МСЭ нового поколения, смотрящий глубже и шире

Cisco ASA с функциями FirePOWER

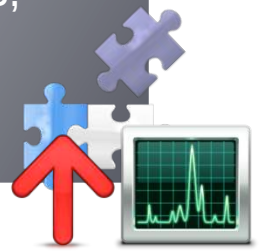
Назим Латыпаев
Системный Инженер
nlatypae@cisco.com

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Проблемы с традиционной моделью «эшелонированной» безопасности

Точечные продукты

Высокая сложность, меньшая эффективность



Ручные и статические механизмы

Медленный отклик, ручное управление, низкая результативность

Слабая прозрачность

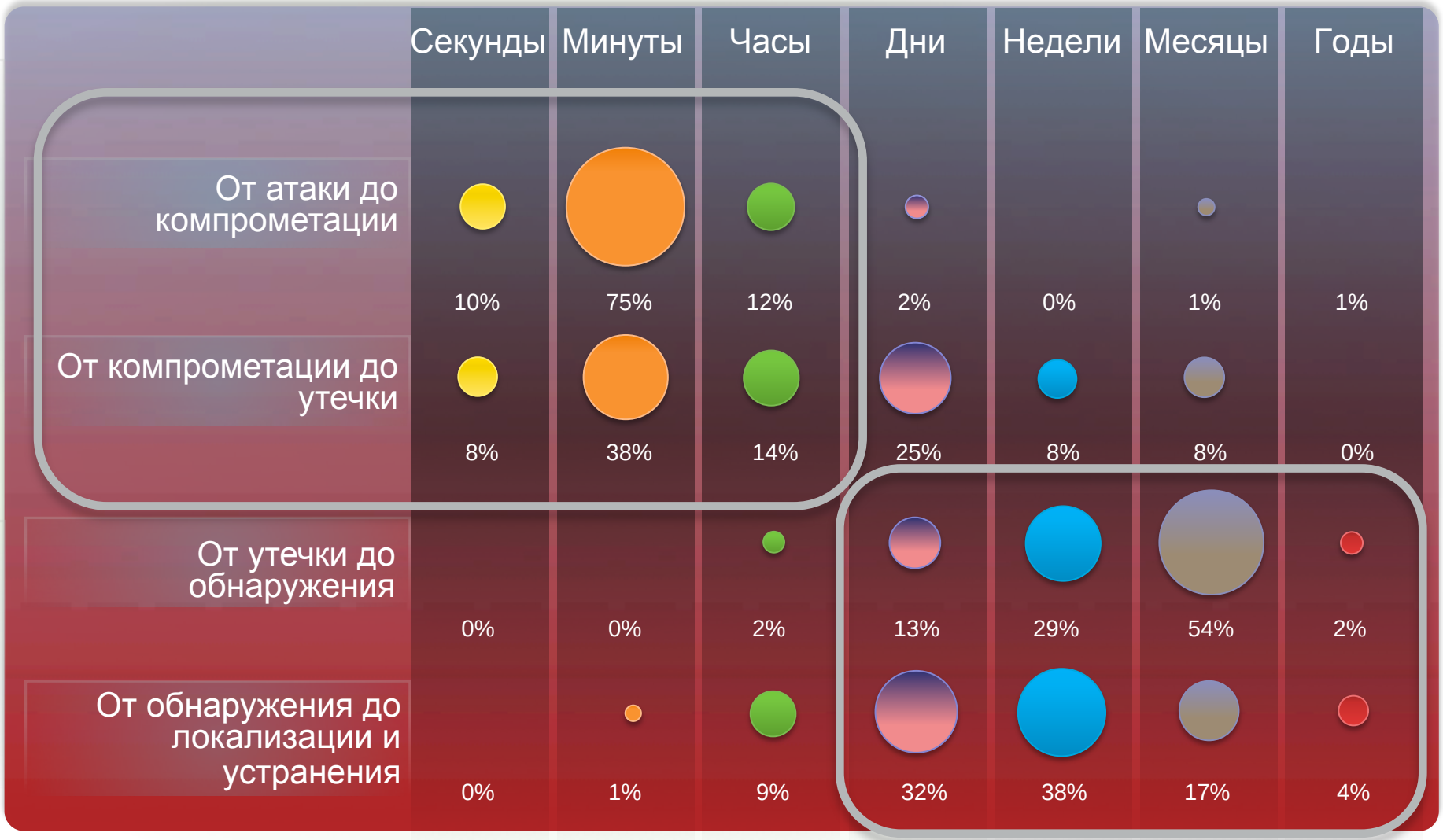
Многовекторные и продвинутые угрозы остаются незамеченными

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Результат печален – потребитель проигрывает

Взломы осуществляются за минуты

Обнаружение и устранение занимает недели и месяцы

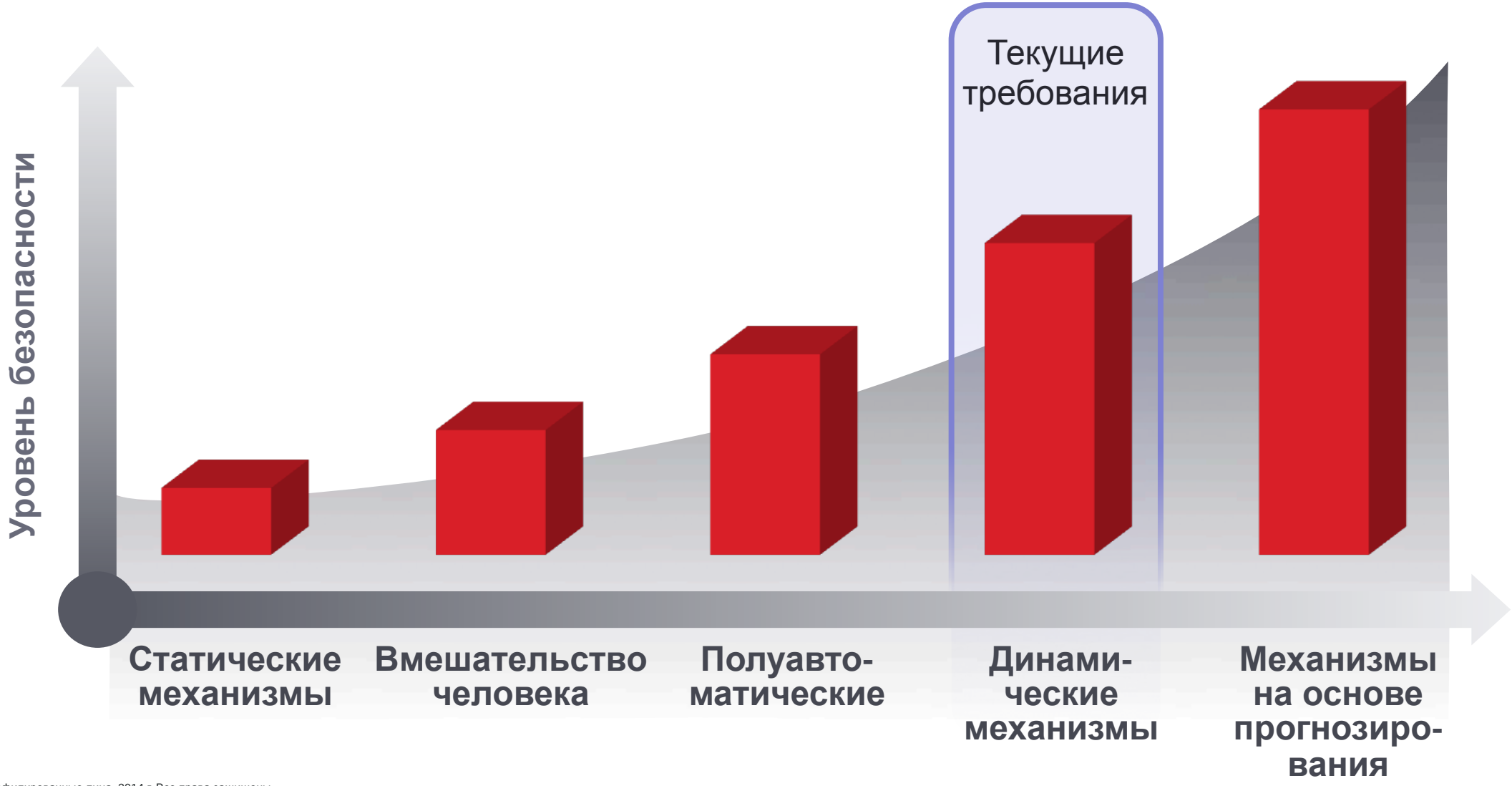


Временная шкала событий в % от общего числа взломов

Источник: 2012 Verizon Data Breach Investigations Report

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Эволюция механизмов безопасности



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Cisco: в центре внимания — безопасность!

Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделене Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

AMP + FirePOWER
AMP > управляемая защита от угроз

Cognitive + AMP

Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

Приобретение компании ThreatGRID

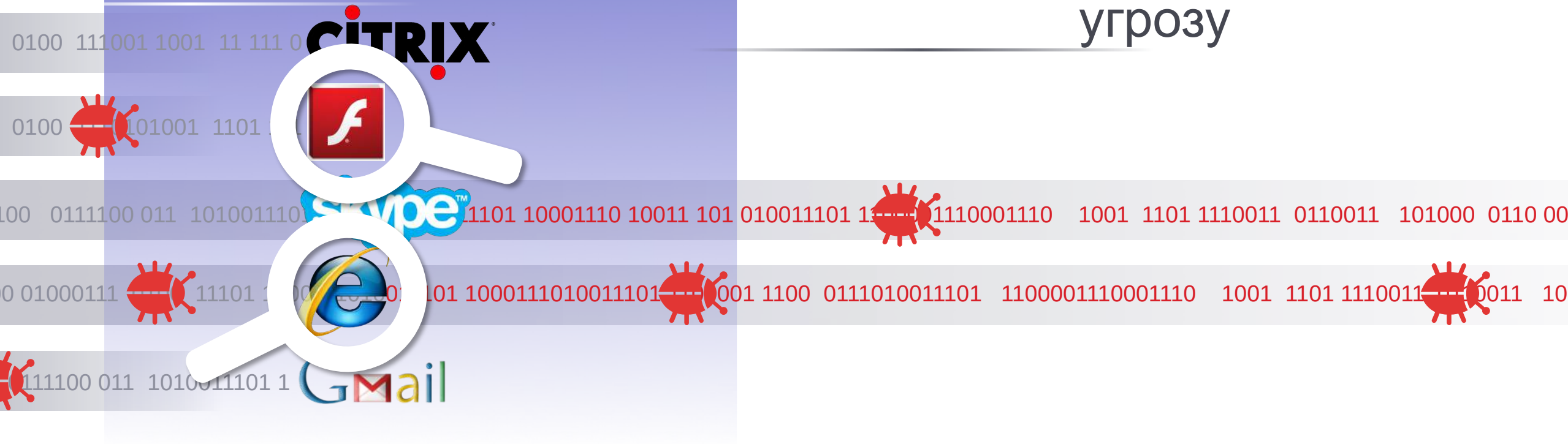
- Коллективный анализ вредоносного кода
- Анализ угроз

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Что не так с прежними МСЭ нового поколения?

