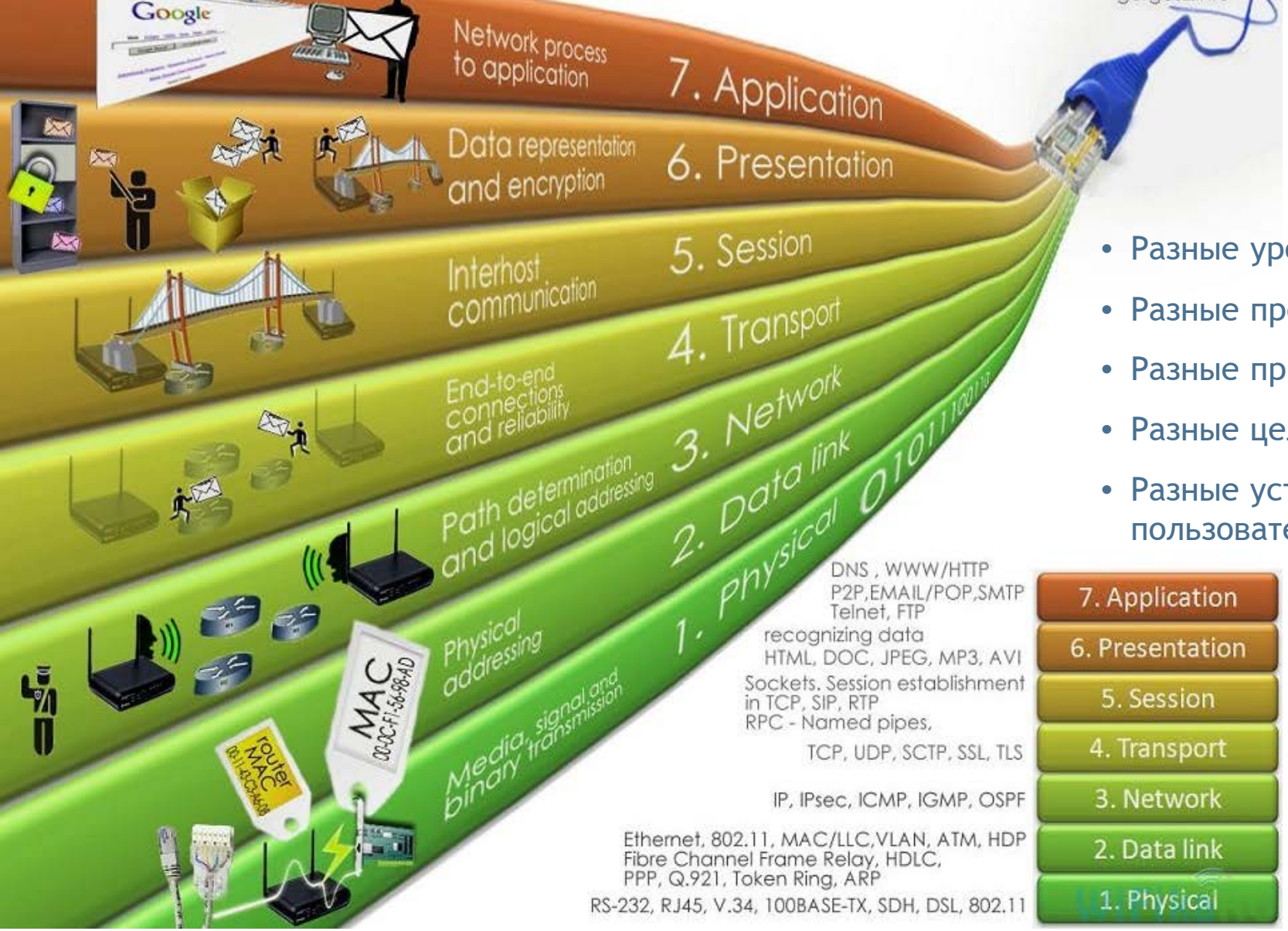
Безопасный WEB

webcontrol



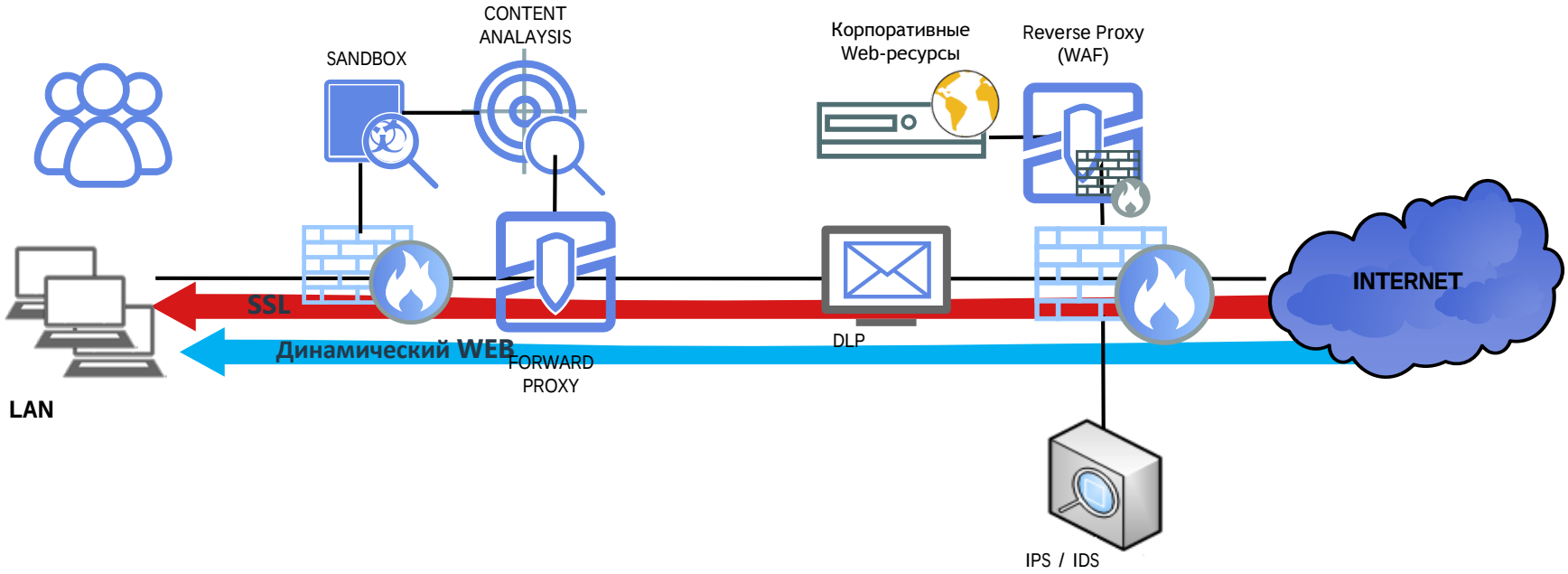
- Разные уровни
- Разные протоколы
- Разные приложения
- Разные цели атаки
- Разные устройства и пользователи

