселевские таблицы, разрозненные утилиты, конфликты IP-адресов, «слепые зоны» — всё это в гибридной среде из онпрем, AWS и Azure становится критической точкой отказа.

Решение BlueCat

Unified DDI (DNS + DHCP + IPAM) — единый источник правды для всей сетевой инфраструктуры. Платформы **Micetro и Integrity** обеспечивают полную видимость каждого IP-адреса и каждого DNS-запроса в любой точке гибридной сети.

Результат

Сеть работает без сбоев, быстрее масштабируется и значительно лучше защищена от киберугроз уже на сетевом уровне.

BLUECAT — ПРЕИМУЩЕСТВА

Ключевые преимущества BlueCat

Единый источник правды (SSOT)

Полная видимость от локального ЦОД до любого облачного провайдера. Управление всеми DNS-зонами из одного окна, без разрозненных инструментов.

API-First подход

Интеграция с Terraform, Ansible и CI/CD-пайплайнами. Новый сервер в облаке получает IP и DNS-имя за секунды — вместо 3 дней ожидания тикета в поддержку.

Protective DNS

90% малвари использует DNS для C2-коммуникации. BlueCat интегрируется с Threat Intelligence (CrowdStrike) и блокирует вредоносные домены до загрузки на ПК сотрудника.

Agentic AI (LiveAssist)

ИИ-ассистент для глубокой аналитики и траблшутинга сети. Обрабатывает миллионы DNS-запросов в секунду без деградации производительности.

BLUECAT — КЕЙСЫ

Кейсы использования BlueCat

Управление Multi-Cloud

Единое управление DNS в AWS, Azure и GCP из одного интерфейса. Когда инфраструктура распределена между несколькими облаками и своим ЦОД — BlueCat связывает DNS-зоны без боли для сисадмина.

Zero Trust и безопасность

Когда антивирус «молчит», а устройство упорно достукивается до домена в даркнете — BlueCat не только блокирует запрос, но и показывает точный IP-адрес заражённого хоста для расследования.

Автоматизация NetOps

Ускорение развёртывания IT-инфраструктуры в **10 раз**. Автоматическое выделение IP и DNS-имён устраняет ручные операции и человеческий фактор в сетевых изменениях.

Слияния и поглощения (M&A)

Когда компания А покупает компанию Б с пересекающимися подсетями (например, обе используют 192.168.x.x) — BlueCat элегантно разрешает конфликты без остановки бизнеса.

BLUECAT — ДОВЕРИЕ

Кто доверяет BlueCat?

Для кого BlueCat?

Если падение сети на 15 минут стоит компании миллионы долларов штрафов и недополученной прибыли — это клиент BlueCat. Решение класса Enterprise для организаций, где доступность сети — критический бизнес-актив.

Отрасли и признание

- Крупнейшие мировые банки и финансовые институты
- Глобальные розничные сети и e-commerce платформы
- Системы здравоохранения и транспортные хабы

Признан лидером в отчётах **Enterprise Management Associates (EMA)**

BlueCat — это фундамент, без которого не взлетит ни один новый сервис и не откроется ни один новый филиал.

ВЕНДОР 3

Stellar Cyber — Мозг вашего SOC

Проблема: Alert Fatigue

Среднестатистический Enterprise использует от **20 до 50 разрозненных инструментов ИБ** (фаерволы, антивирусы, сканеры), которые не общаются между собой. Результат — тысячи разрозненных алертов в день, выгорание аналитиков и пропущенные реальные атаки.

Решение: Open XDR на базе ИИ

Stellar Cyber забирает телеметрию со всех систем, прогоняет её через многослойный ИИ и вместо **1000 непонятных красных строк** выдаёт 3 готовых инцидента с полным контекстом: кто атаковал, откуда пришёл, что заразил и как это остановить.

SOFTPROM

Softprom — Value Added IT Distributor

STELLAR CYBER — ПРЕИМУЩЕСТВА

Ключевые преимущества Stellar Cyber

Multi-Layer AI™

Графовый ИИ, Machine Learning и LLM для анализа, корреляции и триажа. Система описывает ход атаки человеческим языком и автоматически приоритизирует инциденты.

Bring Your Own EDR

Более **400 готовых интеграций**. Используете CrowdStrike, SentinelOne или Microsoft Defender? Stellar Cyber усиливает их данными и не заставляет отказываться от существующих инвестиций.