Фокусируются на приложениях…

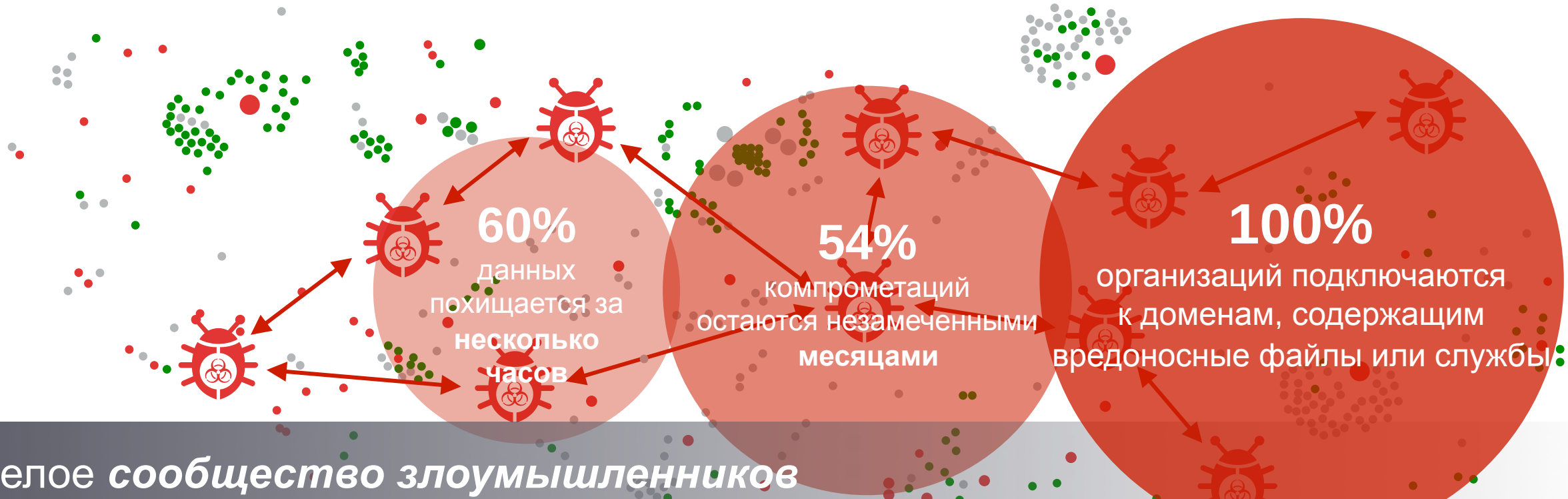
Но полностью упускают из вида угрозу



Прежние МСЭ нового поколения могли уменьшить область атаки, но усовершенствованный вредоносный код часто обходил защитные механизмы.

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Современный ландшафт угроз требует большего, чем просто контроль приложений



Целое ***сообщество злоумышленников*** остается нераскрытым, будучи у всех на виду
Они стремительно атакуют и остаются неуловимыми

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Комплексная защита от угроз в течение всего жизненного цикла атаки

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Первый в отрасли МСЭ нового поколения, смотрящий шире и глубже других

Cisco ASA с функциями FirePOWER

Особенности

- Межсетевое экранирование Cisco® ASA в сочетании с системой предотвращения вторжений Sourcefire® нового поколения
- Усиленная защита от вредоносного кода Advanced Malware Protection (AMP)
- Лучшие в своем классе технологии анализа ИБ (SI), мониторинга и контроля приложений (AVC) и фильтрации URL-адресов

Преимущества

- Непревзойденная, многоуровневая защита от угроз
- Беспрецедентная прозрачность сетевой активности
- Комплексная защита от угроз на всем протяжении атаки
- Снижение стоимости и сложности систем

«С помощью многоуровневой защиты организации смогут расширить возможности для мониторинга, внедрить динамические механизмы безопасности и обеспечить усиленную защиту в течение всего жизненного цикла атаки»

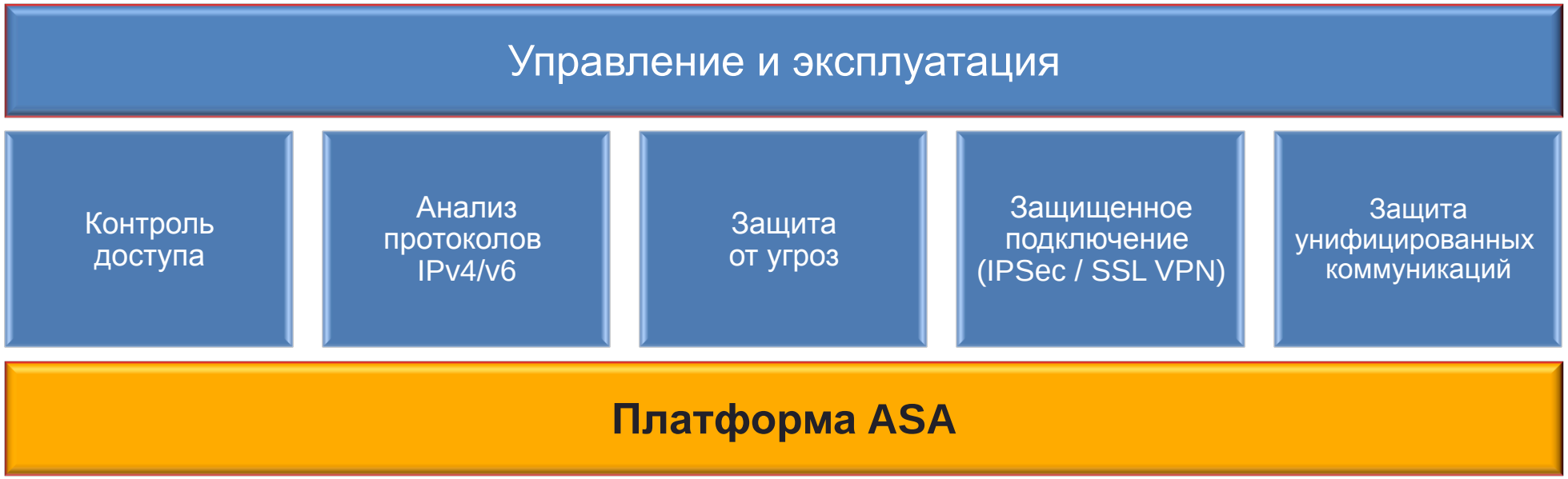
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Непревзойденная комплексная и многоуровневая защита

- Самый популярный межсетевой экран ASA корпоративного класса с функцией контроля состояния соединений
- Система гранулярного мониторинга и контроля приложений (Cisco® AVC)
- Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- Фильтрация URL-адресов на основе репутации и классификации
- Система Advanced Malware Protection с функциями ретроспективной защиты

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

В основе лежит платформа Cisco ASA 5500-X



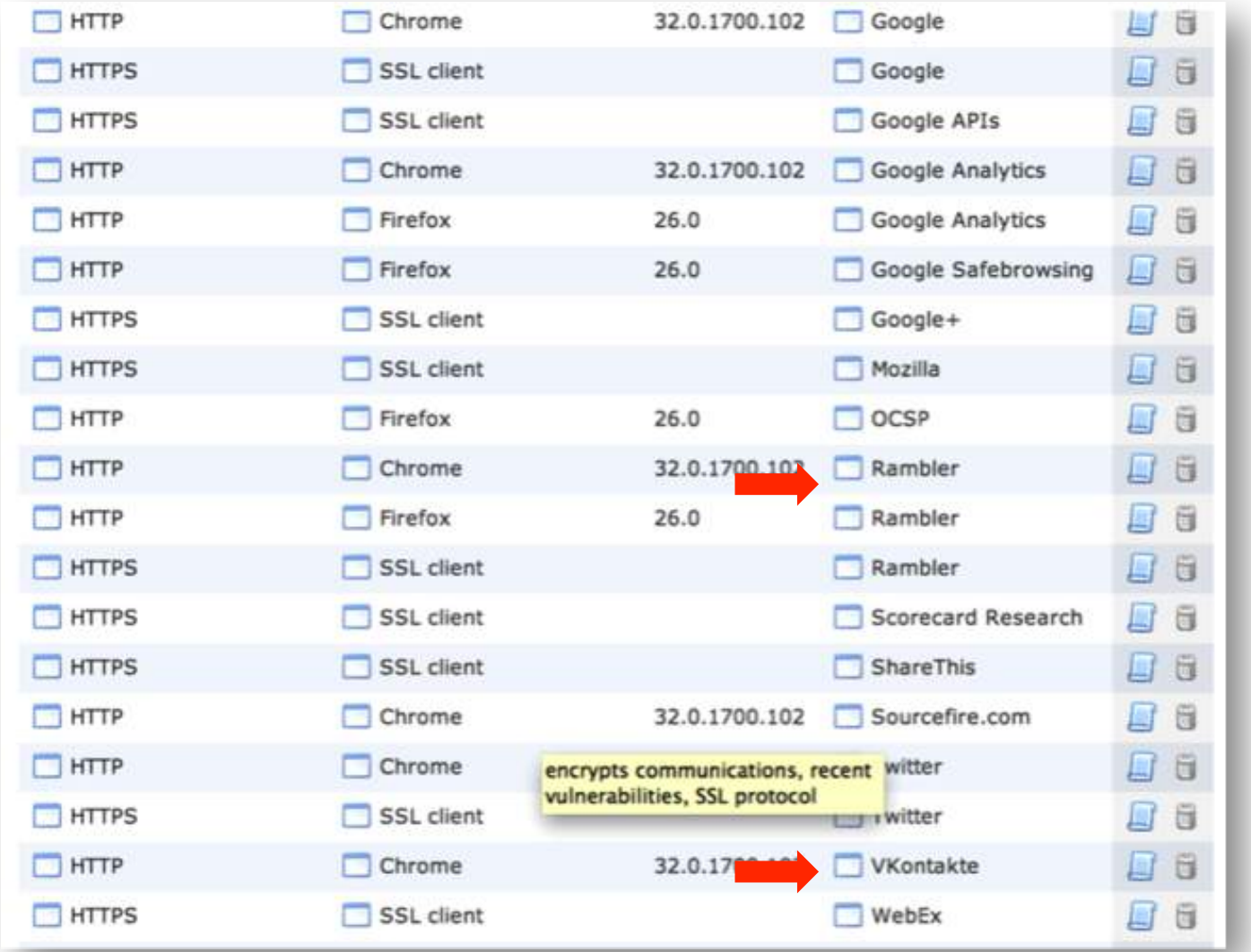
- Высокопроизводительная масштабируемая платформа
- Высокая доступность, надежность и отказоустойчивость
- Интеллектуальные сетевые сервисы
- Виртуализация, прозрачность функционирования
- Широкий модельный ряд
- Сертификация производства в ФСТЭК по 3-му классу для МСЭ

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Распознавание приложений

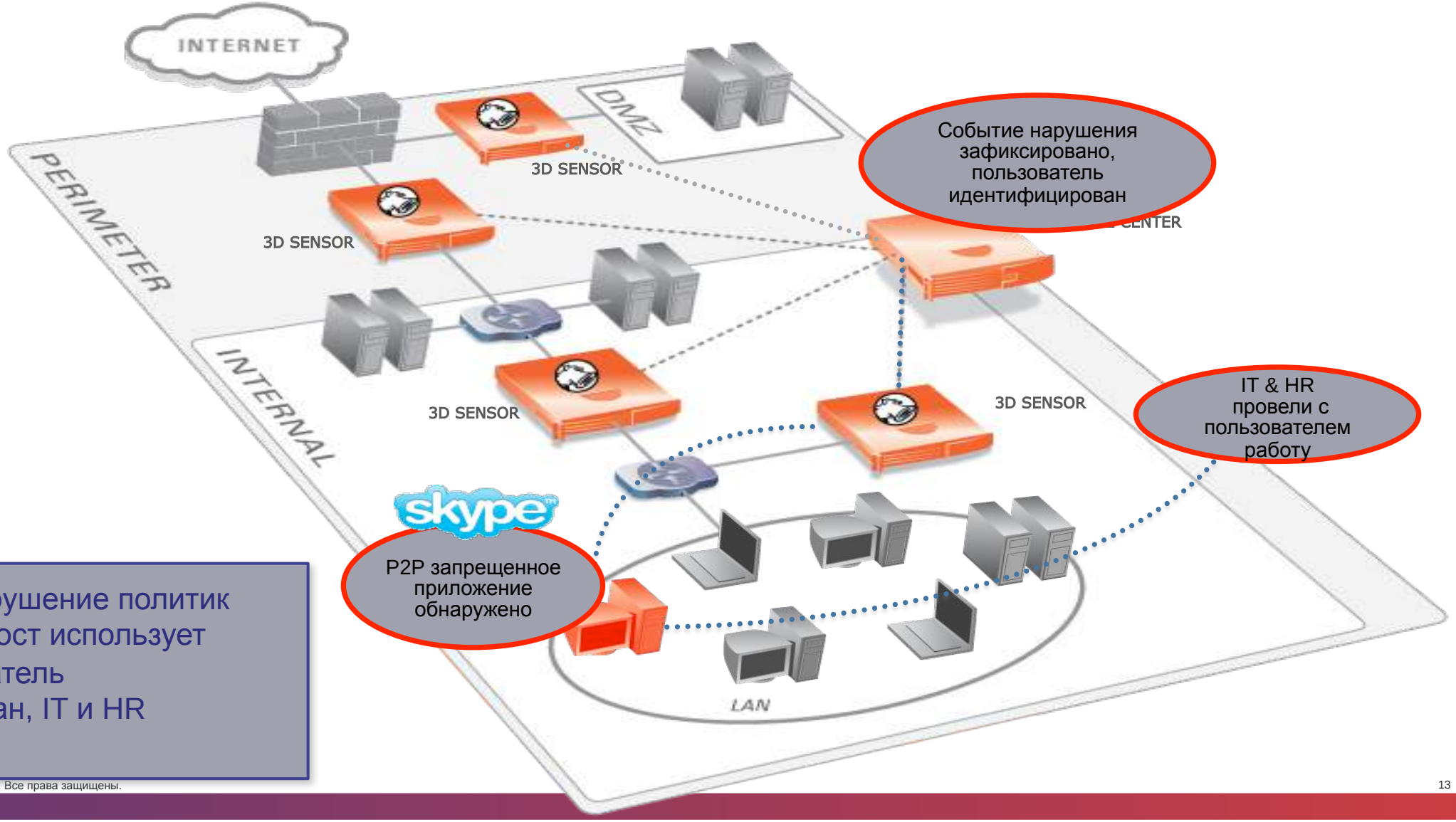
Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности

FirePOWER for ASA распознает и «российские» приложения



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

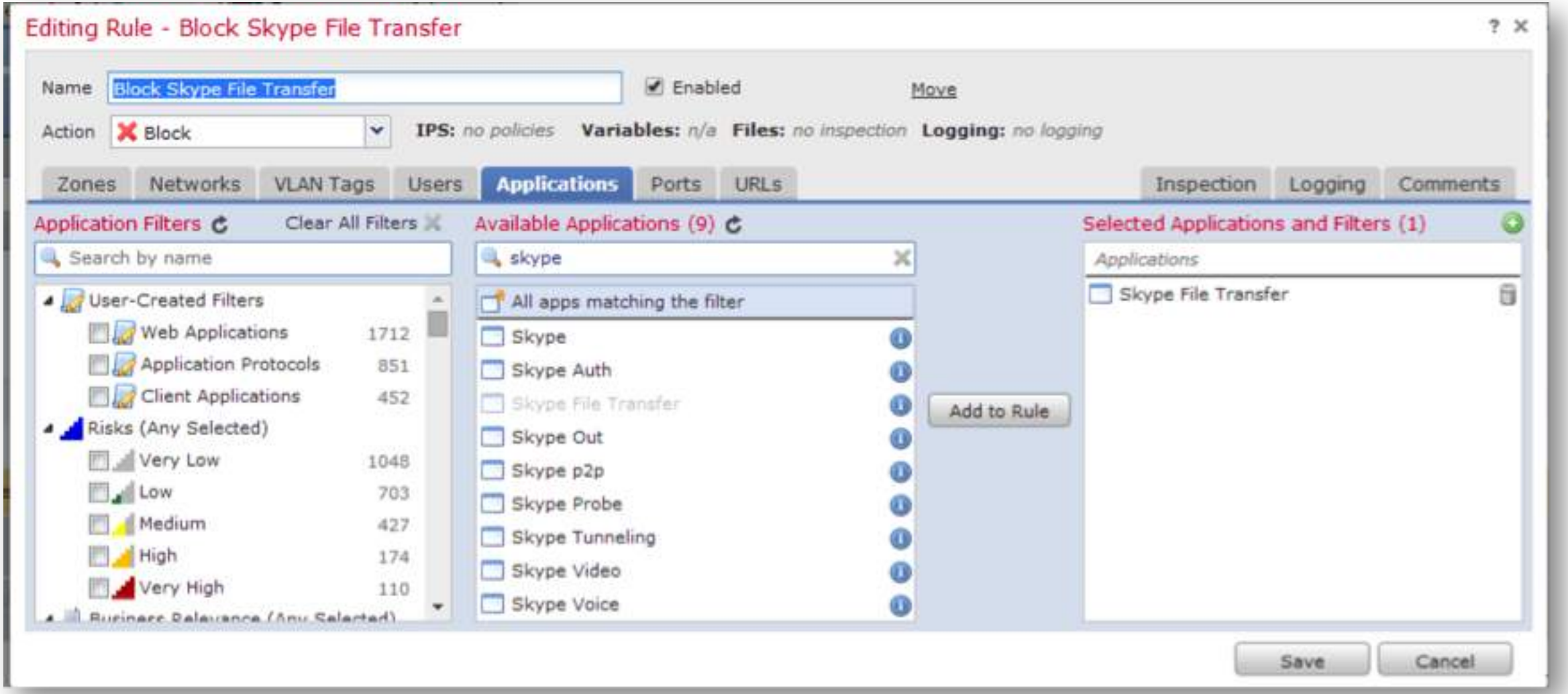
Идентификация приложений «на лету»



Обнаружено нарушение политик безопасности. Хост использует Skype. Пользователь идентифицирован, IT и HR уведомлены.

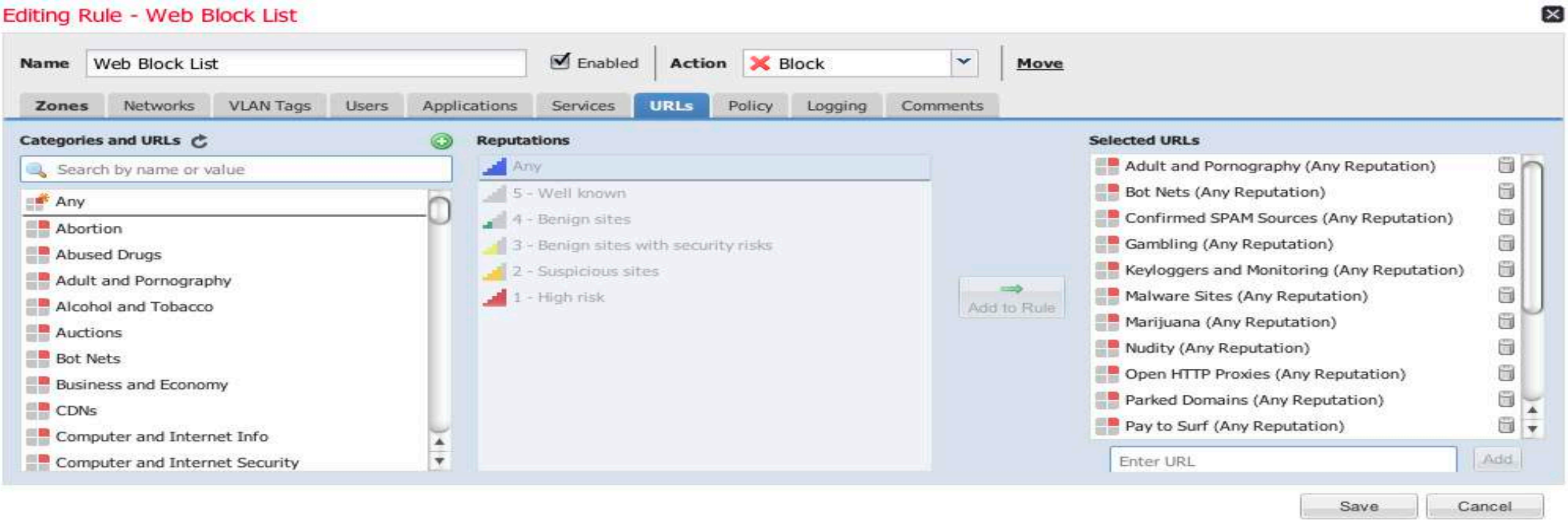
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Блокирование передачи файлов Skype



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Фильтрация URL

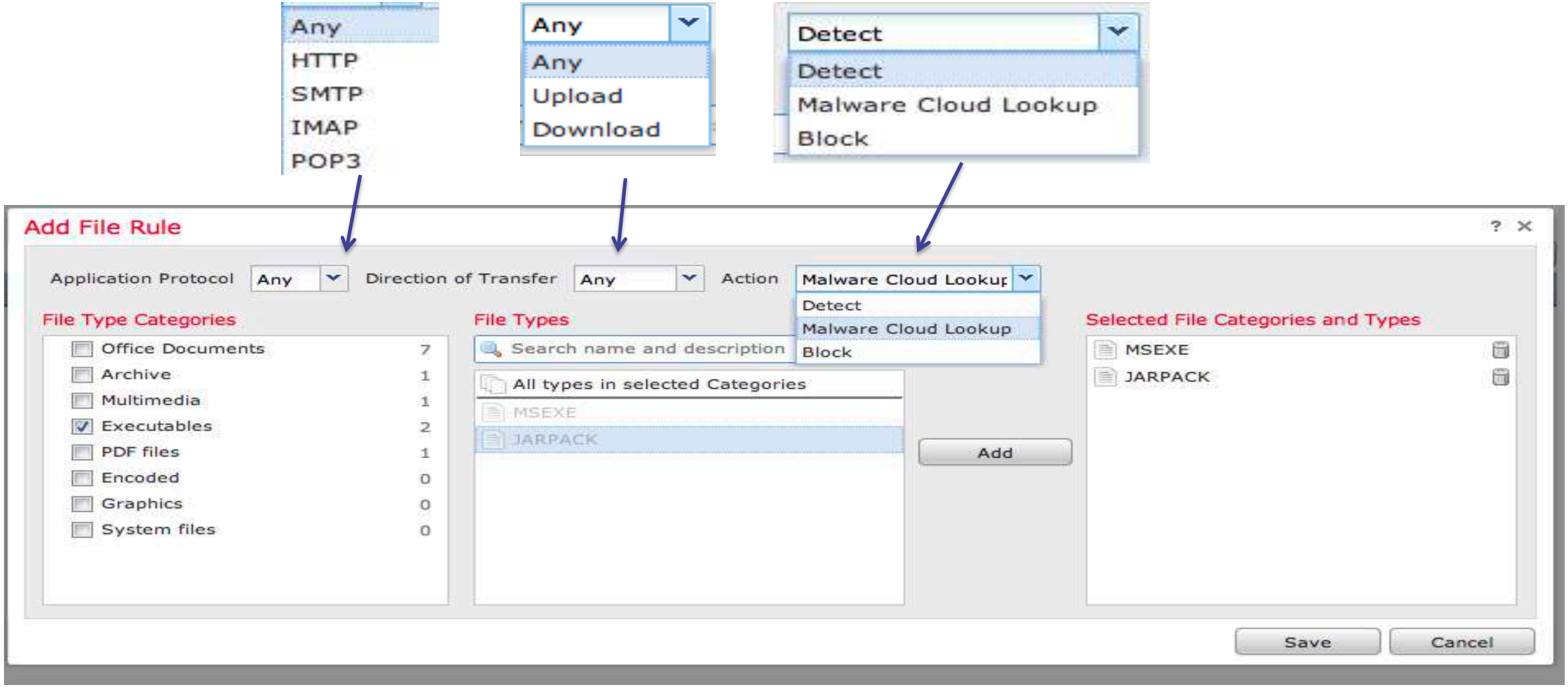


Различные категории URL

URLs категорированы по уровню рисков

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Контроль по типам файлов и направлению передачи



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Геолокация и визуализация местонахождения атакующих

Top Events by Source Country

Country Name	Count
United States	162
Germany	36
China	18
Japan	13
France	11
Russia	4
North Korea	2
Pakistan	1
Iraq	1
Iran	1