webcontrol

Сетевая модель

Web Security: важная роль веб-прокси

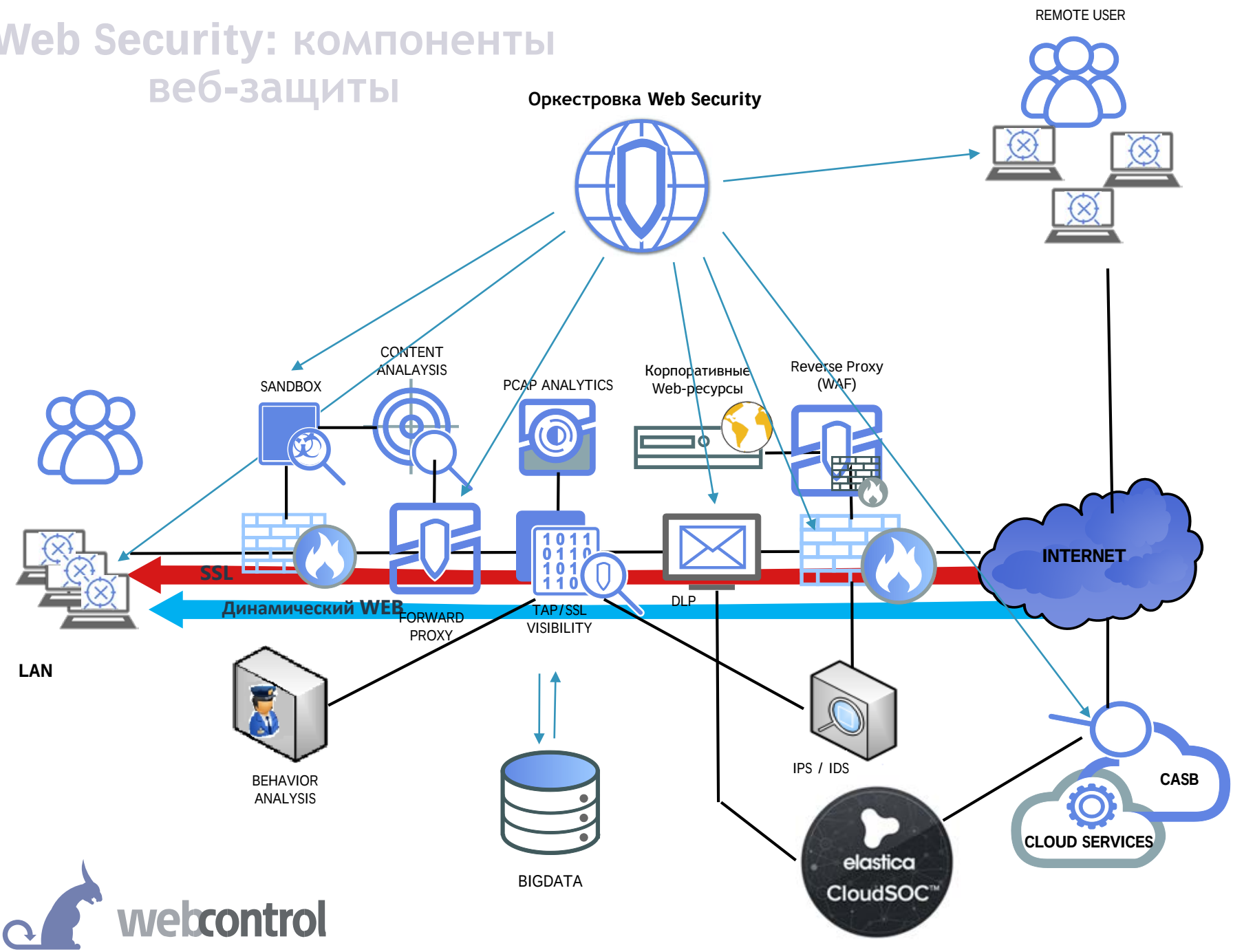
Через web-канал злоумышленники распространяют огромное количество вредоносного ПО.



