



UserGate SUMMA.

100% видимость трафика на базе собственных разработок



Наш офис разработки находится в Технопарке Новосибирского Академгородка – в месте, где тысячи талантливых разработчиков, инженеров, ученых занимаются производством высокотехнологичных продуктов.

Дополнительные офисы:
г. Москва, г. Санкт-Петербург,
г. Хабаровск.



О компании UserGate

2001

запуск первой версии UserGate Proxy

2009

начало разработки первого российского NGFW UserGate

2010

создан внутренний стартап, в рамках которого началась разработка новой платформы

2012

UserGate – резидент Академпарка в Новосибирске

2019

открытие первого московского офиса UserGate

2018

создание экспертной лаборатории и начало разработки собственных аппаратных платформ

2016

выпуск нового UserGate как решения класса UTM

2015

UserGate – резидент Сколково

2020

открытие офиса UserGate в Хабаровске

начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

2021

выход на рынок экосистемы безопасности UserGate SUMMA

2022

открытие офиса в Санкт-Петербурге



Как USERGATE изменился В 2023 ГОДУ

- значительное увеличение штата **технической поддержки**;
- два офиса разработки + открытие офиса в РБ.;
- полноценный отдел pre-sale, состоящий из высококвалифицированных инженеров;
- отдел сервиса и качества (emergency team);
- технические лаборатории на базе подразделений UserGate;
- авторизованные учебные центры и новые учебные курсы+ академия UserGate ;
- тщательная проработка всех feature request
- выход версии релиз кандидат 7.1 (с SIEM, UG Client)

Ландшафт угроз 2024

A decorative graphic on the right side of the slide, consisting of a complex network of light blue lines and dots, resembling a molecular structure or a data network, set against a dark blue background.



Ландшафт угроз

- таргетированные атаки от проправительственных группировок;
- видим применение бот-сетей для организации DDOS-атак, как правило приуроченных к какому-то событию;
- высокую активность сохраняют «шифровальщики» (ransomware);
- скорость реакции на выходящие PoC очень высокая;
- наиболее популярными остаются веб-приложения и чаще эксплуатируют уязвимости имеющие PoC.

Требования регуляторов





Требования регуляторов

- 187-ФЗ от 26.07.2017
- 152-ФЗ от 27.07.2006
- Приказ ФСТЭК №21 от 18.02.2013
- Приказ ФСТЭК №17 от 11.02.2013
- 436-ФЗ от 29.12.2010
- Приказ Минздрава России №911н от 24.12.2018
- 114-ФЗ от 25.07.2002



Сертификат ФСТЭК России № 3905

Решение UserGate имеет действующий сертификат ФСТЭК России по 4 уровню доверия до 26.03.2026 г.

- **Требования к МЭ**

- Профиль защиты МЭ типа А 4-го класса защиты
- Профиль защиты МЭ типа Б 4-го класса защиты
- Профиль защиты МЭ типа Д 4-го класса защиты

- **Требования к СОВ**

- Профиль защиты СОВ уровня сети 4-го класса защиты

- Уровень доверия 4:**
- классы защиты СЗИ 4;
 - ЗО КИИ 1 категории;
 - ГИС 1 класса;
 - АСУ ТП 1 класса;
 - ИСПДн 1 уровня;
 - ИСОП II класса.

Ожидания рынка





Ожидания рынка

- Снижение стоимости 1 Гб/с/руб (FPGA, производительность)
- Стабильность решения
- Сервис
- Зрелое сообщество
- Реальный кибербез
- Внятный road-map
- **Функционал**
- ...



Функционал

- VPN (ssl vpn)
- NAC, EDR
- Полноценный debug
- Полноценный Proxy
- Ssl-inspection с проверкой IDPS L7
- 10k-500k rules
- Максимальный стек сетевых технологий



Функционал

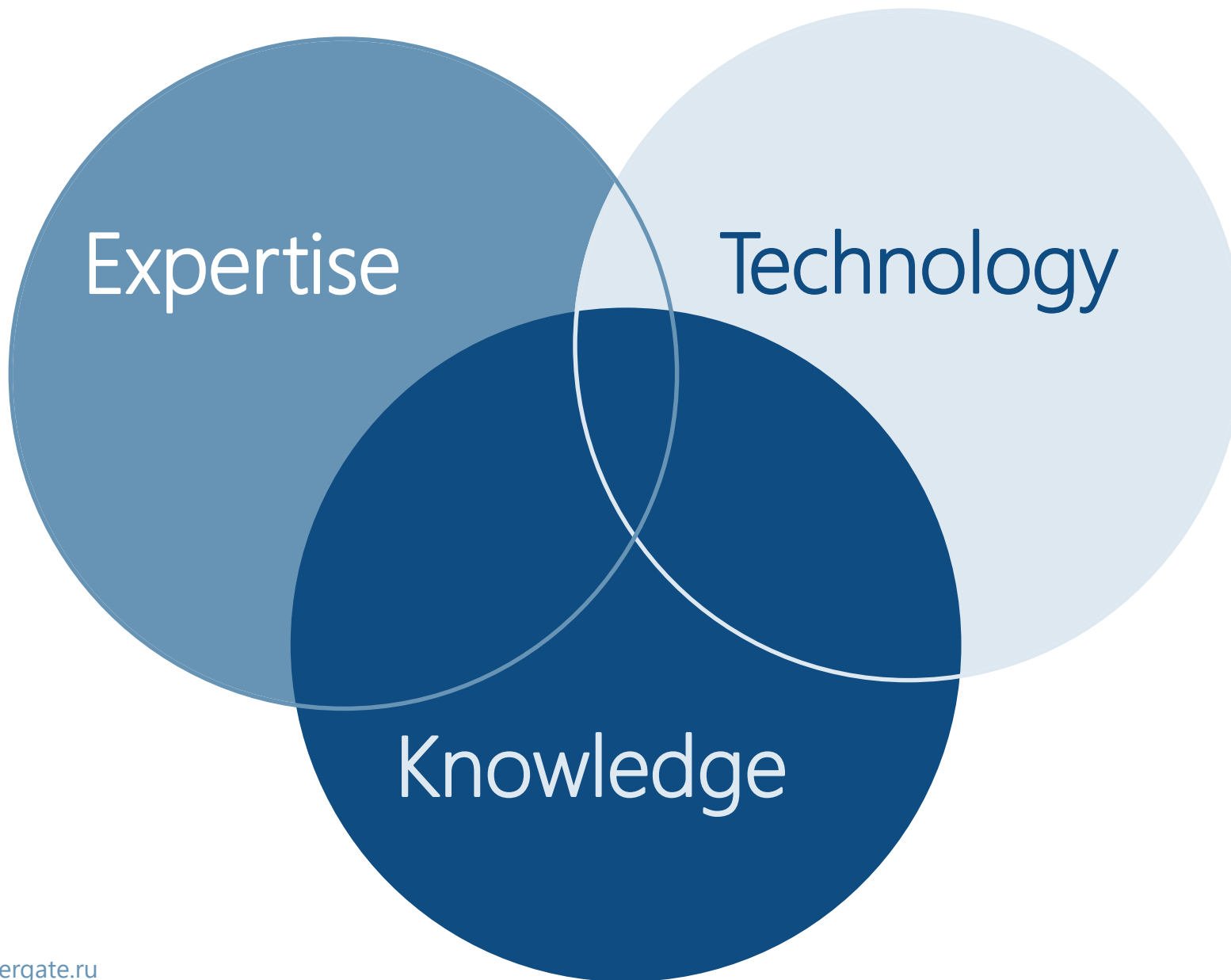
- Автоматизация процессов ИБ
- CLI
- VDOM
- UserID
- ...