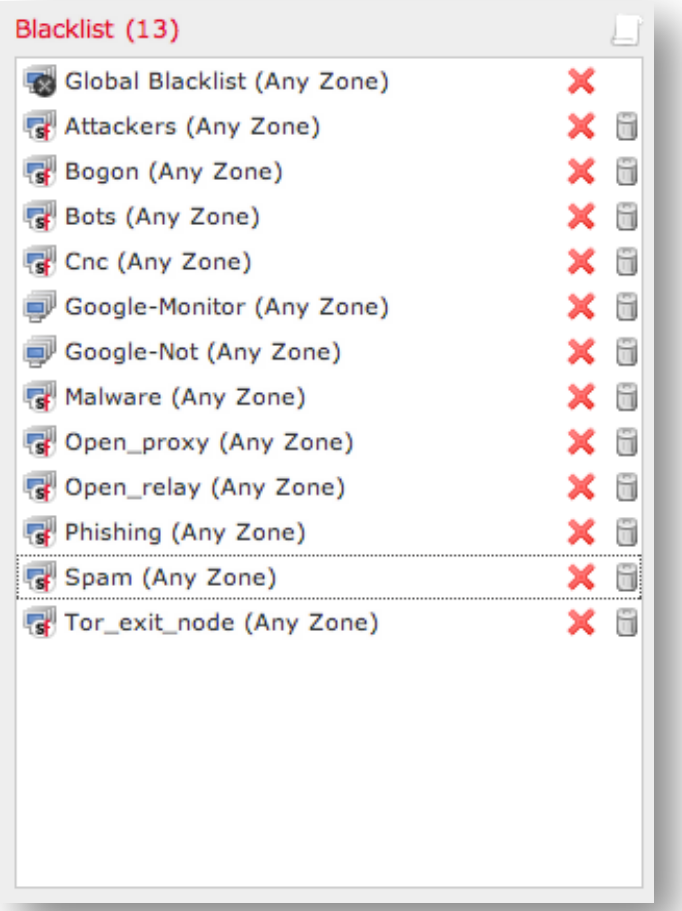
Last updated 1 minutes ago

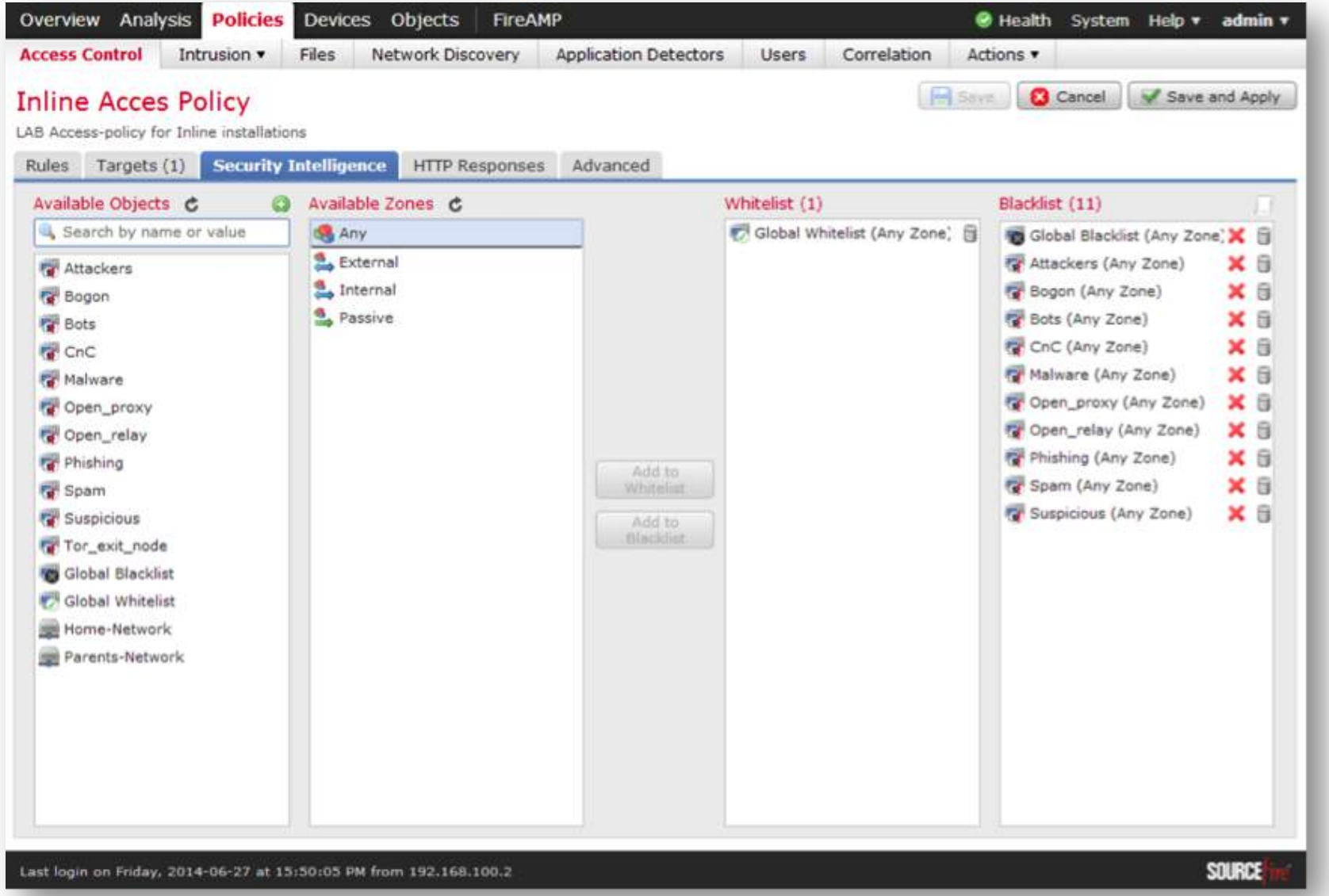
Initiator IP	Initiator Location	Responder IP
76.100.209.66	USA	10.4.32.112
10.4.10.131		10.4.32.112
10.4.10.131		10.4.32.112
10.4.33.95		10.5.32.206
89.188.101.82	ISR	10.5.32.206
200.189.215.85	BRA	10.4.33.44
10.4.31.237		10.5.32.206
10.4.11.216		10.5.39.206

Визуализация карт, стран и городов для событий и узлов

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

«Черные списки»: свои или централизованные

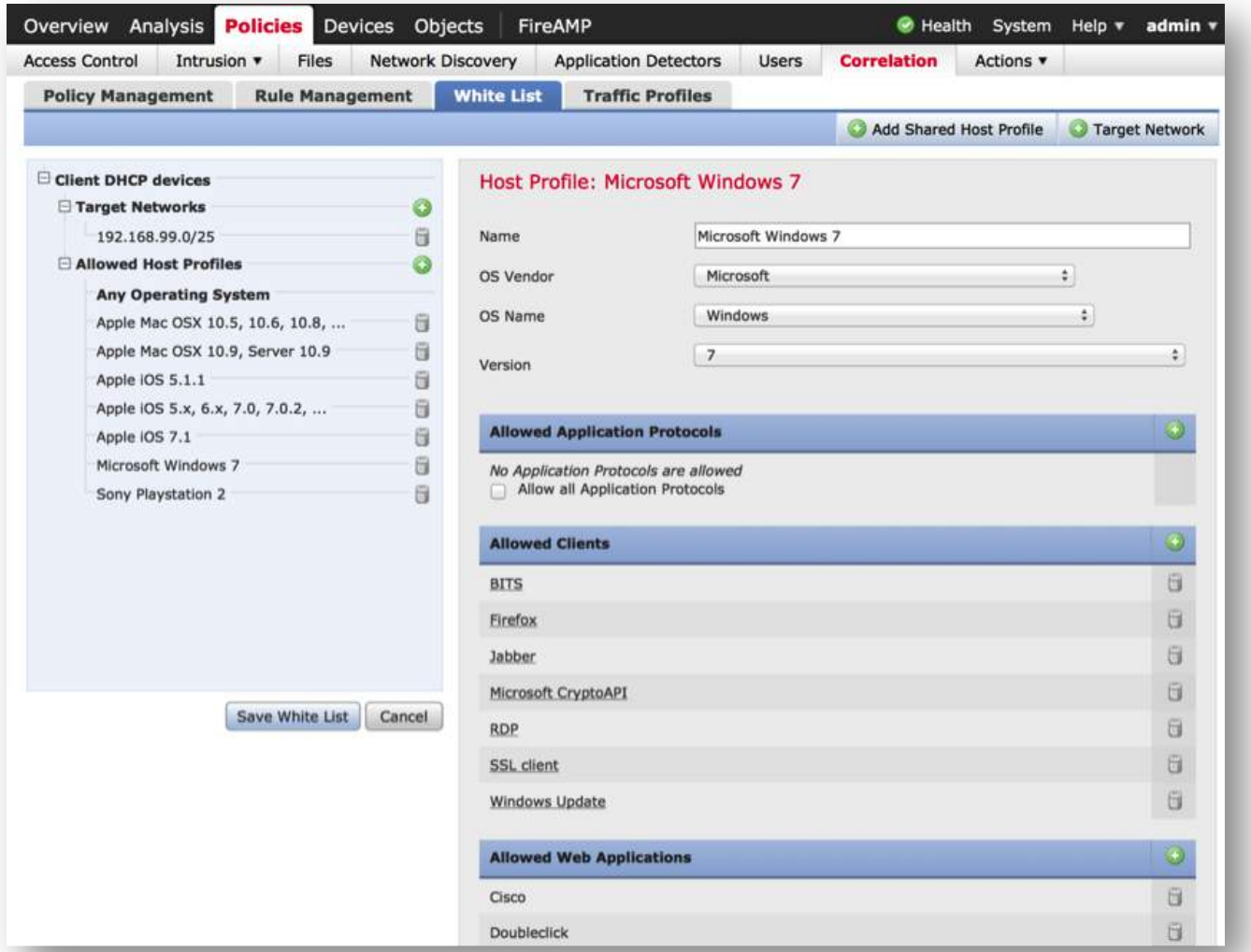




© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

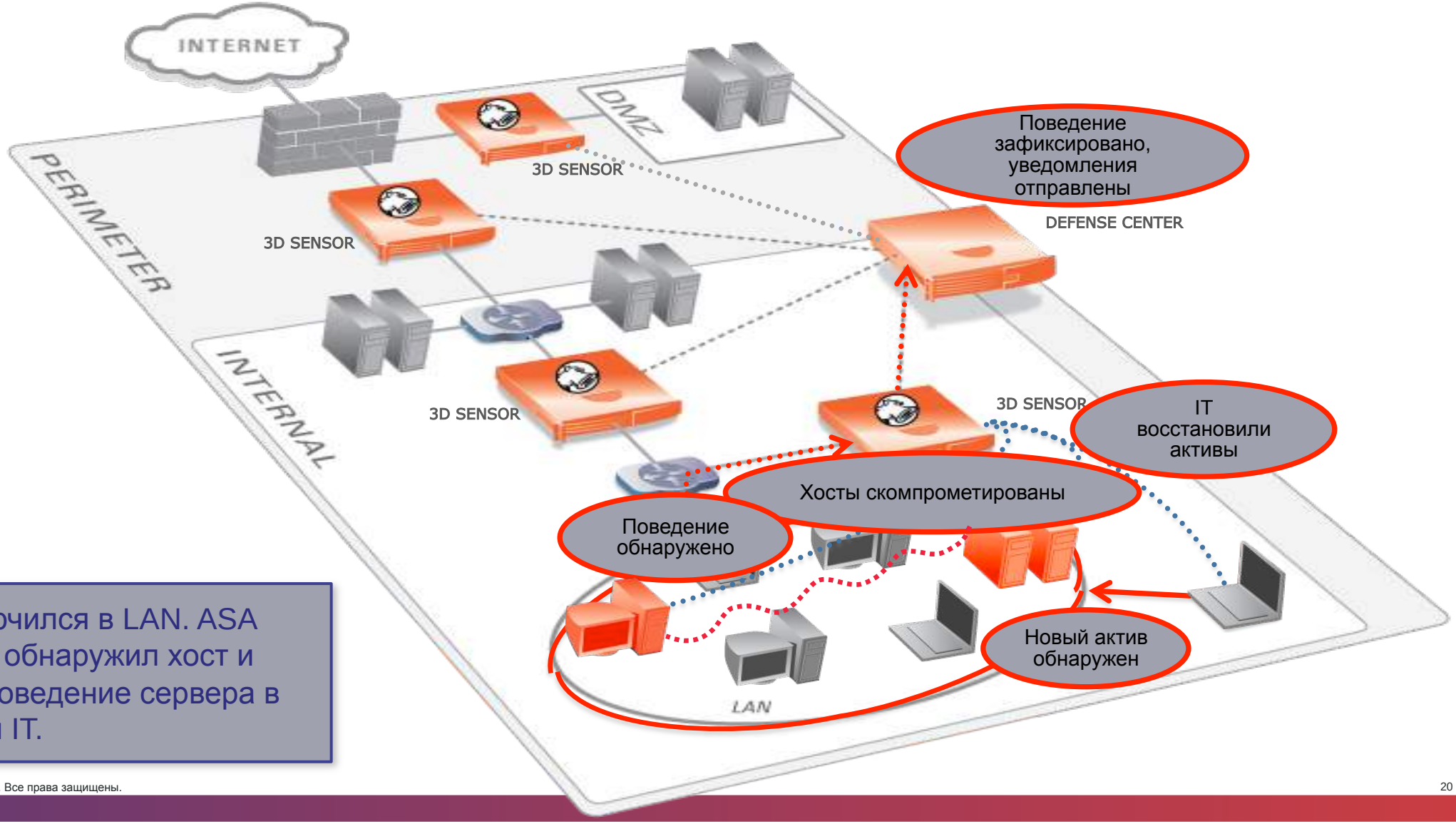
Создание «белых списков» / «списков соответствия»

- Разрешенные типы и версии ОС
- Разрешенные клиентские приложения
- Разрешенные Web-приложения
- Разрешенные протоколы транспортного и сетевого уровней
- Разрешенные адреса / диапазоны адресов
- И т.д.