На прокси может проверяться 100% трафика между пользователями и HTTP/HTTPS сайтами. Это дает возможность эффективно обнаруживать и блокировать вредоносный код.

webcontrol

Web Security: компоненты веб-защиты



webcontrol

Advanced Secure Gateway

Извлечение и управление файлами

Дешифрация SSL, извлечение документов
Передача файлов на проверку по ICAP
Запрет доставки на основе вердикта
Потоковые дешифрованные данные для расследования инцидентов

Проверка файлов для предотвращения вредоносных программ и продвинутых угроз

Белый / Черный список
Двойные AV сигнатуры
Анализ статического кода
Фильтрация перед песочницей

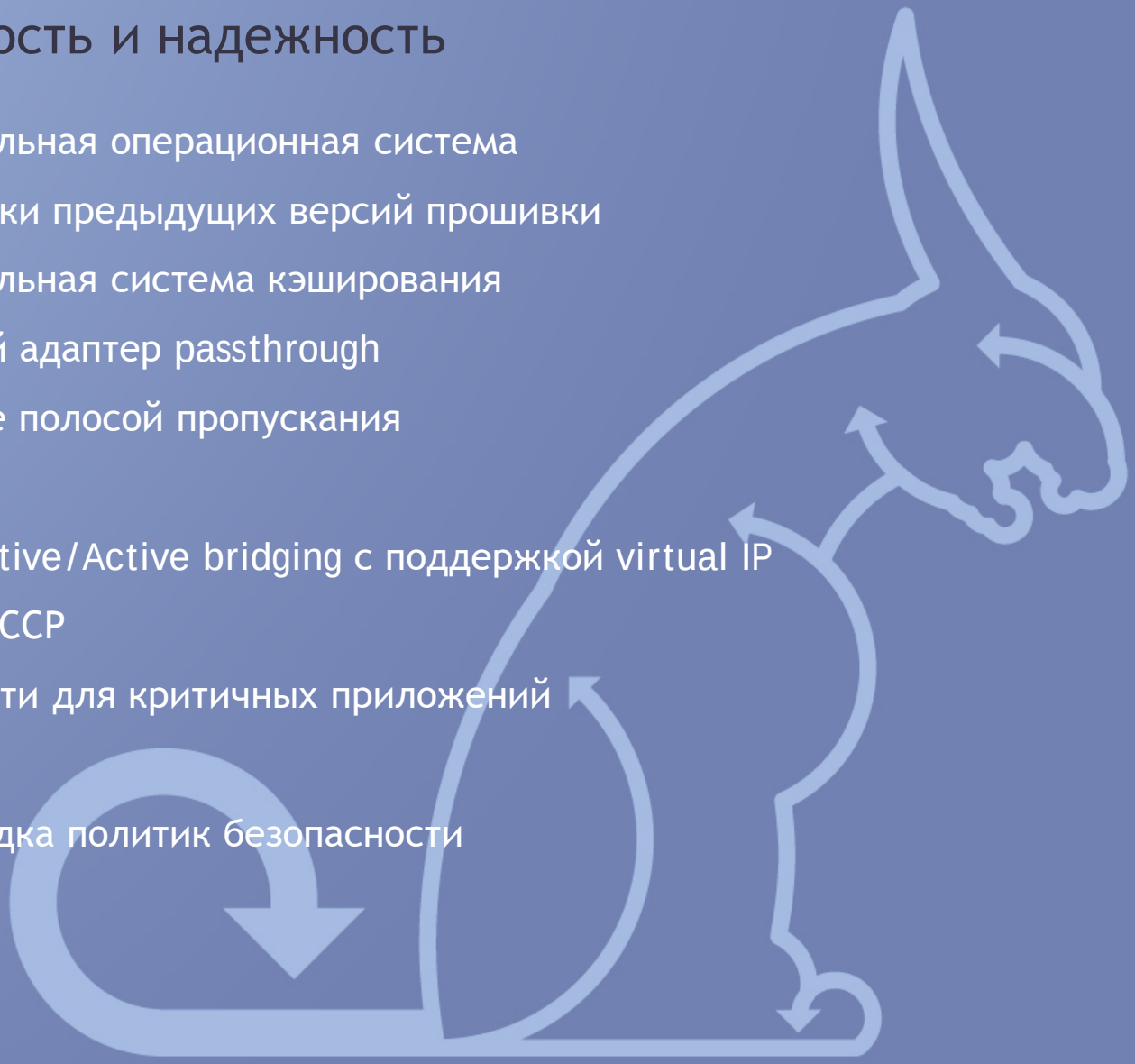
Единое управление доступом

Аутентификация, применение политик, журналирование
Обнаружение и контроль теневого (shadow) IT