Волшебная кнопка





Волшебная кнопка





Expertise

Технологии бесполезны если нет экспертизы в решении

- Сигнатуры IDPS/L7
- Правила для WAF
- Правила корреляции для SIEM
- Наполнение базы IoC, a/virus, url, IP
- Анализ защищенности
- SOC



Knowledge

Academy UserGate

- Программа обучения на базе собственных курсов или курсов партнеров
- Тестирование инженеров

Pre-sales UserGate

- Лабораторные (pre-sales)
- Знания особенностей работы других вендоров

О технологиях



UserGate NGFW

Межсетевой экран следующего поколения



Next-Generation Firewall

- Высокая скорость обработки трафика
- Идентификация пользователей
- Применение гибких политик к пользователям
- Контроль приложений на L7 уровне по всем портам
- Интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и поддержкой TLS ГОСТ
- Инспекция SSH
- Защита от DoS-атак



Безопасный доступ





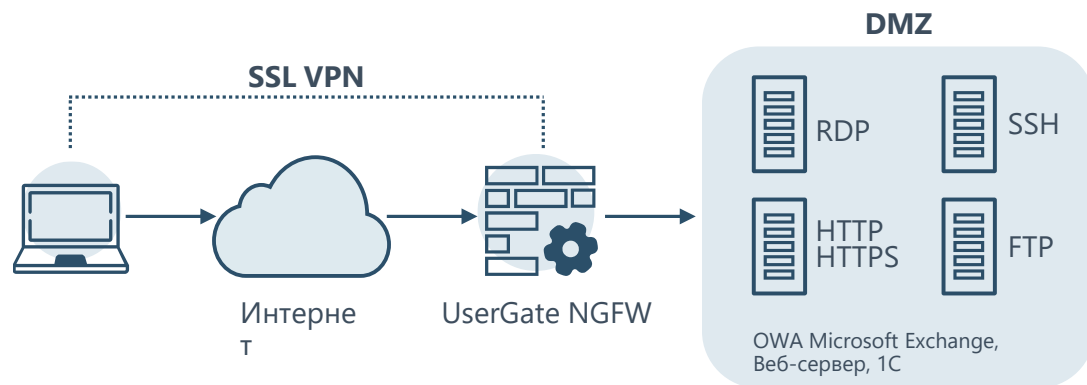
Next-Generation Firewall



Reverse Proxy – обратный прокси используется для безопасной публикации корпоративного портала и различных внутренних систем, таких как CRM, ERP, почта, а также для обеспечения доступа к определенным файлам, находящимся на внутренних серверах.



SSL VPN (Веб-портал) – позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через любой браузер, предоставляя удобство использования SSO для опубликованных сервисов, поддерживающих авторизацию по Kerberos, NTLM, SAML в том числе с поддержкой MFA.



Remote access VPN – для удаленного доступа клиентов.

Site-to-Site VPN – для защищенного соединения офисов.

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных – протокол IPSec. Поддерживается многофакторная авторизация пользователей при подключении к сервису VPN.



IDPS (COB)





Система обнаружения вторжений

Позволяет реагировать на атаки злоумышленников, использующих известные уязвимости, а также распознавать вредоносную активность внутри сети.

The screenshot displays the interface of an intrusion detection system. On the left, there is a search filter panel with four columns: 'Уровень угрозы' (Threat Level), 'Протокол' (Protocol), 'Категория' (Category), and 'Класс' (Class). The 'Уровень угрозы' column has five options: 1 (очень низкий), 2 (низкий), 3 (средний), 4 (высокий), and 5 (очень высокий). The 'Протокол' column has three options: icmp, ip, tcp, and udp. The 'Категория' column has a scrollable list of categories including activex, attack_response, current_events, dns, dos, exploit, ftp, imap, info, malware, misc, mobile_malware, netbios, p2p, and policy. The 'Класс' column has a scrollable list of classes including attempted-user, attempted-admin, attempted-dos, attempted-recon, attempted-user, bad-unknown, default-login-attempt, denial-of-service, misc-activity, network-scan, non-standard-protocol, not-suspicious, policy-violation, and protocol-command-decode. A 'Применить' (Apply) button is at the bottom right of the filter panel.