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Обнаружение посторонних / аномалий / несоответствий



Новый хост включился в LAN. ASA with FirePOWER обнаружил хост и ненормальное поведение сервера в ЦОД и уведомил IT.

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Анализ происходящего на узлах

Кто на хосте

Идентифицированная операционная система и ее версия

Серверные приложения и их версия

Клиентские приложения

Версия клиентского приложения

Приложение

Какие еще системы / IP-адреса использует пользователь? Когда?

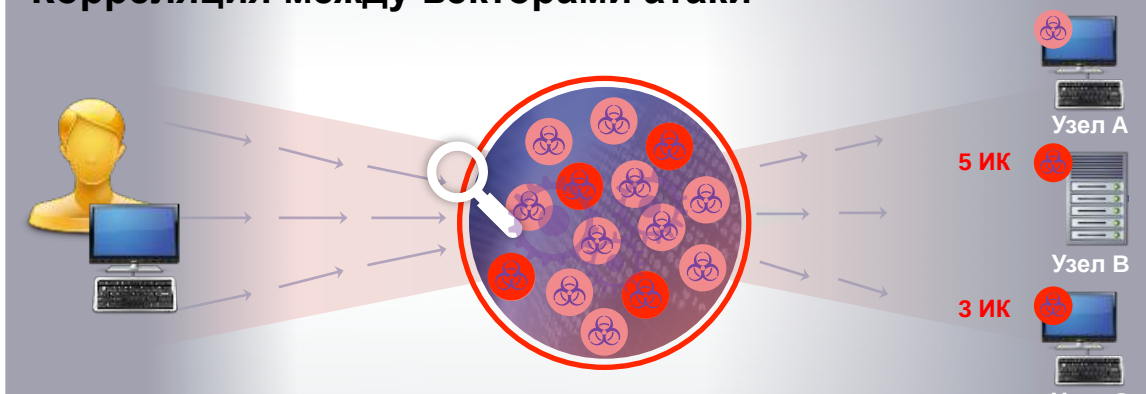
Автоматизированная, комплексная защита от угроз

Непревзойденная защита в течение всего жизненного цикла атаки

Корреляция между контекстом и угрозами

Оценка вредоносного воздействия

Корреляция между векторами атаки

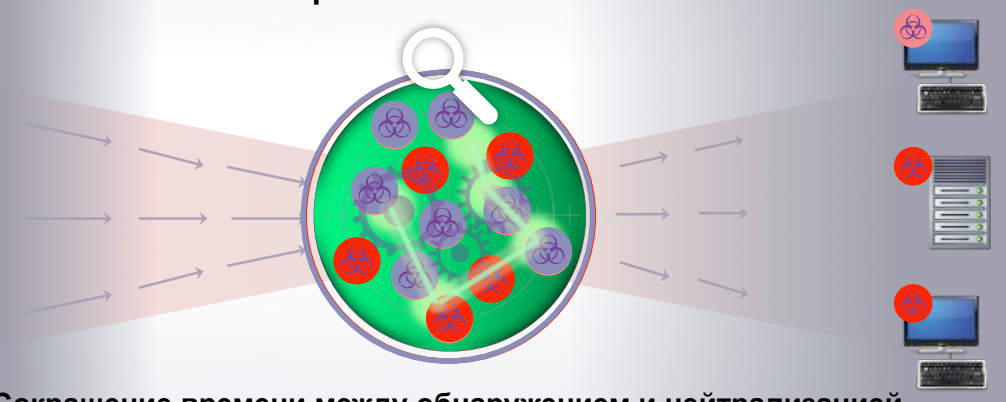


Раннее предупреждение о современных типах угроз

Динамические механизмы безопасности

Адаптация политик к рискам

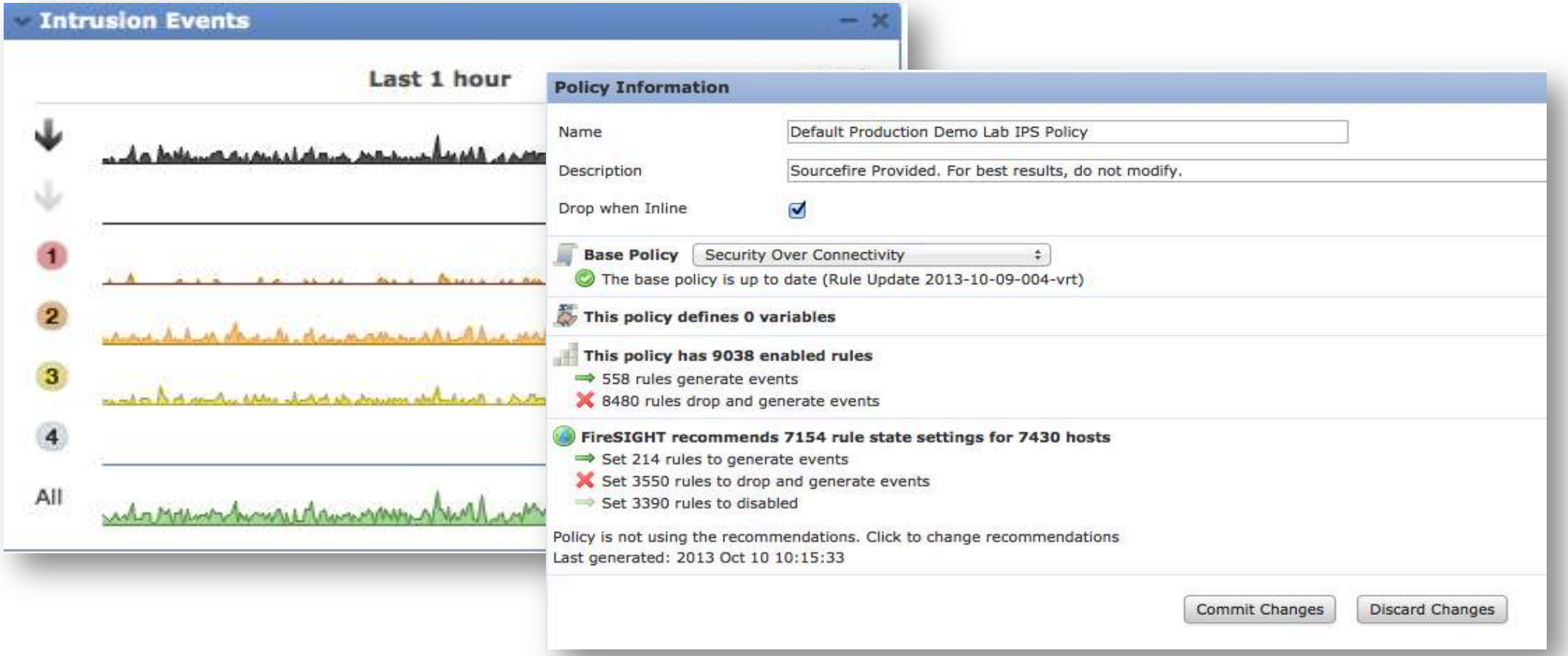
Ретроспективная защита



Сокращение времени между обнаружением и нейтрализацией

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

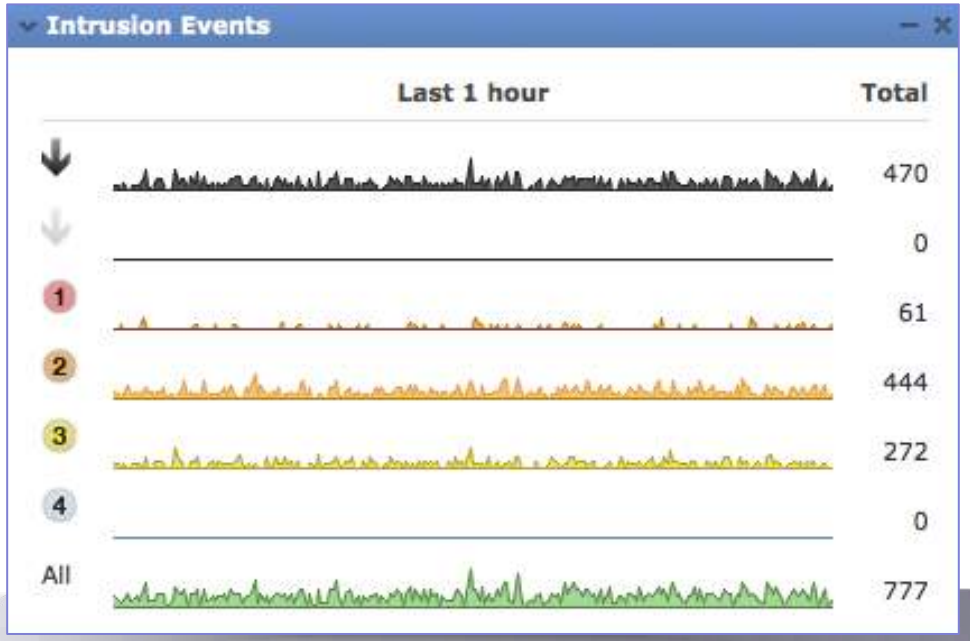
Автоматизация создания и настройки политик



Анализ сети, протоколов, приложений, сервисов, устройств, ОС, уязвимостей и др. позволяет автоматизировать создание политик и правил МСЭ и IPS

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Оценка вредоносного воздействия



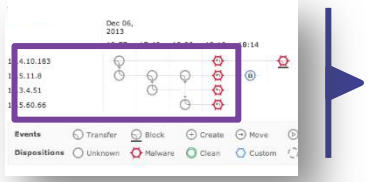
Каждому событию вторжения присваивается уровень воздействия атаки на объект

УРОВЕНЬ ВОЗДЕЙСТВИЯ	ДЕЙСТВИЯ АДМИНИСТРАТОРА	ПРИЧИНЫ
1	Немедленно принять меры, опасность	Событие соответствует уязвимости, существующей на данном узле
2	Провести расследование, потенциальная опасность	Открыт соответствующий порт или используется соответствующий протокол, но уязвимости отсутствуют
3	Принять к сведению, опасности пока нет	Соответствующий порт закрыт, протокол не используется
4	Принять к сведению, неизвестный объект	Неизвестный узел в наблюдаемой сети
0	Принять к сведению, неизвестная сеть	Сеть, за которой не ведется наблюдение

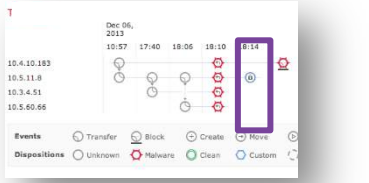
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Анализ траектории движения вредоносных программ