Всё в одном

NG-SIEM, NDR, UEBA, SOAR и Threat Intelligence Platform — всё «под капотом» единой платформы. Ни один модуль не требует отдельной лицензии.

Единая лицензия

Никаких скрытых платежей за новые модули. Предсказуемые расходы: покупая платформу, вы получаете полный стек ИБ-инструментов по одной понятной ставке.

STELLAR CYBER — КЕЙСЫ

Кейсы использования Stellar Cyber

1

Замена SIEM

Переход от «хранилища логов» к платформе активного реагирования. Stellar Cyber добавляет мощную аналитику и SOAR поверх или вместо устаревшего SIEM.

2

MSSP / SOC-as-a-Service

Многоарендная архитектура позволяет MSSP вести 50+ клиентов в одной консоли. ИИ делает 80% рутинной работы — **8-кратное ускорение** расследований.

3

Защита OT/ICS

Единая видимость классической IT-инфраструктуры и промышленной сети. Выявление аномалий в SCADA-среде без специализированных агентов.

4

Выявление инсайдеров

UEBA-модуль замечает: бухгалтер начал скачивать гигабайты баз данных в 3 часа ночи. Поведенческая аналитика выявляет скомпрометированные учётные записи.

STELLAR CYBER — ДОВЕРИЕ

Кто доверяет Stellar Cyber?

14K+

Клиентов

По всему миру, от небольших команд ИБ до глобальных аутсорсеров

1/3

Топ-250 MSSP

Почти треть ведущих мировых MSSP строят SOC на Stellar Cyber

Признание аналитиков

Stellar Cyber отмечен в Gartner Magic Quadrant как один из ведущих игроков в категории Network Detection and Response (NDR). Профессионалы, зарабатывающие на кибербезопасности, выбирают платформу за скорость расследований (MTTD/MTTR) и масштабируемость без найма сотен новых аналитиков.

- Идеально для компактных команд ИБ в крупном Enterprise и для аутсорсеров безопасности любого масштаба.

ВЕНДОР 4

Seclore — Интеллектуальная защита данных

Проблема: Данные покидают периметр

Традиционные DLP-системы контролируют только границы. Как только файл отправлен подрядчику, скопирован на флешку или попал в облако — **вы теряете над ним контроль**. Периметр больше не существует.

Решение: Data-Centric Security

Seclore «оборачивает» файл в криптографическую броню. Политика доступа живёт **внутри самого документа**. Где бы файл ни находился — он запрашивает сервер Seclore: «Можно ли этому человеку меня открыть?» Защита работает даже на чужой флешке, в чужом облаке и на личном устройстве сотрудника.

SECLORE — ПРЕИМУЩЕСТВА

Ключевые преимущества Seclore

Гранулярный контроль (DRM)

Запрет на печать, копирование текста (Ctrl+C), создание снимков экрана (PrintScreen). Настройка прав вплоть до конкретного действия для конкретного получателя.

Отзыв доступа в 1 клик

Подрядчик закончил проект? Одним кликом все отправленные ему чертежи и документы превращаются в нечитаемый «кирпич» — даже если они хранятся у него локально.

Аудит 360°

В реальном времени: кто, когда, откуда и с какого устройства открывал файл. Отчёт покажет попытки несанкционированной печати, открытие из нетипичной страны и другие аномалии.

Платформа ARMOR

AI Discovery автоматически находит конфиденциальные файлы и применяет политики. Бесшовная интеграция с Microsoft 365, SharePoint и ведущими DLP-решениями.

SECLORE — КЕЙСЫ

Кейсы использования Seclore

Защита интеллектуальной собственности

Производственные и фармацевтические компании отправляют CAD-чертежи и химические формулы смежникам. Seclore «привязывает» их к конкретным получателям — данные не утекут к конкурентам.

Защита от инсайдеров и BYOD

Уволенный сотрудник скачал клиентскую базу перед уходом? Без активных прав доступа в Seclore он никогда не откроет её дома, на личном устройстве или на новой работе.

Защита от ИИ-рисков

Сотрудники «скармливают» конфиденциальные отчёты в ChatGPT для создания саммари (Data Exposure Risk). Seclore физически блокирует чтение зашифрованного файла публичными нейросетями.