On the right, there is a 'Сигнатуры' (Signatures) section with a table of detected signatures. The table has five columns: 'Сигнатура' (Signature), 'Прото...' (Protocol), 'Класс' (Class), 'CVE', and 'Категория' (Category). The table contains 12 rows of data, each with a red '5' icon in the first column.

Сигнатура	Прото...	Класс	CVE	Категория
UPDATE Protocol Trojan Communication detected on http ports	tcp	trojan-activity	Нет	trojan
dbms_repat.alter_priority_varchar2 buffer overflow attempt	tcp	attempted-user	Нет	sql
Suspected CHAOS CnC Inbound (persistence enable)	tcp	trojan-activity	Нет	trojan
CygniCon CyViewer ActiveX Control SaveData Insecure Method Vulnerability	tcp	attempted-user	Нет	activex
Win32/Infostealer.Snifula File Upload	tcp	trojan-activity	Нет	trojan
Possible ZyXEL P660HN-T v1 RCE	tcp	attempted-user	Нет	exploit
User-Agent (Win95)	tcp	trojan-activity	Нет	malware
STAT overflow attempt	tcp	attempted-admin	CVE-2001-1021,CVE-2001-0...	ftp
Terror EK CVE-2016-0189 Exploit	tcp	trojan-activity	CVE-2016-0189	current_even
Hazir Site SQL Injection Attempt -- giris_yap.asp sifre UPDATE	tcp	web-application-attack	CVE-2006-7161	web
Rialto SQL Injection Attempt -- searchoption.asp acreage1 INSERT	tcp	web-application-attack	CVE-2006-6927	web



Контентная фильтрация



Механизмы фильтрации

- фильтрация по категориям;
- морфологический анализ;
- безопасный поиск;
- белые и черные списки;
- блокировка контекстной рекламы;
- запрет загрузки определенных видов файлов;
- антивирусная проверка трафика;
- интернет-фильтрация, инспекция SSL-трафика с поддержкой TLS 1.3 и TLS ГОСТ.



- крупнейшая база электронных ресурсов – более 600 миллионов сайтов;
- 80+ категорий;
- ежедневное обновление списка сайтов;
- повторная проверка уже внесенных ресурсов на предмет изменения контента и актуальности информации о категории.

Группы URL категорий			
+ Добавить ✎ Редактировать ✖ Удалить ↻ Обновить			
Название			
Threats			
Parental Control			
Productivity			
Safe categories			
Recommended for morphology checking			
Recommended for virus check			

Списки морфологии			
+ Добавить ✎ Редактировать ✖ Удалить ↻ Обновить			
Название списка	Author	Порог	
1 Нецензурная лексика	© UserGate	Обычный	🔄
2 Наркотики	© UserGate	Обычный	🔄
3 Порнография	© UserGate	Обычный	🔄
2 Суицид	© UserGate	Обычный	🔄
5 Терроризм	© UserGate	Обычный	🔄
3 Соответствие списку запрещенных матер...	© UserGate	Обычный	🔄
4 Азартные игры	© UserGate	Обычный	🔄
3 Соответствие ФЗ-436 (защита детей)	© UserGate	Обычный	🔄
1 Юридический (DLP)	© UserGate	Обычный	🔄
3 Бухгалтерия (DLP)	© UserGate	Обычный	🔄
3 Финансы (DLP)	© UserGate	Обычный	🔄
5 Персональные данные (DLP)	© UserGate	Обычный	🔄
2 Маркетинг (DLP)	© UserGate	Обычный	🔄
1 Соответствие списку запрещенных матер...	© UserGate	Обычный	🔄

Категории	
+ Добавить ✖ Удалить 📄 Экспорт ↻ Обновить 📂 Импорт	
Название ↑	
4	Азартные игры
2	Жестокое обращение с детьми
2	Игры
2	Наркотики
2	Насилие
5	Незаконное ПО
2	Ненависть и нетерпение
2	Нецензурная лексика
2	Нудизм
4	Обмен картинками
2	Оружие
4	Пиринговые сети
1	Поиск работы
2	Покупки

Списки URL	
+ Добавить ✎ Редактировать ✖ Удалить	
Название ↑	
3	Microsoft Windows Internet checker
5	Соответствие реестру запрещенных сайтов Роскомнадзора (URL)
3	Соответствие списку запрещенных URL Министерства Юстиции РФ (URL)
5	Соответствие списку запрещенных URL Республики Казахстан
1	Список образовательных учреждений
4	Список поисковых систем без безопасного поиска
5	Список фишинговых сайтов



Про SSL-инспекцию



Про SSL-инспекцию

Обязательно:

- Проверка всей цепочки сертификатов!!!
- Выбор алгоритма шифрования (только strong)
- TLS 1.3, TLS ГОСТ
- Проверка движком IDPS

<input checked="" type="checkbox"/>	TLS GOST2012256 with 28147 CNT IMIT
<input checked="" type="checkbox"/>	TLS GOSTR341001 with 28147 CNT IMIT

Профиль SSL:

Записывать в журнал правил:

Атрибуты:

- Блокировать сайты с некорректными сертификатами
- Проверять по списку отозванных сертификатов
- Блокировать сертификаты с истекшим сроком действия
- Блокировать самоподписанные сертификаты

Протоколы SSL

Минимальная версия TLS:

Максимальная версия TLS:

Наборы алгоритмов шифрования

[Установка алгоритмов шифрования для стандартных протоколов](#)