Secure Web Gateway

Производительность и надежность

- Высокопроизводительная операционная система
- Возможность загрузки предыдущих версий прошивки
- Высокопроизводительная система кэширования
- Встроенный сетевой адаптер passthrough
- Сжатие, управление полосой пропускания
- SSL off loading
- Работа в режиме Active/Active bridging с поддержкой virtual IP
- Поддержка DNS и WCCP
- Контроль доступности для критичных приложений
- On-prem или Cloud
- Трассировка и отладка политик безопасности



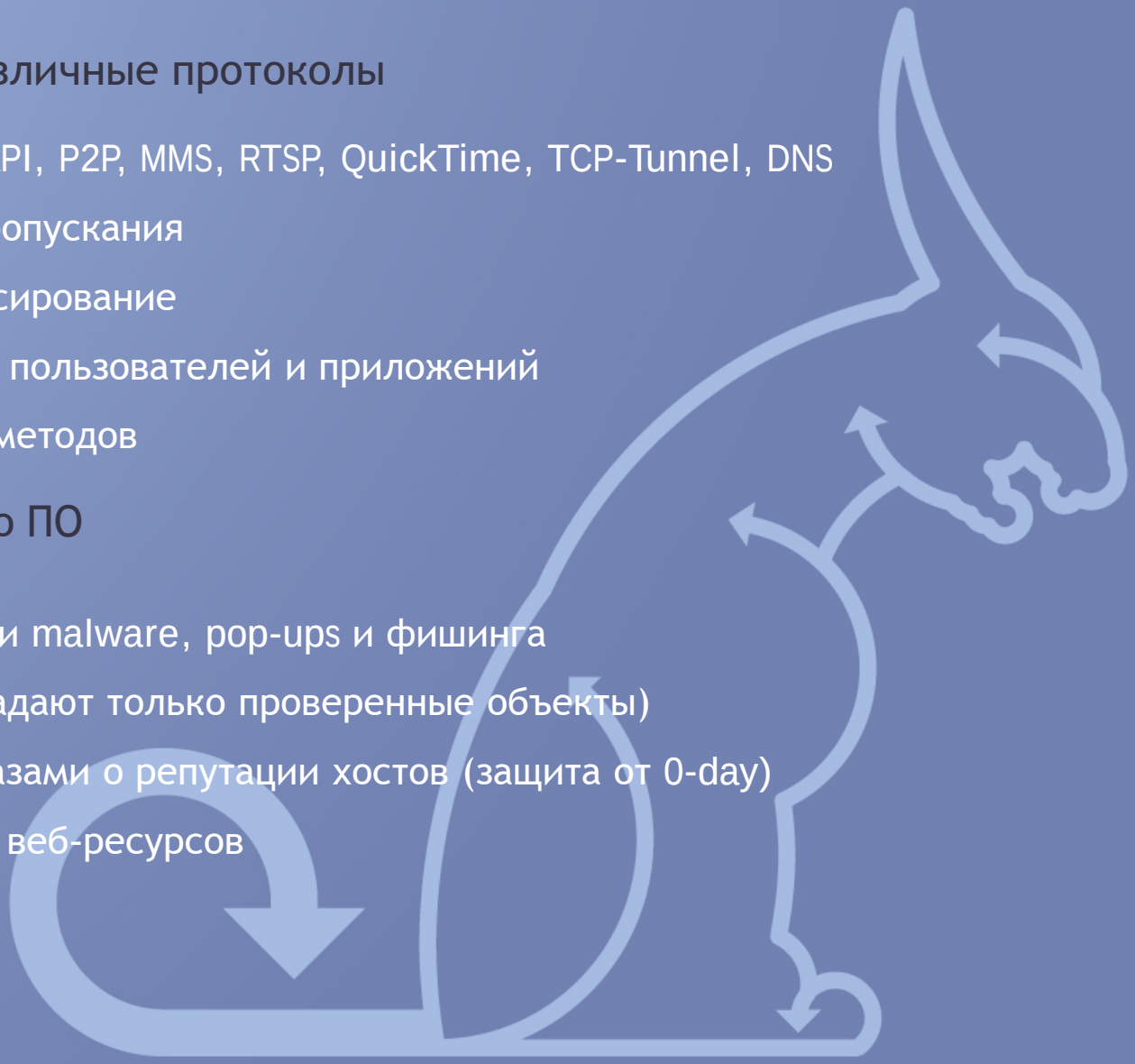
Secure Web Gateway – гибкость и защита

Proxy поддерживает различные протоколы

- HTTP, CIFS, SSL, FTP, MAPI, P2P, MMS, RTSP, QuickTime, TCP-Tunnel, DNS
- Управление полосой пропускания
- SSL-терминация и проксирование
- Контроль трафика всех пользователей и приложений
- Управление на уровне методов