SECLORE — ДОВЕРИЕ

Кто доверяет Seclore?

2000+

Компаний

В 29 странах мира

Seclore — последняя, непробиваемая линия обороны для организаций, где стоимость утечки данных измеряется репутацией и многомиллионными штрафами.

Известные клиенты

HDFC Bank

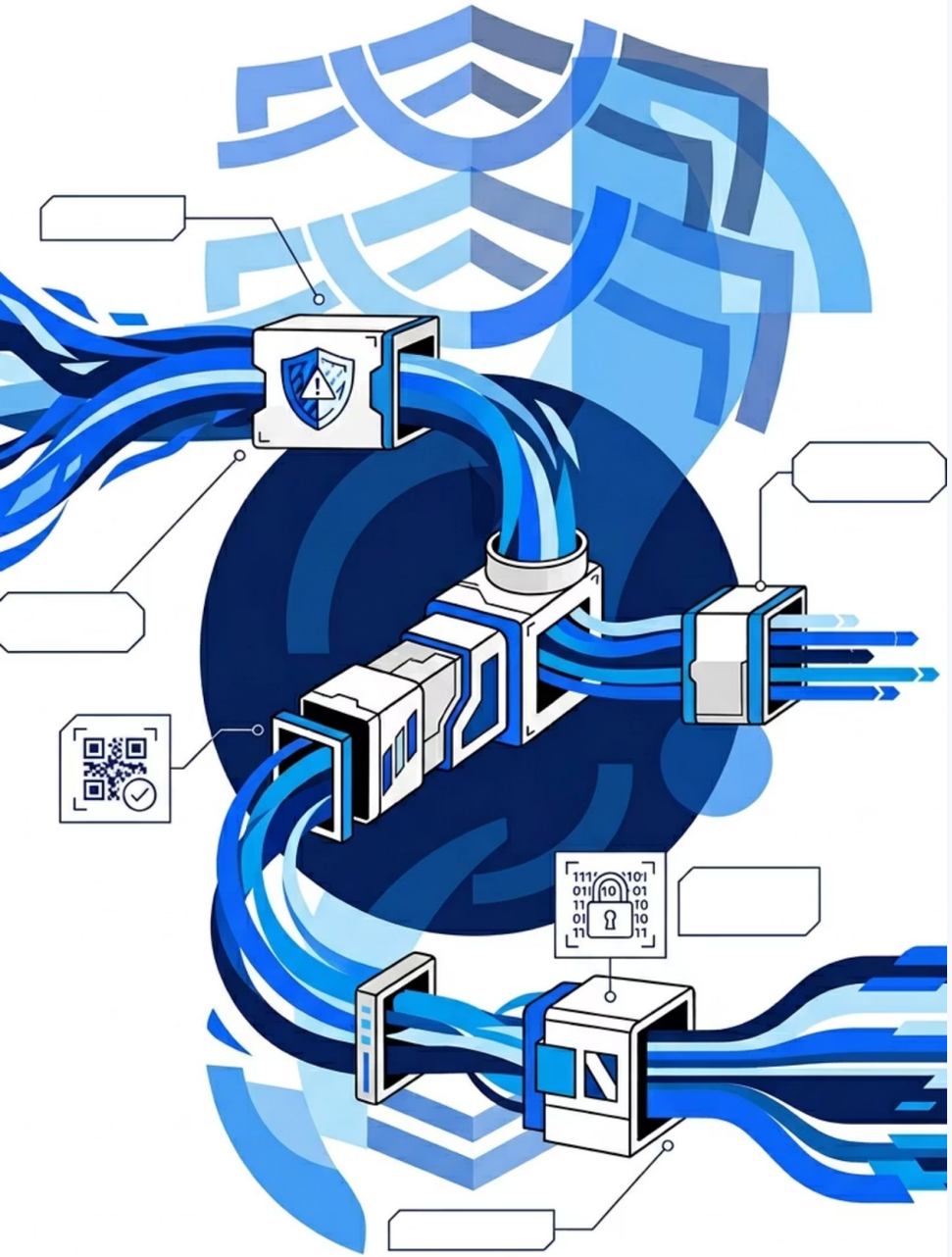
Безопасный обмен финансовой информацией с внешними партнёрами