<input checked="" type="checkbox"/>	TLS ECDHE ECDSA with AES 256 CBC SHA384
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS ECDHE ECDSA with 3DES EDE CBC SHA
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS DHE DSS with AES 128 GCM SHA256
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 128 CBC SHA
<input checked="" type="checkbox"/>	TLS AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS ECDH ECDSA with AES 256 GCM SHA384
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS ECDH ECDSA with AES 128 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDHE RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 CBC SHA
<input checked="" type="checkbox"/>	TLS DHE RSA with AES 256 CBC SHA256
<input checked="" type="checkbox"/>	TLS ECDH RSA with AES 128 GCM SHA256
<input checked="" type="checkbox"/>	TLS DHE DSS with AES 256 GCM SHA384



Новое в 7.1



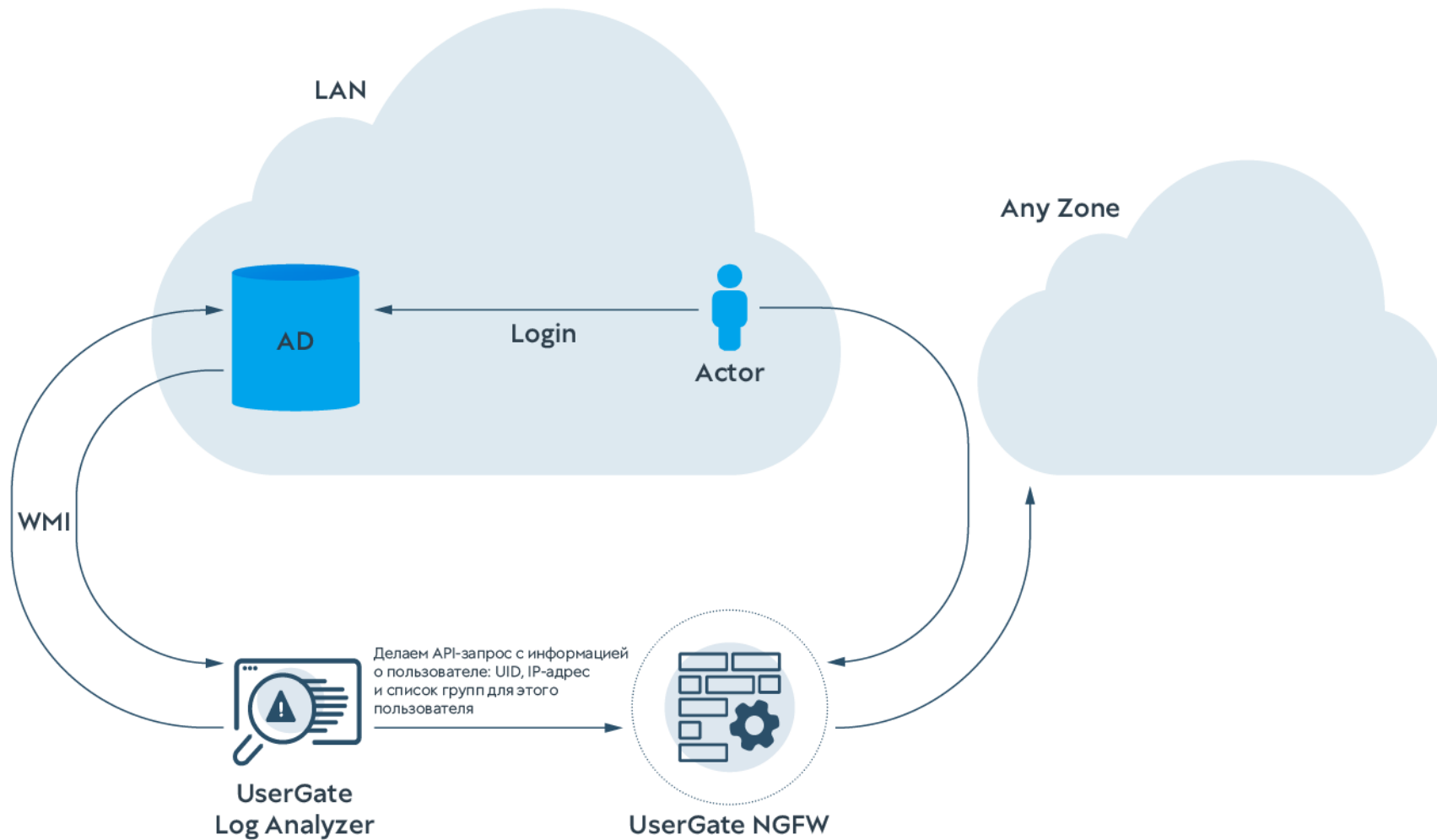


Новое в 7.1

- » UserID
- » Пользовательские сигнатуры IDPS&L7
- » Новый движок IPSv3
- » IKEv2
- » Темная тема
- » UserGate Client
- » UserGate SIEM Light (MVP)



UserID





Создание собственных сигнатур

The screenshot shows a dialog box titled "IPS_CUSTOM_SIGNATURE_DIALOG [Entensys.window.IPSCustomSignaturePropertiesDialog]". It has two tabs: "GENERAL_PROPERTIES" and "IPS_SIGNATURE_UASL", with the latter being active. The dialog contains the following fields and controls:

- Buttons at the top: "Включить", "Отключить", "Восстановить по умолчанию", and "IPS_SIGNATURE_ENABLE: Все".
- Field: "IPS_SIGNATURE_ENABLED:" with a checked checkbox.
- Field: "Название:" with an empty text input box.
- Field: "Описание:" with an empty text area.
- Field: "Угроза сигнатуры:" with a dropdown menu showing "1 очень низкий".
- Field: "Операционная система сигнатуры:" with a dropdown menu showing "SELECT_VALUE".
- Field: "Класс:" with a dropdown menu showing "SELECT_VALUE".
- Field: "Категория:" with a dropdown menu showing "SELECT_VALUE".
- Field: "CVE:" with a text input box containing "IPS_REF_CVE_EXAMPLE".
- Field: "URL:" with a text input box containing "IPS_REF_URL_EXAMPLE".
- Buttons at the bottom: "Сохранить" and "Отмена".