Защита от вредоносного ПО

- Блокирование Spyware и malware, pop-ups и фишинга
- Чистый кэш (в кэш попадают только проверенные объекты)
- Глобальное облако с базами о репутации хостов (защита от 0-day)
- Лучшая база категорий веб-ресурсов



Secure Web Gateway – гибкость и защита

Гибкие политики

- Создание собственных описаний политик для реализации оригинальных правил доступа
- Встроенный редактор для создания нестандартных правил непосредственно через интерфейс управления
- Возможность загрузки политик с внешнего источника

Аутентификация

- SSO, NTLM, LDAP (Active Directory, eDirectory, SunOne), CA eTrust SiteMinder, Microsoft Kerberos, Oracle Access manager, RADIUS и загружаемые сертификаты
- Мультизонные последовательности аутентификации

Управление потоковым трафиком

- MS, Real, QuickTime
- Управление полосой и настраиваемое кэширование

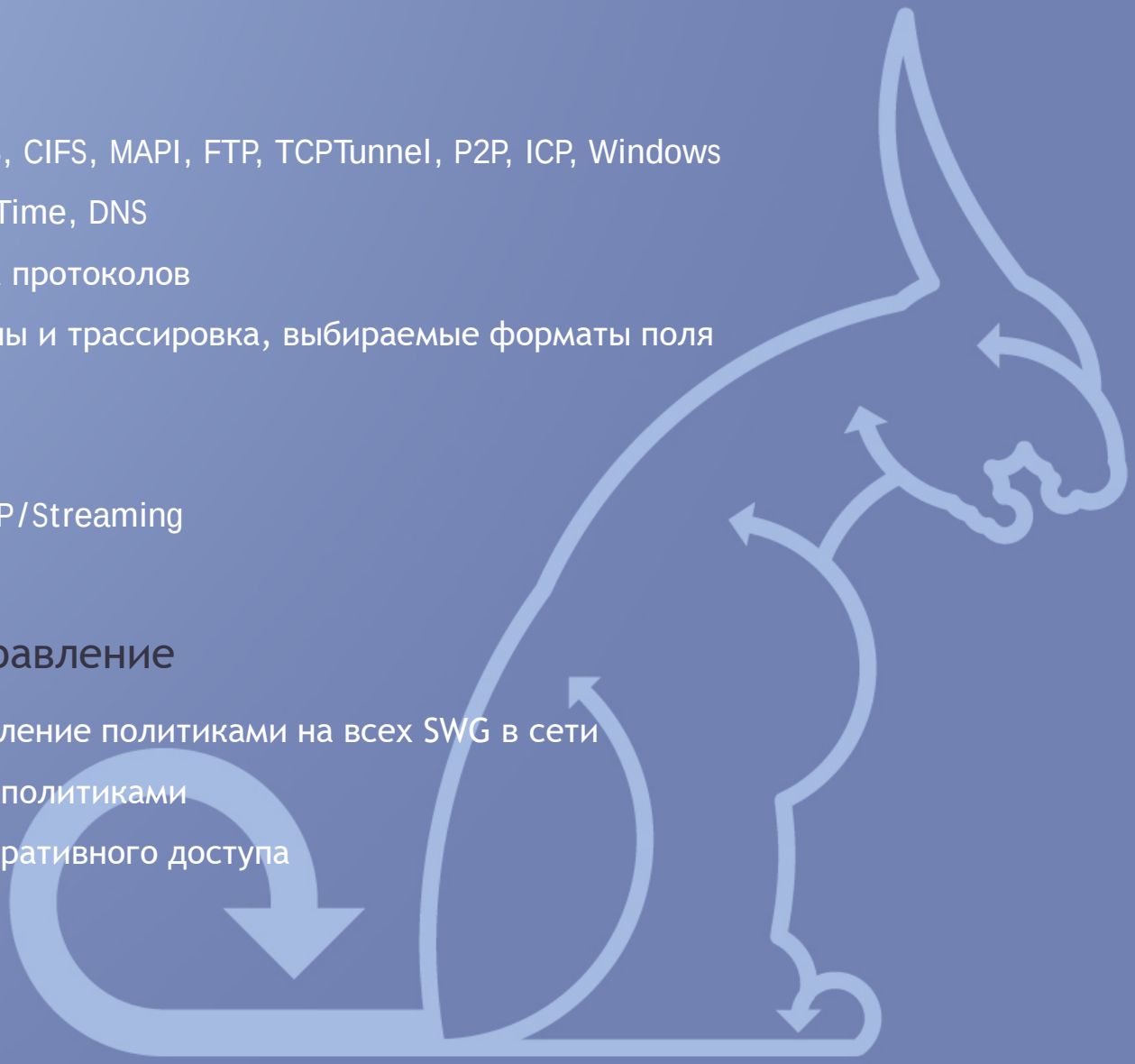
Secure Web Gateway – отчеты и управление