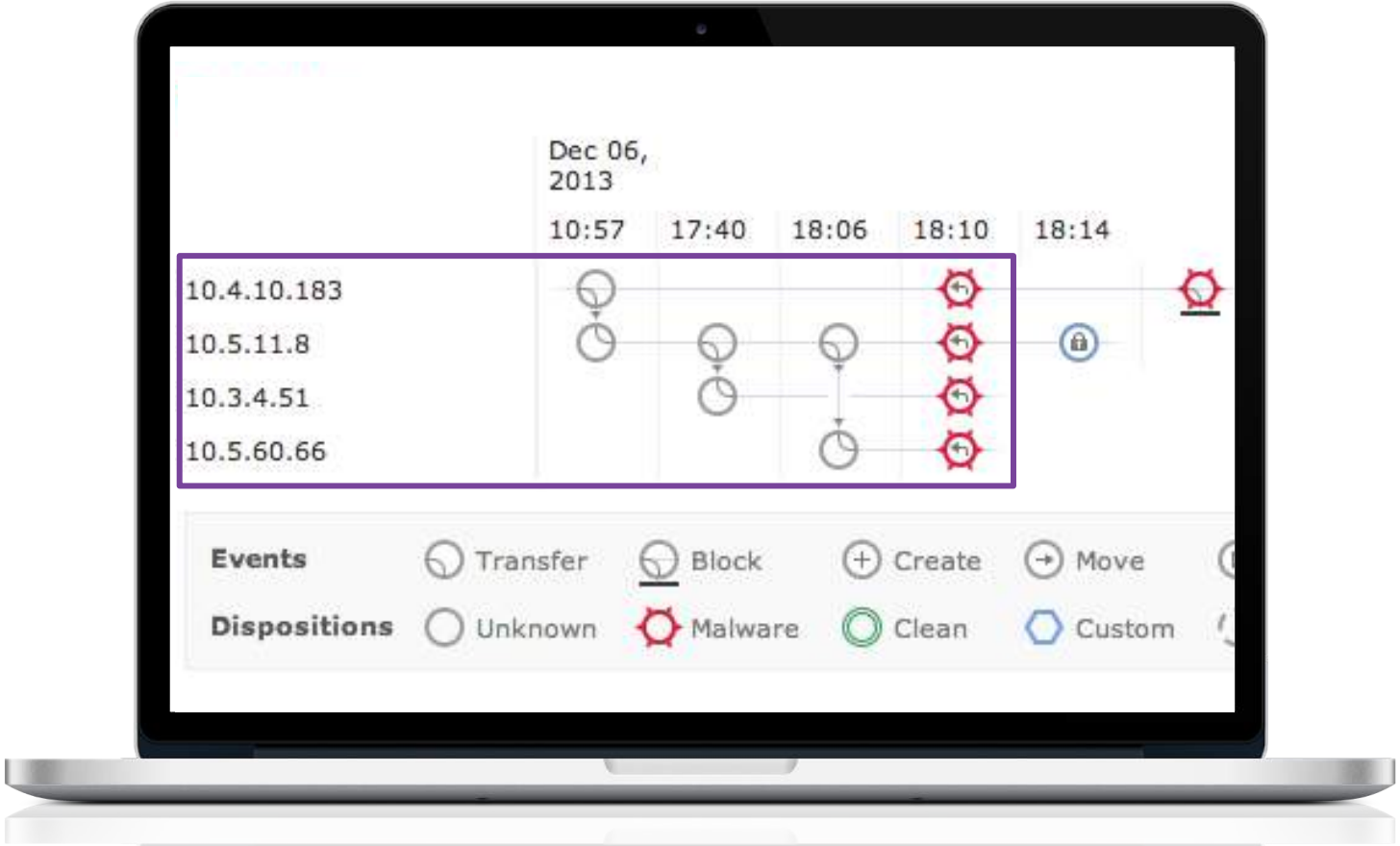
Сеть



Endpoint



Контент



- Сетевая платформа использует индикаторы компрометации, анализ файлов и траекторию движения файла для того, чтобы показать, как вредоносный файл перемещается по сети, откуда он появился, что стало причиной его появления и кто еще пострадал от него

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Обнаружение вредоносного кода с помощью AMP

Фильтрация по репутации

Поведенческое обнаружение

Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Признаки компрометации

Динамический анализ

Расширенная аналитика

Сопоставление потоков устройств

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Обнаружение известного вредоносного кода

Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help ▾ | dcloud ▾

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Malware Events | Hosts ▾ | Users ▾ | Vulnerabilities ▾ | Correlation ▾ | Custom ▾

	Bocinex.exe	4c136a95...271b4828	MSEXE	2
W32.Trojan.Breach.VRT	skunk-straddling.pdf	f02e1bb1...3b483a04	PDF	1
W32.Trojan.Breach.VRT	repair-cadets.pdf	f02e1bb1...3b483a04	PDF	1
W32.Trojan.Breach.VRT	ankles-bushiest.pdf	f02e1bb1...3b483a04	PDF	1
W32.Spy:Malwaregen.17db.1201	Weelsof.exe	e32ecc71...881078ce	MSEXE	1
W32.Spy:Malwaregen.17db.1201	IRCBot.exe	e32ecc71...881078ce	MSEXE	1
W32.Spy:Malwaregen.17db.1201	InternetAntivirus.exe	e32ecc71...881078ce	MSEXE	1
W32.Spy:Malwaregen.17db.1201	Dofoil.exe	e32ecc71...881078ce	MSEXE	1
W32.Banker:Spy.16hi.1201	Korgo.exe	b73b0e49...b67c4049	MSEXE	1
W32.Banker:Spy.16hi.1201	Hacker_Defender.exe	b73b0e49...b67c4049	MSEXE	1
W32.8BBFF65DB8-100.SBX.VIOC	Helompy.exe	8bbff65d...75dc60d6	MSEXE	1
W32.8BBFF65DB8-100.SBX.VIOC	Bofra.exe	8bbff65d...75dc60d6	MSEXE	1
W32.7FF810938B-100.SBX.VIOC	Pramro.exe	7ff81093...293edc5c	MSEXE	1
W32.7FF810938B-100.SBX.VIOC	Oficla.exe	7ff81093...293edc5c	MSEXE	1
W32.7FF810938B-100.SBX.VIOC	Dishigy.exe	7ff81093...293edc5c	MSEXE	1
W32.7FF810938B-100.SBX.VIOC	Conhook.exe	7ff81093...293edc5c	MSEXE	1
W32.7AF5A19B73-100.SBX.VIOC	Sefnit.exe	7af5a19b...5b44869b	MSEXE	1

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Полная информация о вредоносном коде

SOURCEfire

10 installs
0 detections (7 days)

Support ? Help Logout

Dashboard Analysis Outbreak Control Reports Management Accounts

Device Trajectory for **Alex-PC**

TIMEZONE **UTC**

23 Mar 29
13:22 17:06

Mar 30
13:10 13:25 13:49 14:16

14:17 14:18 15:11 15:26 15:29

[System]
[PE]
[PE]
.rar
keygen.exe [PE]
....exe [PE]
keygen.exe [PE]
....exe [PE]
....exe [PE]
tar.bz2
keygen.exe [PE]
exe [PE]
exe [PE]
06P5F2DM
16LN5RMT
8LNCRY5Z
57QW9BPG
ABHN2D1G
CLD0NH0T
B8KZ6WBZ
FSGQXVC5
ED4FZUUQ
JRY0SXO5
IDR_HTML_SCANNING[1]
N1HHOB7A
MNX9O4K6

Detected W32.Variant:BL.17et.1201 as **setup6.exe** (0a28fce..b5a858) [PE Executable] .

Moved by **Launcher_i502752981.exe**, 1.1.2.41 (733269a..77e8ac) [PE Executable] executing as Alex@Alex-PC.

Downloaded from http://**downloads.doubleoptmedia.com/setup6.exe**.

The file was not quarantined. It was moved or deleted before it could be quarantined.

At 17:06:54, Sat Mar 29 2014 UTC [less details]

File full path: C:\Users\[redacted]\AppData\Local\Temp\setup6.exe

File SHA-1: 0f08be1974b52b9899a5c0176f63cf4fd5f9bd06.

File MD5: ffcf0bc8b030f6807847554ac652d239.

File size: 68752 bytes.

File signed by M/s Children Code with certificate serial 355cdfd525f643928f3a5700d87f0799 from COMODO Code Signing CA 2. Expires 23:59:59, Tue Feb 10 2015 UTC. The certificate was trusted by the computer.

File cert MD5: f28a9d85fbd75c991c36100435a695a9.

File cert SHA-1: 11526192e45421c3361585449e41a415e0a81b0a.

Parent file SHA-1: b61c213b52f11ebb6f4ed5b6759c57e70095a290.

Parent file MD5: 1b9fdc9a68f4ea67ffb456d1285571cd.

Parent file size: 338432 bytes.

Parent process id: 1800.

Parent process SID: S-1-5-21-2126426059-4290411445-2997762626-1000.

Detected by the SHA SPERO engines

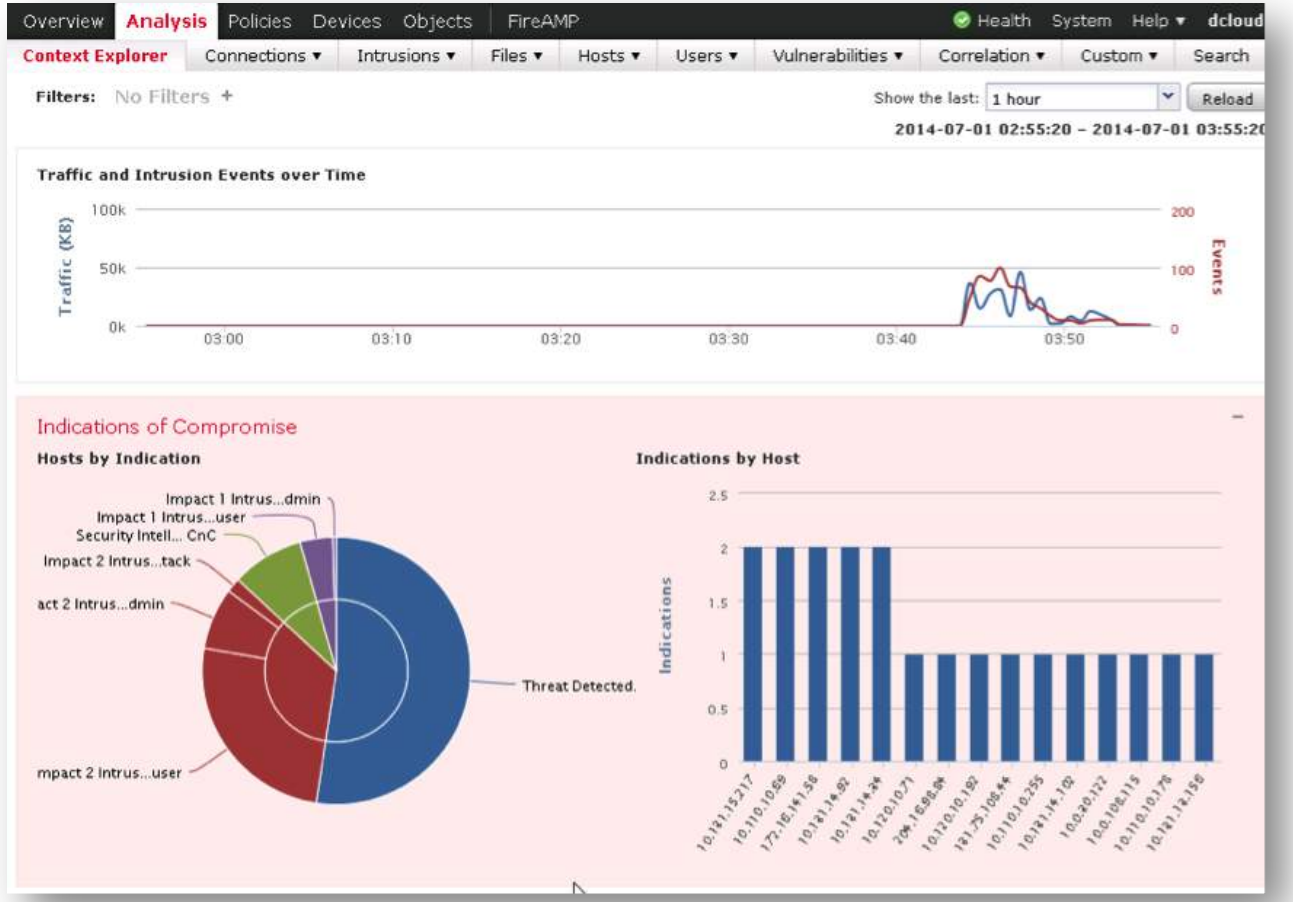
TIME: Feb 23 13:30 — May 16 12:15

EVENT TYPE: create, copy, move, execute, open, connection, scan detection, exec block, compromised?, restore, reboot, scan, defs update, policy update, connector update, scan schedule, uninstall