Создание своего профиля IDPS

с возможностью автоматического обновления
при появлении новых сигнатур соответствующего типа

Свойства профиля COB [Entensys.window.IPSProfilePropertiesDialog]

IPS_GENERAL_PROPERTIES | IPS_FILTERS_TAB | **IPS_SIGNATURE_TAB**

BTN_OVERRIDE | Включить | Отключить | Восстановить по умолчанию | Показать Все ▾

IPS_SIG...	Название сигнатуры ↑	IPS_SIGNAT...	Операционн...	Протокол	Класс
20020090	(MS00-021)Microsoft NT / Win...	IPS_SIG...	Windows	tcp	denial-of-ser...
20020052	(MS00-040)Microsoft Windows ...	IPS_SIG...	Cisco	tcp	denial-of-ser...
22000122	(MS00-092)Microsoft SQL Serv...	IPS_SIG...	Windows	tcp	arbitrary-cod...
22000124	(MS00-092)Microsoft SQL Serv...	IPS_SIG...	Windows	tcp	arbitrary-cod...
22000170	(MS02-038)Microsoft SQL Serv...	IPS_SIG...	Windows	tcp	arbitrary-cod...
22000160	(MS02-039)Microsoft SQL Sla...	IPS_SIG...	Windows	udp	arbitrary-cod...
22040024	(MS03-051)Microsoft FrontPag...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20020194	(MS04-007)LSASS.EXE Remot...	IPS_SIG...	Linux	tcp	denial-of-ser...
20140538	(MS05-053)Internet Explorer W...	IPS_SIG...	Windows	tcp	denial-of-ser...
20142806	(MS06-001)Windows Metafile ...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20142804	(MS06-001)Windows Metafile ...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20141458	(MS06-014)Internet Explorer M...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20020490	(MS06-035)Microsoft Windows ...	IPS_SIG...	Windows	tcp	denial-of-ser...
20020500	(MS06-035)Microsoft Windows ...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20020492	(MS06-063)Microsoft Windows ...	IPS_SIG...	Windows	tcp	denial-of-ser...
20024	(MS07-003)Microsoft Outlook V...	IPS_SIG...	Windows	tcp	arbitrary-cod...
20140380	(MS07-014)Microsoft Word 200...	IPS_SIG...	Windows	tcp	arbitrary-cod...
24040132	(MS07-017)Microsoft Windows ...	IPS_SIG...	Windows	tcp	arbitrary-cod...

« < | Страница 1 из 132 | > » | Найти: Всего: 9280 (найдено: 3293)

Сохранить | Отмена

A decorative graphic on the right side of the slide, consisting of a complex network of light blue lines and dots, resembling a molecular structure or a data network.

В рамках UserGate SUMMA



UserGate Client

Endpoint Protection / VPN / EDR / NAC



UserGate Client – агент SUMMA

- видимость событий безопасности;
- контроль устройства;
- доступ с нулевым доверием.



Сбор информации с устройства

- состояние, память и производительность;
- безопасность;
- USB-устройства;
- элементы автозагрузки;
- процессы;
- службы;
- ключи реестра;
- программное обеспечение;
- установленные обновления.



Персональный межсетевой экран

Свойства правила межсетевого экрана [Entensys.window.endpoint.FirewallRulePropertiesDialog]

Общие Пользователи Источник Назначение Сервис Приложения Списки URL Категории сайтов Типы контента Время HIP

Включено:

Название:

Описание:

Область применения:

Действие:

Прокси-сервер:

Журналирование:

Вставить:

Сохранить Отмена



НАС

Профили устройств:

- продукт;
- процесс;
- запущенная служба;
- ключи реестра;
- установленные обновления.



VPN

- Client2Site – IPSec/L2TP, IKEv2;
- SSL VPN;
- «принудительный» VPN.



Экспертиза, IoC

Данные из логов, которые можно обогатить и найти следы компрометации:

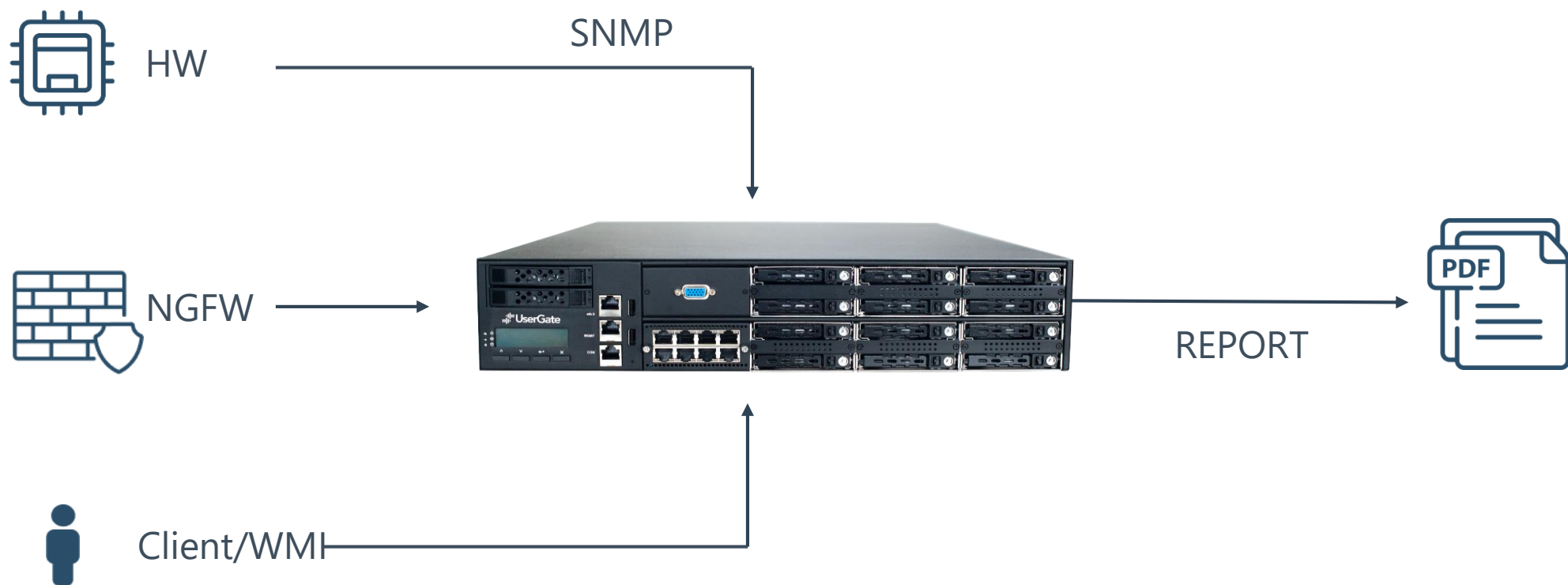
- IP-адреса;
- домены;
- имена и хеши файлов;
- ветки реестра.