Отчетность

- Стандартно: HTTP, HTTPS, CIFS, MAPI, FTP, TCPTunnel, P2P, ICP, Windows media, Real Media, QuickTime, DNS
- Автоматическая загрузка протоколов
- Настраиваемые протоколы и трассировка, выбираемые форматы поля / текст/ файла
- Статистика трафика
- История HTTP/HTTPS/FTP/Streaming
- Ресурсы

Централизованное управление

- Централизованное управление политиками на всех SWG в сети
- Управление групповыми политиками
- Разграничение административного доступа

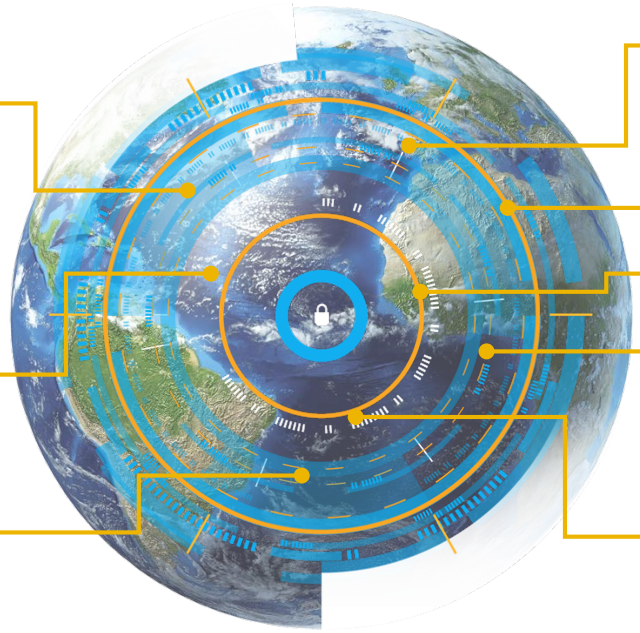


URL-категоризация vs Расширенный анализ

Источник данных	URL база	On-site анализ	Динамический анализ репутации в облаке
Статические списки категорий	✓	✓	✓
Динамические списки категорий			✓
Категоризация веб-контента			✓
Оценка риска по URL-категории		✓	✓
Многофакторная оценка риска			✓
Геолокация		✓	✓
Наглядность данных в веб-приложениях			✓

webcontrol

Big Data на службе Global Intelligence Network



175M
конечных точек

Обнаружено
430 миллионов
новых вредоносных программ за год

8,4 Миллиарда
email сканируется ежемесячно

9 центров обнаружения угроз

63M сенсоров атаки
в **157** странах

Защищено **12 000**
облачных приложений

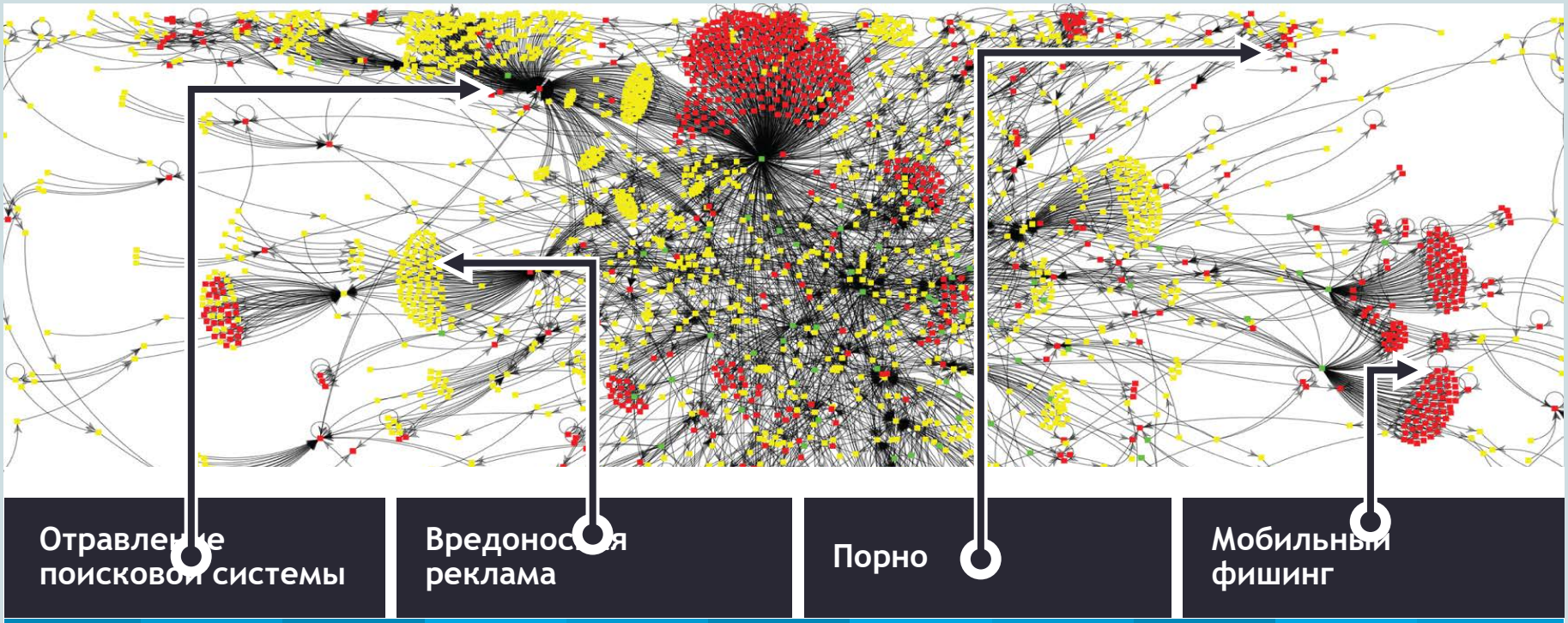
402M
WEB атак заблокировано за прошлый год