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

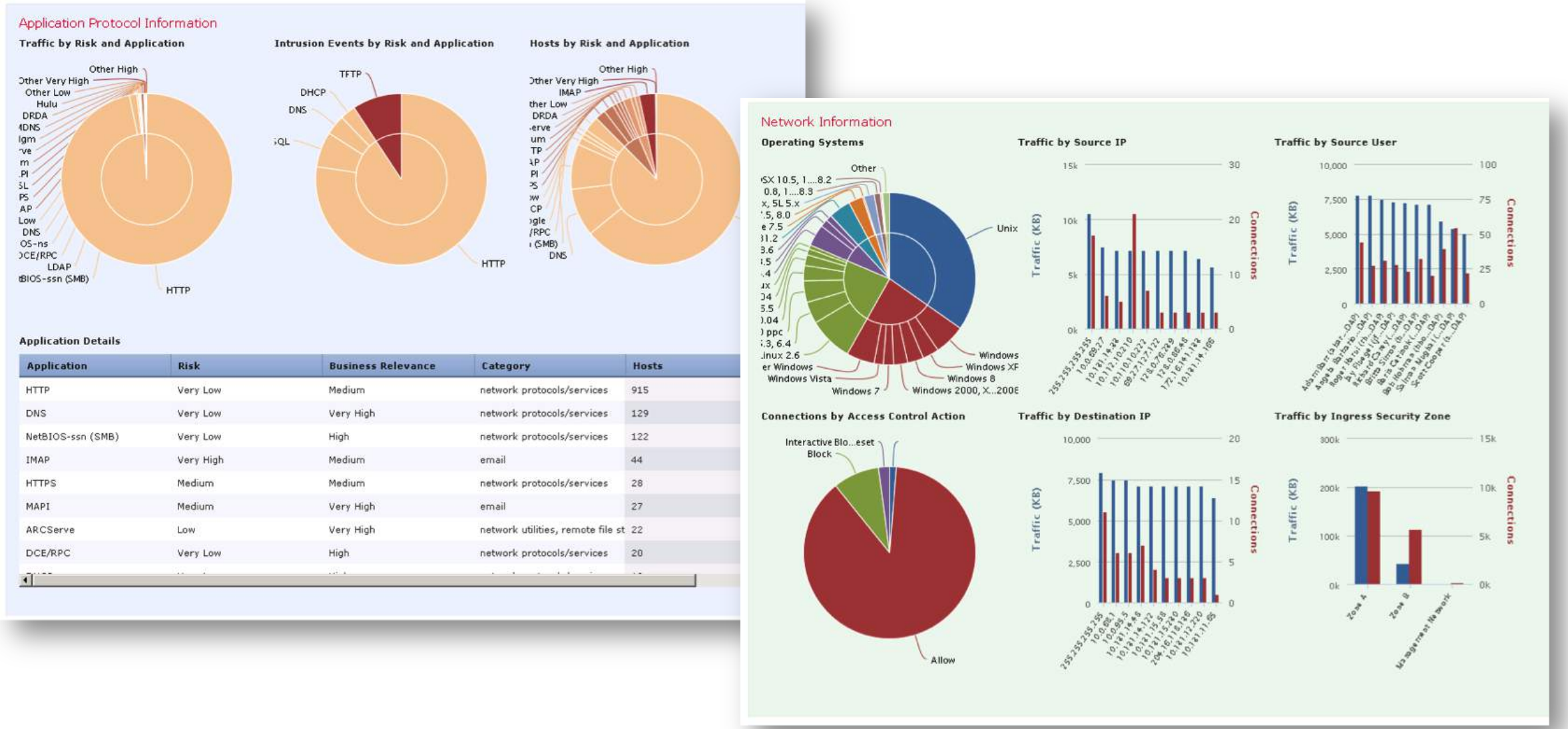
Мониторинг общей информации о сети

- Корреляция событий безопасности, трафика и вредоносного кода
- Активность конкретных пользователей и их приложений
- Используемые ОС и активность сетевого обмена
- Оценка событий по уровню воздействия и приоритета
- Статистика по вредоносному коду и зараженным файлам
- Геолокационные данные
- Категории сайтов и посещаемые URL



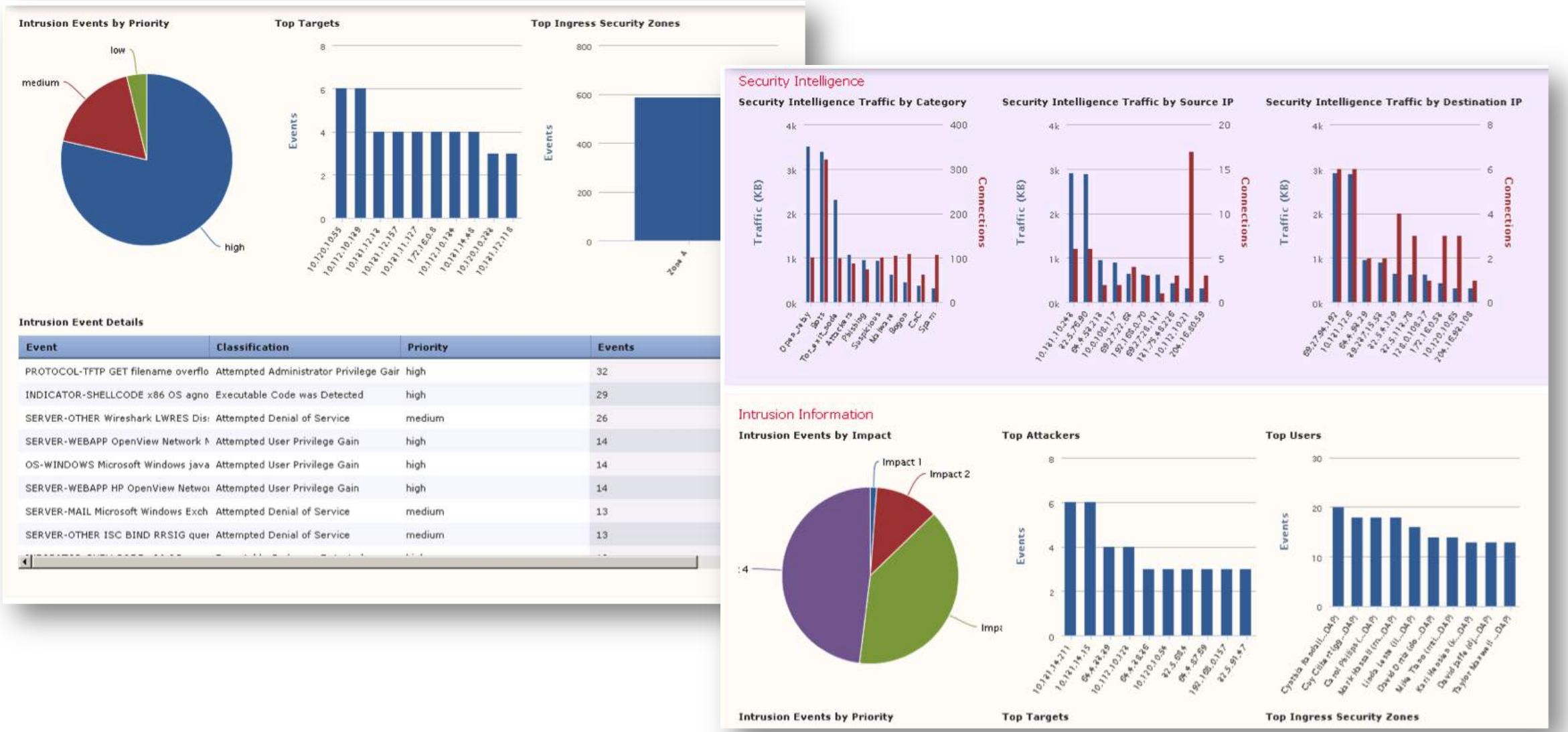
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Мониторинг общей информации о сети



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Мониторинг общей информации о сети



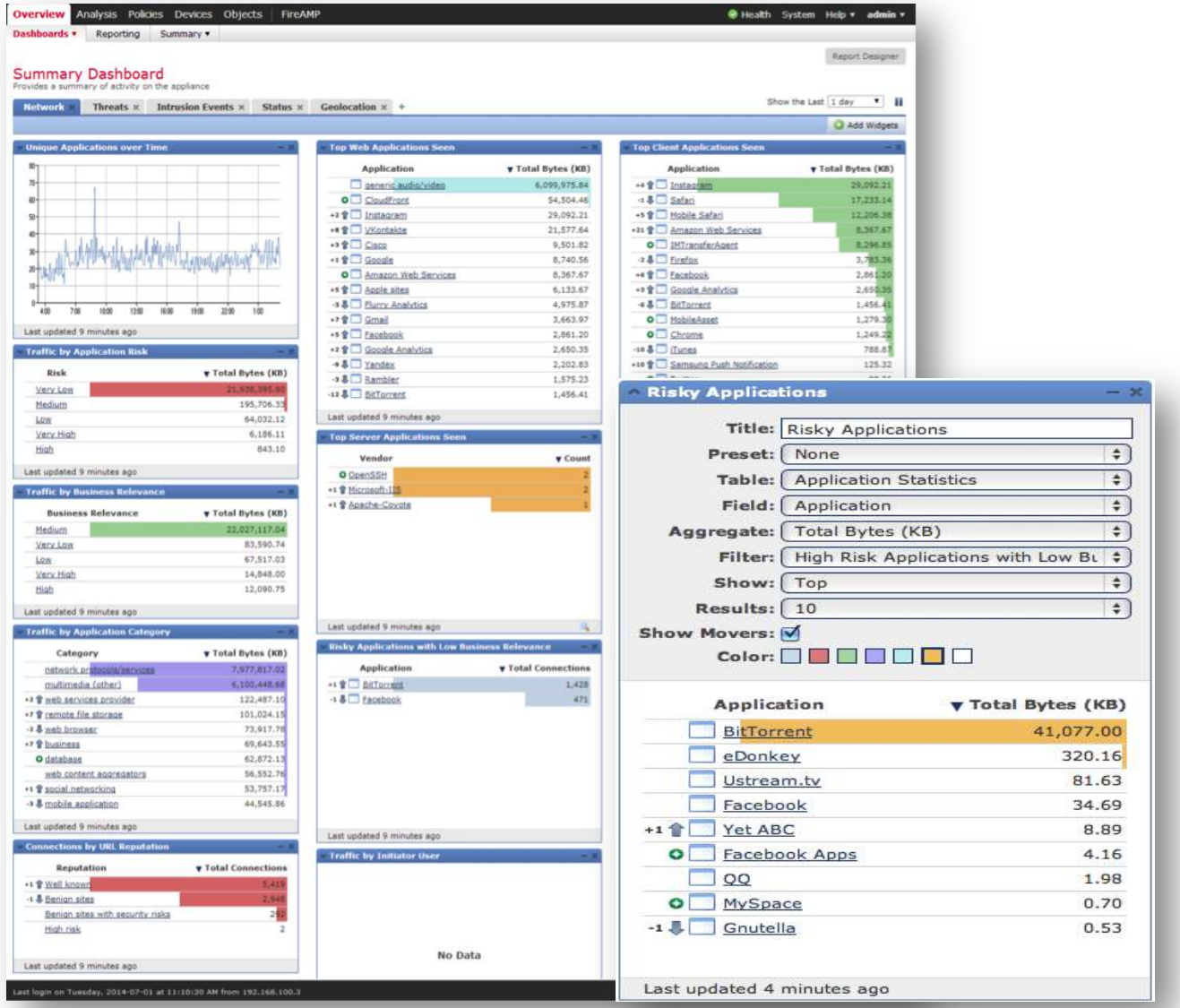
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Мониторинг общей информации о сети