Анализ инцидентов





Анализ инцидентов





Новый продукт - SIEM Light



Что есть?

Нормализация событий от сторонних источников

Корреляция событий и поиск инцидентов

Оповещение и автоматическое реагирование

Workflow для расследования (IRP)

Журналы и отчетность

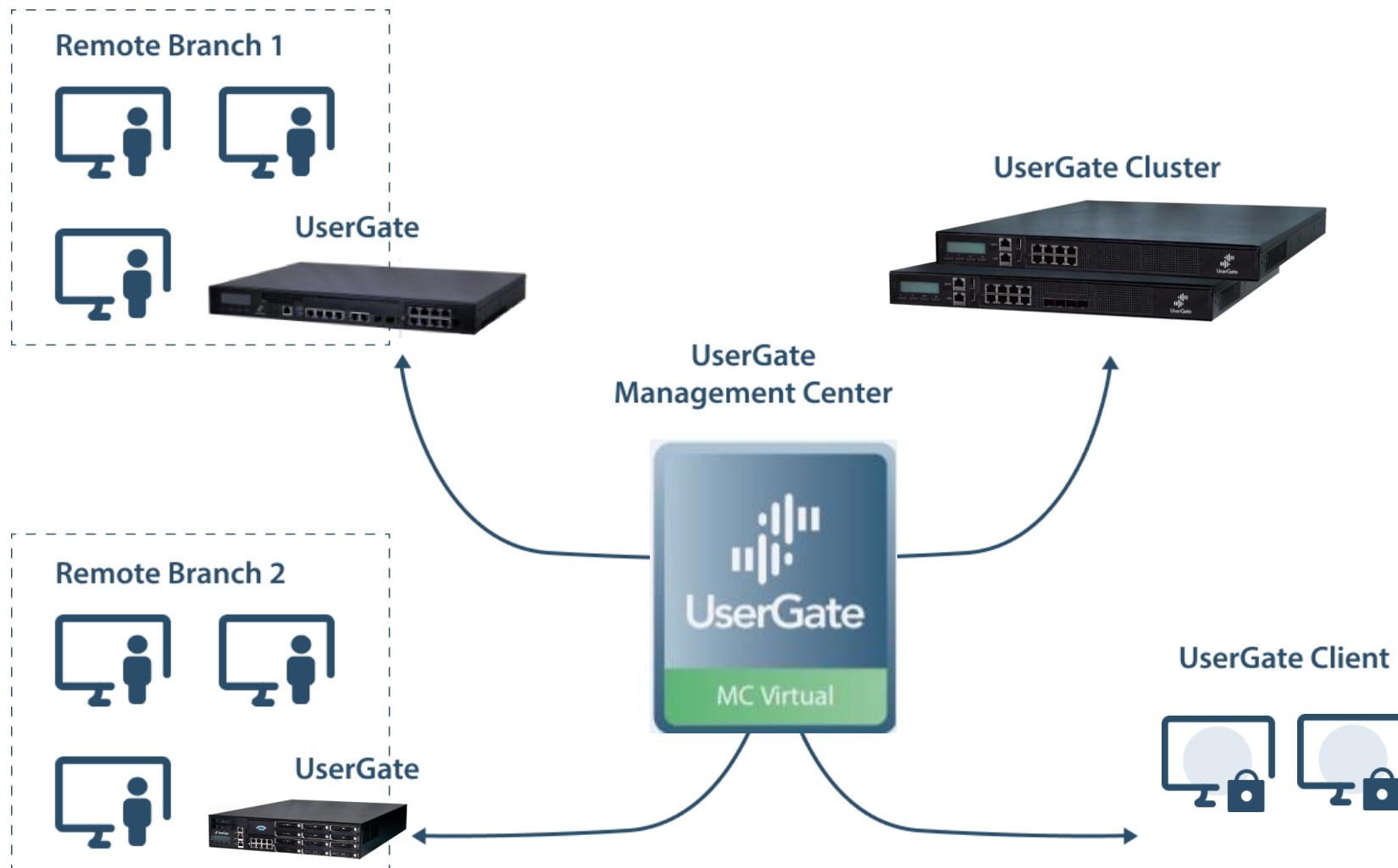
ЭКСПЕРТИЗА

Централизованное управление





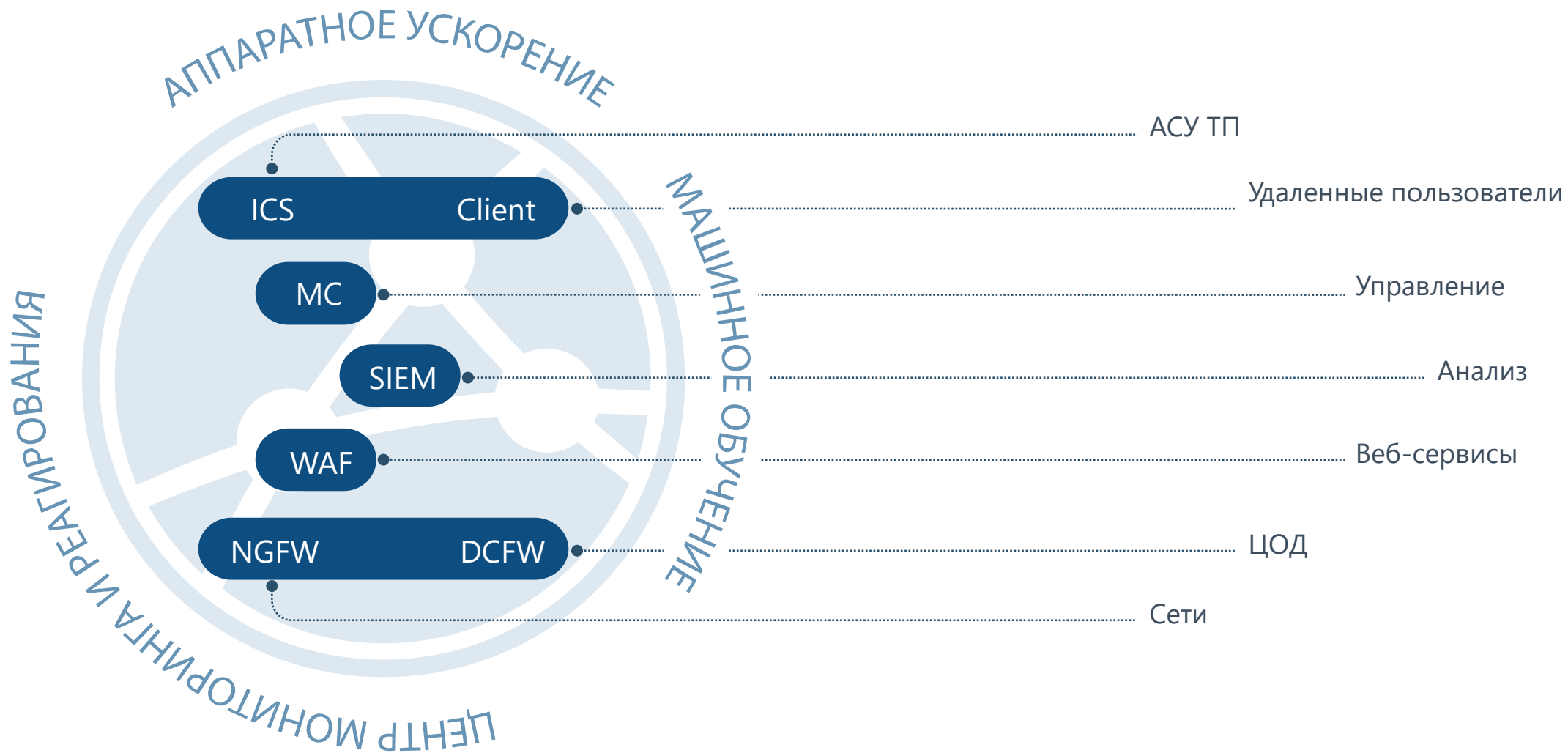
Управление устройствами





UserGate SUMMA

100% видимость событий безопасности

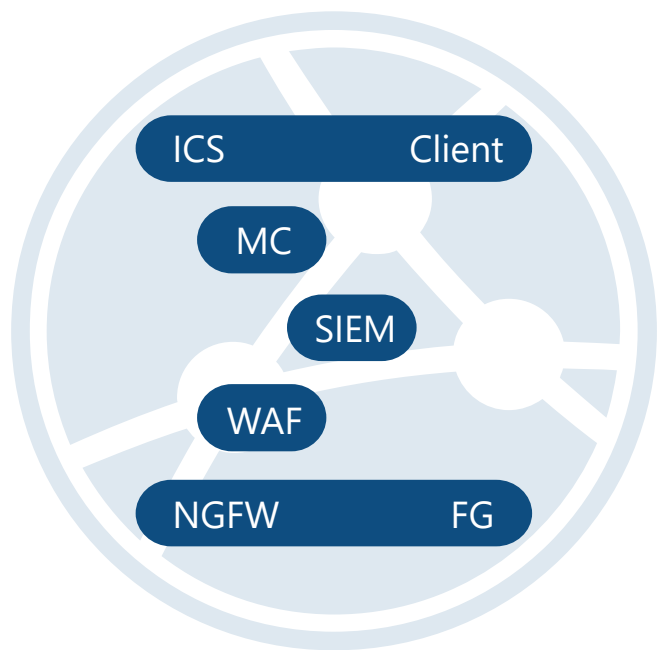




Формы поставки



Продукты UserGate SUMMA доступны в виртуальном исполнении



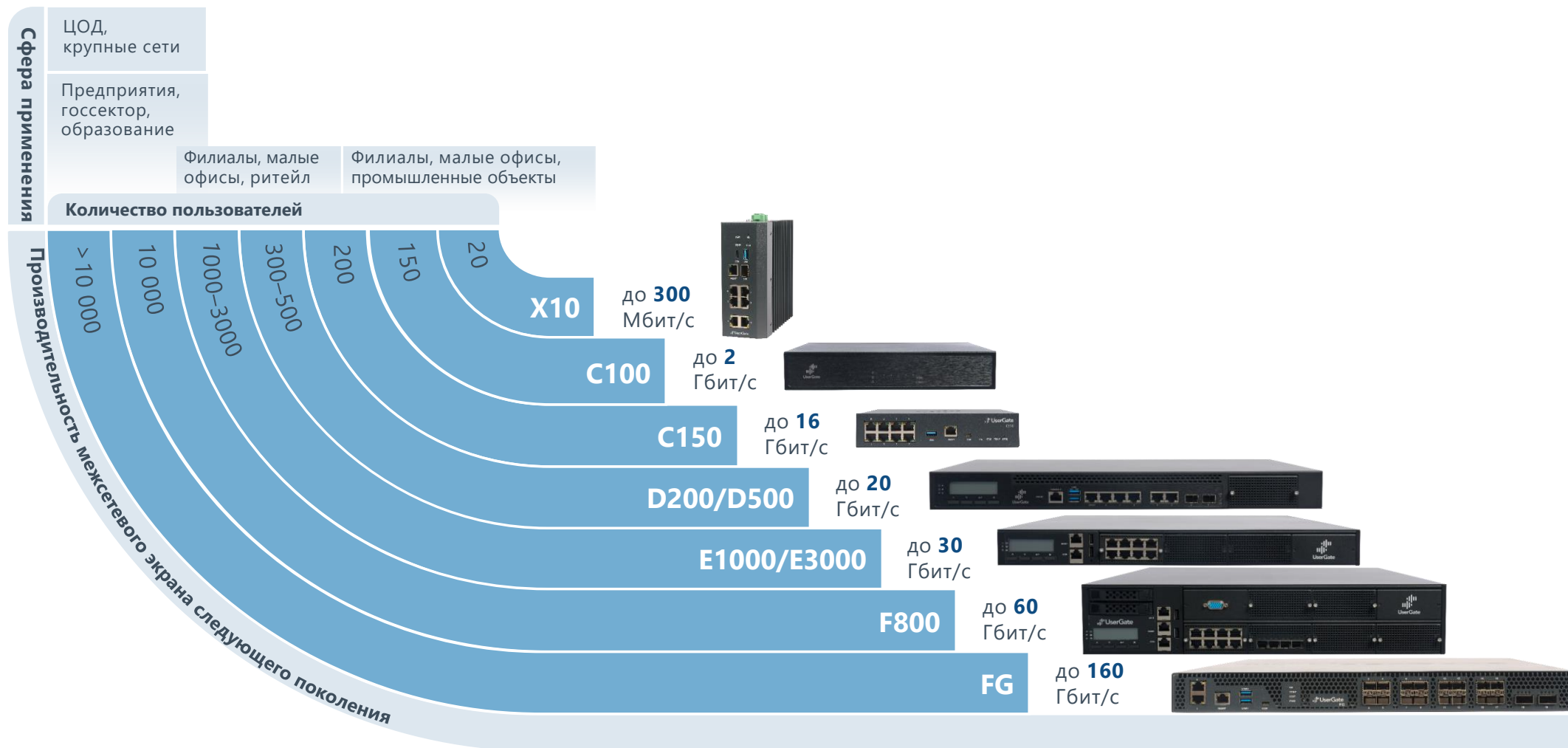
Гипервизоры:





UserGate NGFW

Модельный ряд аппаратных платформ



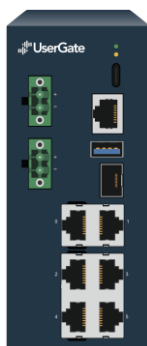