American Auto Co. / Shilpa Medicare

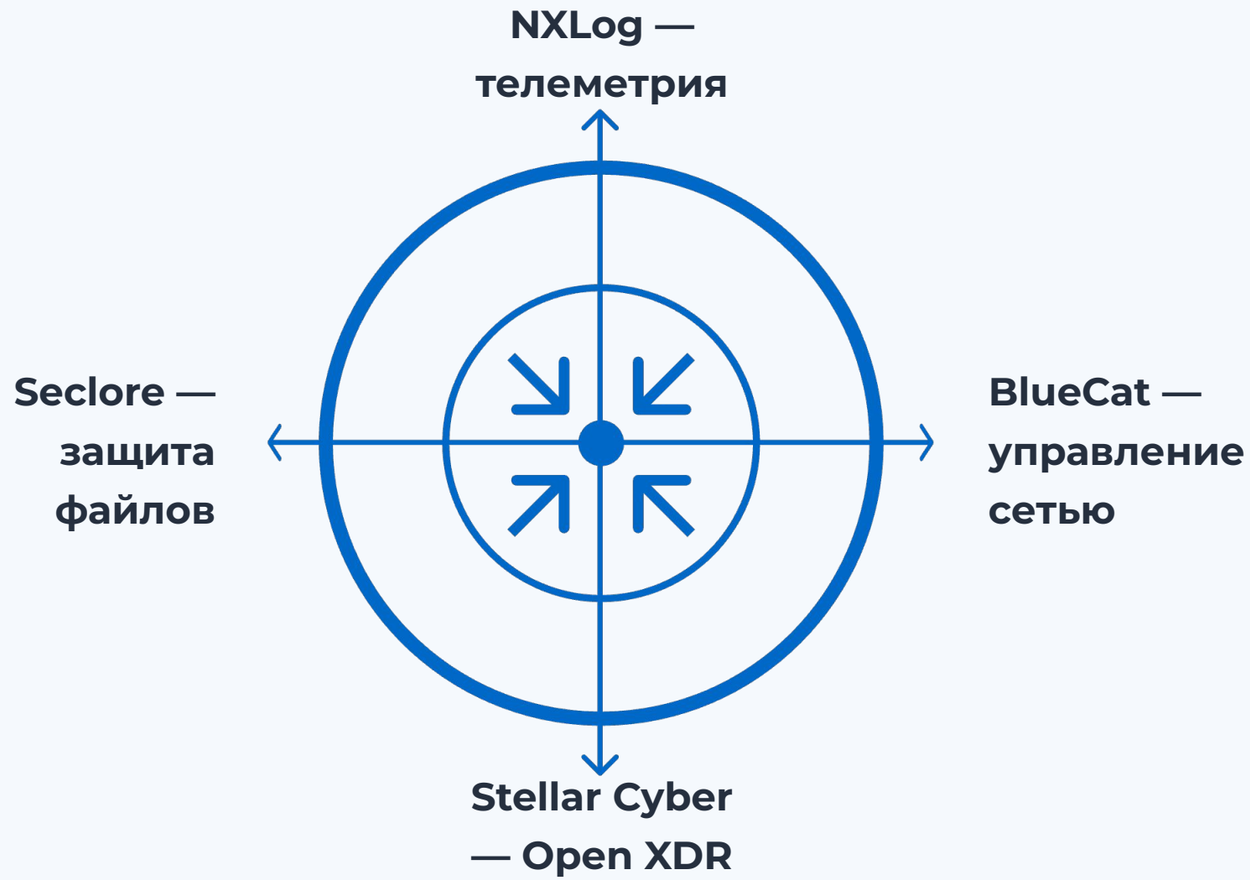
Защита производственных секретов и фармацевтических патентов

Экосистема интеграций

Microsoft 365, SharePoint, Forcepoint, Symantec — DLP находит файл, Seclore автоматически его шифрует



Четыре вендора — одна архитектура защиты



Каждый продукт закрывает уникальный пласт задач: от сбора «правильных» данных на входе — до защиты документов на выходе за пределы периметра. Вместе они образуют зрелую, глубокоэшелонированную архитектуру кибербезопасности. Следующий шаг — **Proof of Concept (PoC)** по любому из представленных решений.

Готовы к пилоту? Мы готовы организовать PoC по каждому из четырёх продуктов в вашей инфраструктуре — обращайтесь к нашим специалистам.