1 Миллиард
ЦУИ запросов сканируется ежедневно

Одна из самых больших гражданских сетей кибер-расследований
3,7 триллиона строк кода безопасности

webcontrol

Определение Malnet



Содержимое и шифрация SSL не имеют значения.

Тип устройства неважен. **Тип атаки не имеет значения.**

И речь не только о Zero-day эксплойтах.

webcontrol

GIN – источники обучения от Negative day

осведомленность

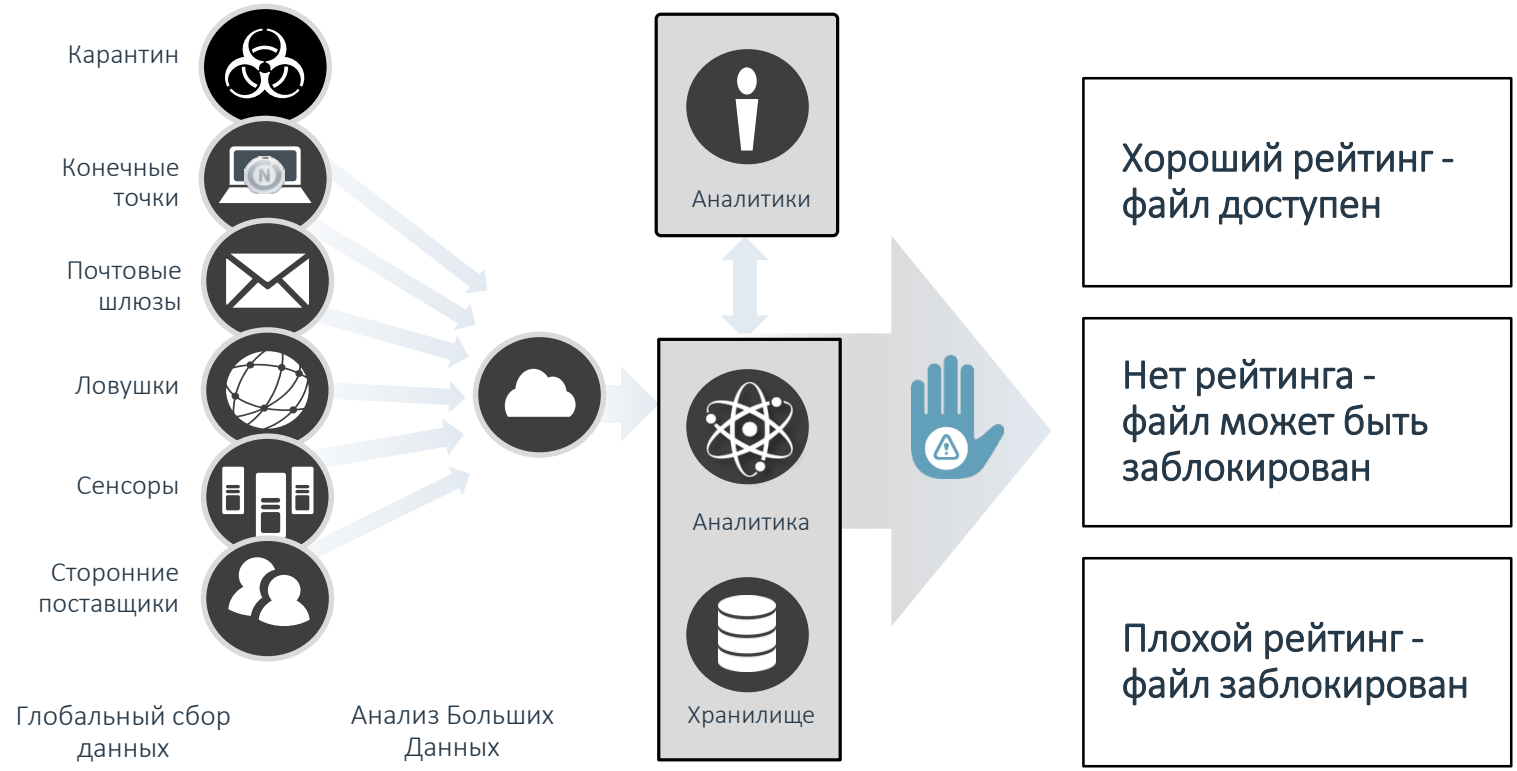
интеллект

проактивность

webcontrol

Анализ репутации

Обнаружение по возрасту, частоте и расположению



ГЛОБАЛЬНАЯ СЕТЬ АНАЛИЗА КИБЕРУГРОЗ

webcontrol

Люди

их поведение увеличивает риски потери данных

Эволюция привычек пользователей:

Увеличение объема активной информации за пределами корпоративного периметра

Облака и мобильные приложения

Публикация данных, которые не должны быть опубликованы

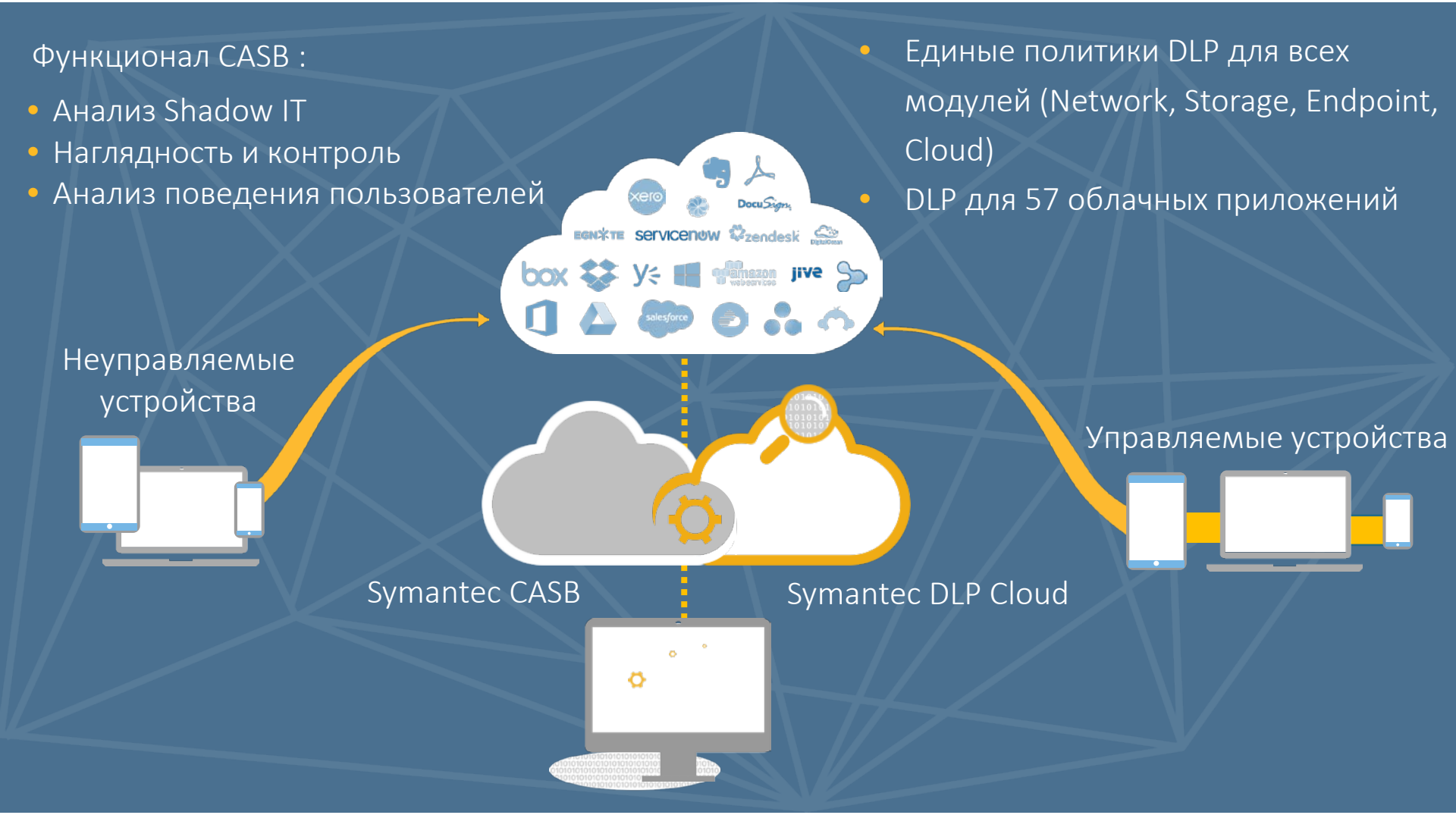
Хранение конфиденциальной информации в ненадежных местах

CASB & DLP

Функционал CASB :

- Анализ Shadow IT
- Наглядность и контроль
- Анализ поведения пользователей

- Единые политики DLP для всех модулей (Network, Storage, Endpoint, Cloud)
- DLP для 57 облачных приложений



webcontrol

Защита данных в облаке

Office 365, Gmail, Box …

Детектирование

Использование существующих политик DLP

Защита

Визуальные теги, карантин, уведомление по email, анализ использования данных в облаке, шифрование и/или обезличивание данных…

webcontrol

http://web-control.ru/