A decorative graphic on the right side of the slide, consisting of a network of light blue lines and dots, resembling a molecular structure or a data network, set against a dark blue background.

Собственные разработки железа



Собственные аппаратные платформы

МПТ



Модель X10

- FW до 2,5 Гб/с
- ARM 4 cores
- 6 портов 1GbE с поддержкой bypass
- 1 порт SFP
- два блока питания
- от – 40 °C до +70 °C
- крепление на DIN-рейку



Модель C150

- FW до 8 Гб/с
- ARM 8 cores
- 8 портов 1GbE с поддержкой bypass
- два блока питания
- от 0 °C до +70 °C



Новые платформы



FG



C150



B50

A decorative graphic on the right side of the slide, consisting of a complex network of light blue lines and dots, resembling a molecular structure or a data network, set against a dark blue background.

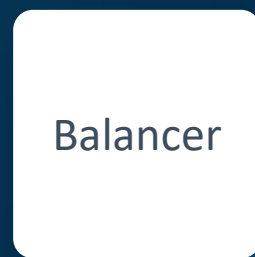
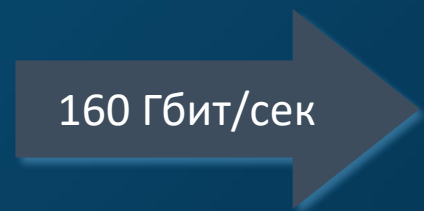
Высокопроизводительный FW

UserGate FG

- » CPS - 80 000 сессий в секунду
- » CC - 11 000 000 TCP сессий
- » UDP 1518 byte - 150+ гбит/с
- » EMIX - 65 гбит/с (цифра из ограничения тестового стенда)
- » CPS - 35 000, 10 000 правил
- » 80M PPS



2x100 + 16x10, wirespeed





Реализованные проекты



ГБУ РС (Я) Республиканский центр информационных технологий

ПАК UserGate F8000 и UserGate Log Analyzer

- Защита от атак и угроз;
- Безопасный выход в интернет;
- Фильтрация трафика;
- Контроль приложений;
- Анализ событий и инцидентов.



ООО «АльфаСтрахование — ОМС»

Контентная фильтрация web-трафика

- Переход с иностранного вендора;
- Оптимизация оборудования;
- Безопасный выход в интернет;
- Фильтрация трафика.



Пилотирование UserGate



DEMO

Отправьте заявку на пилотирование или
запросите демонстрацию решений
UserGate

sales@usergate.ru

8 (800) 500-40-32



**Спасибо
за внимание!**