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Мониторинг сетевых событий

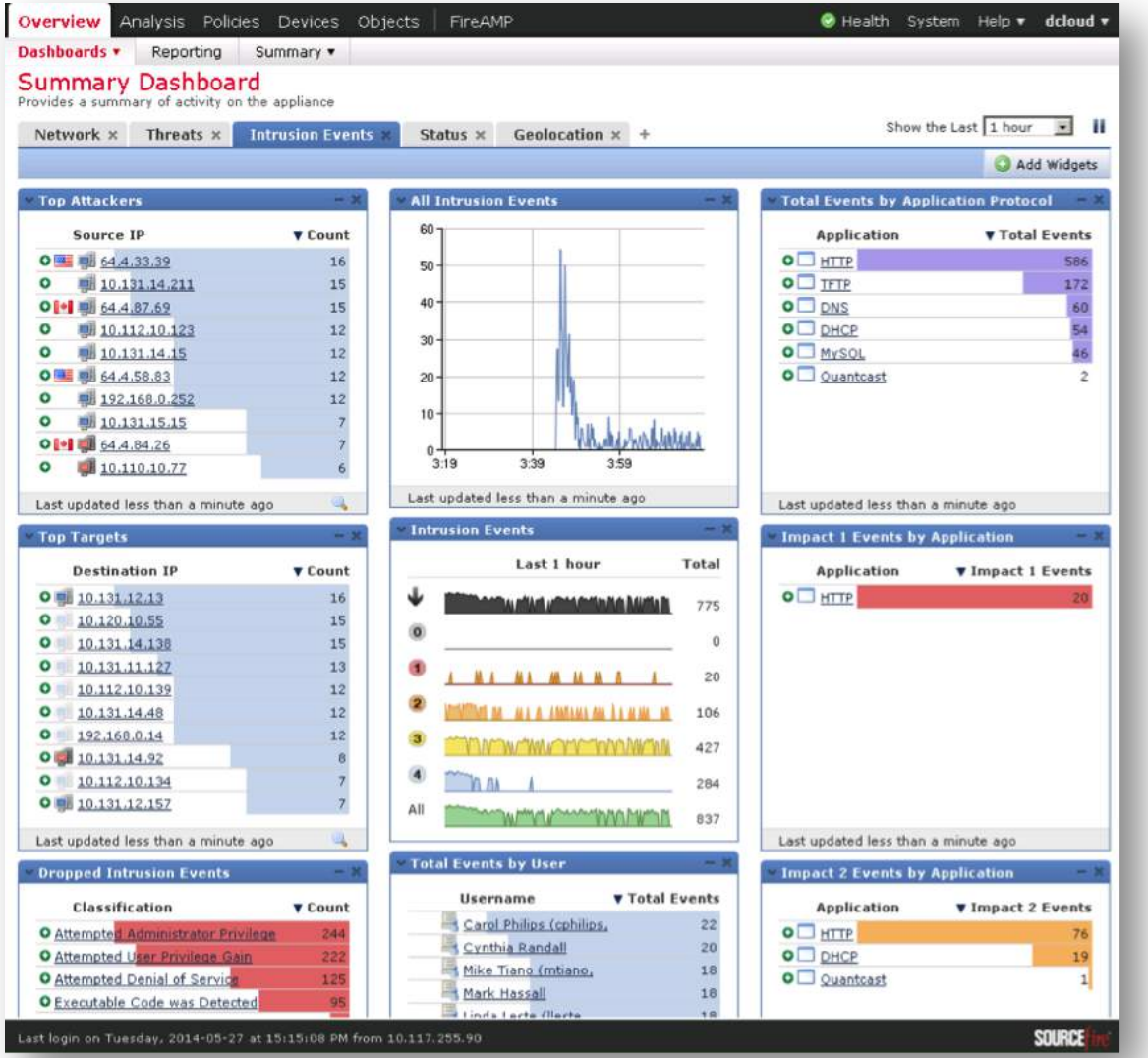
- Использование сервисов
- Использование приложений
- Использование операционных систем
- Распределение соединений
- Активность пользователей
- Уязвимые узлы и приложения
- И т.д.



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Мониторинг событий безопасности

- Основные нарушители
- Основные атаки
- Заблокированные атаки
- Основные цели
- Приоритет событий
- Уровень воздействия



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

ASA with FirePOWER объединяет все вместе

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Объединяя все вместе, ASA with FirePOWER

Объем и контрольные точки

- Эл. почта
- Оконечные устройства
- Интернет
- Сеть
- Система предотвращения вторжений IPS
- Устройства

Поток телеметрических данных

- Идентифицирующие метки и метаданные файла
- Файловый и сетевой ввод/вывод
- Информация о процессе

Непрерывная передача

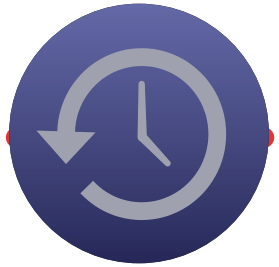
0111010011101 1100001110001110 1001 1101 1110011 011001
1110 1001 1101 1110011 0110011 101000 0110 00 011100
100001 1100 0111010011101 1100001110001110 1001 1101

Непрерывный анализ

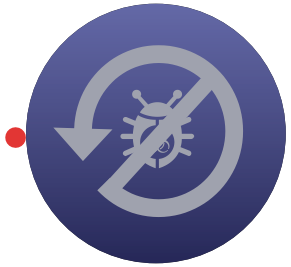
© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

…позволяет непрерывно анализировать широкий спектр угроз и реагировать на них…

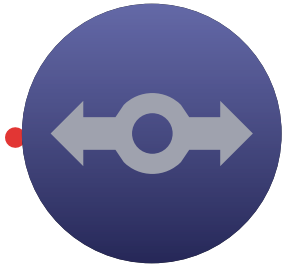
Повышенные уровни обнаружения, отслеживания и реагирования



Анализ пост-фактум

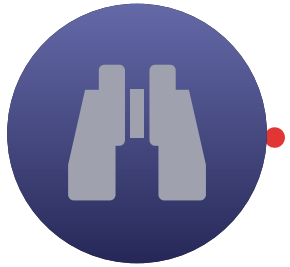


Ретроспективное обнаружение



Поведенческие признаки вторжения

Траектория



Поиск угроз

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

… что дает уверенность и контроль того, откуда именно следует начать

Кто

Сфокусируйтесь сначала на этих пользователях

Что

Эти приложения пострадали

Где

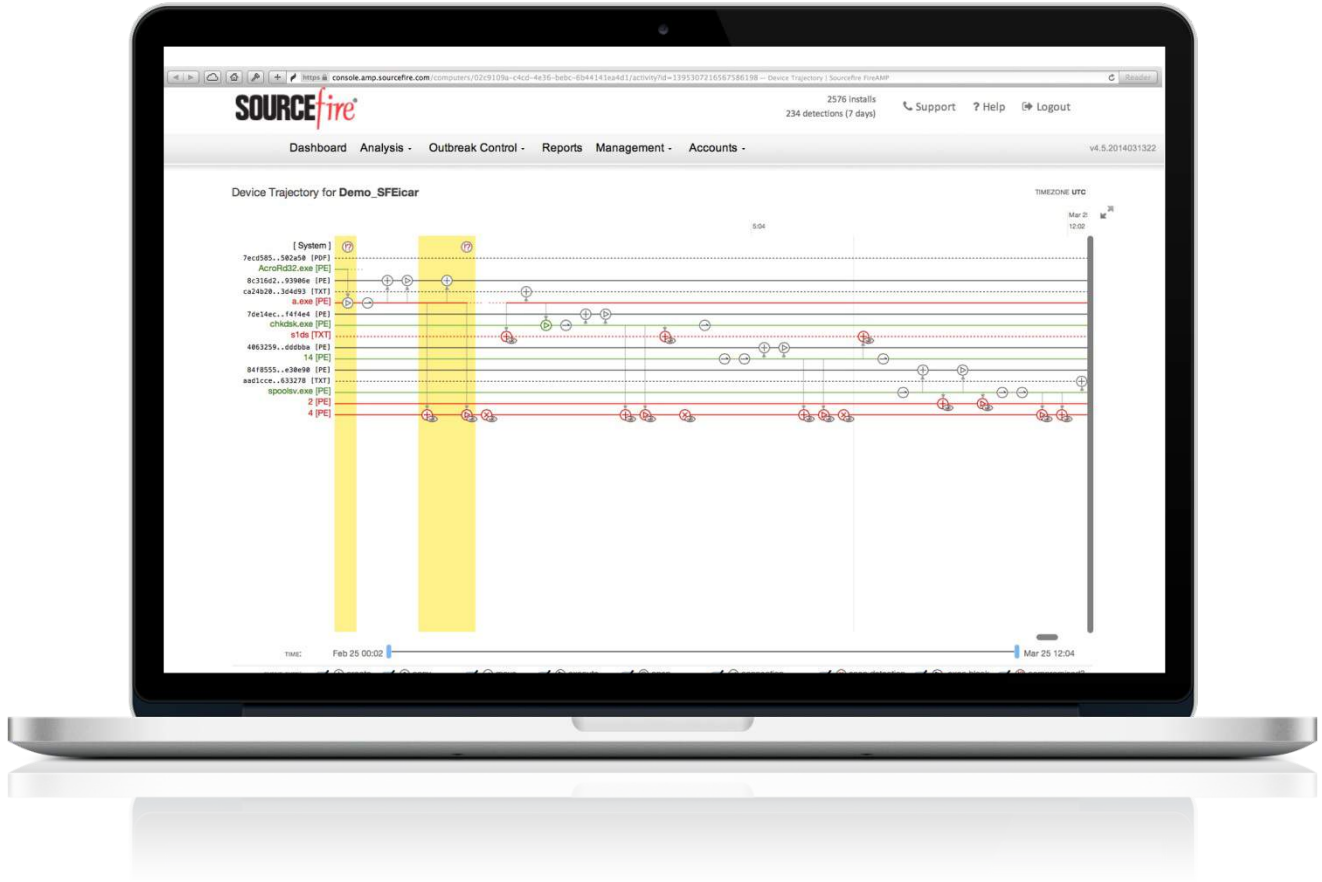
Взлом затронул эти области сети

Когда

Такова картина атака с течением времени

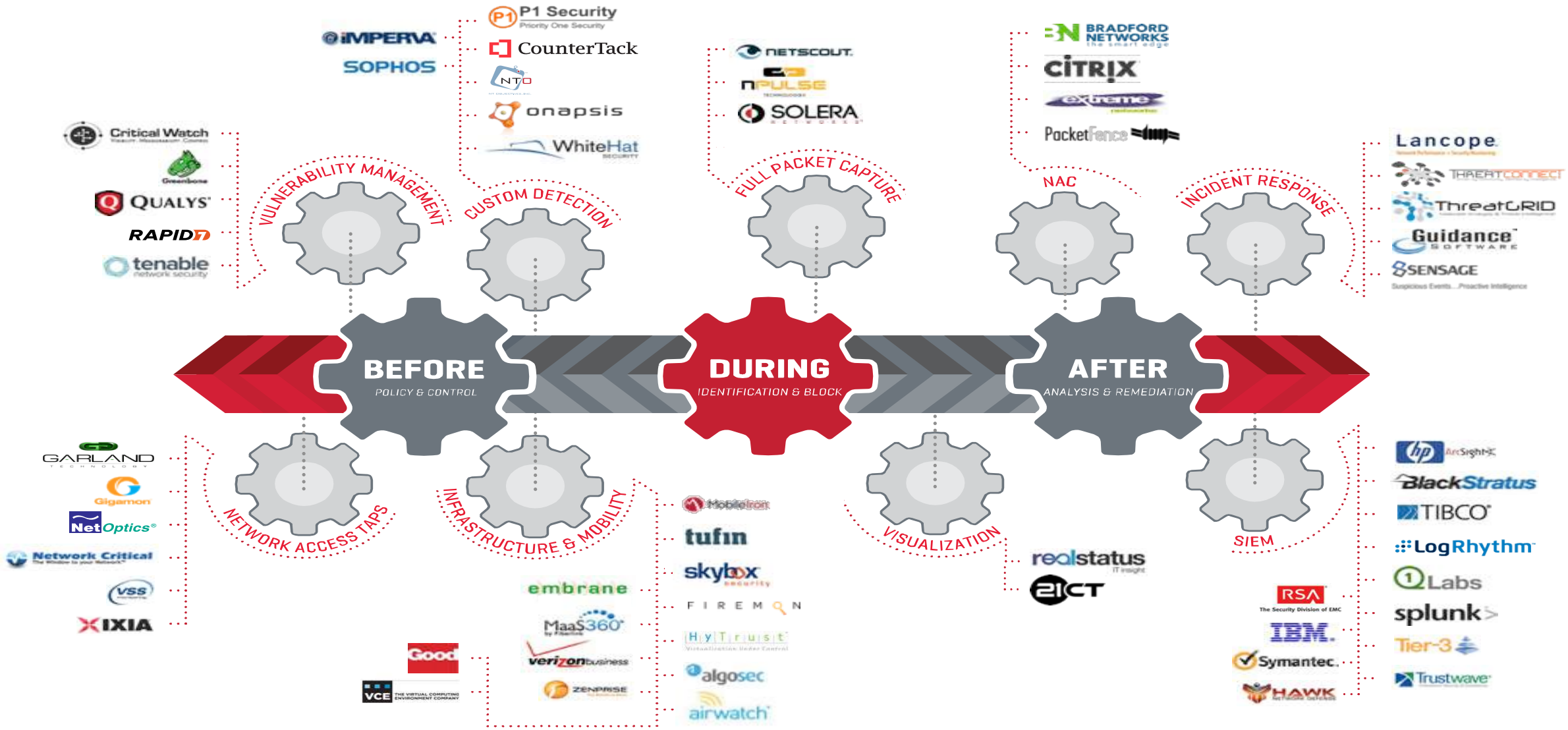
Как

Это источник угрозы и путь ее распространения



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Экосистема Cisco ASA with FirePOWER



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

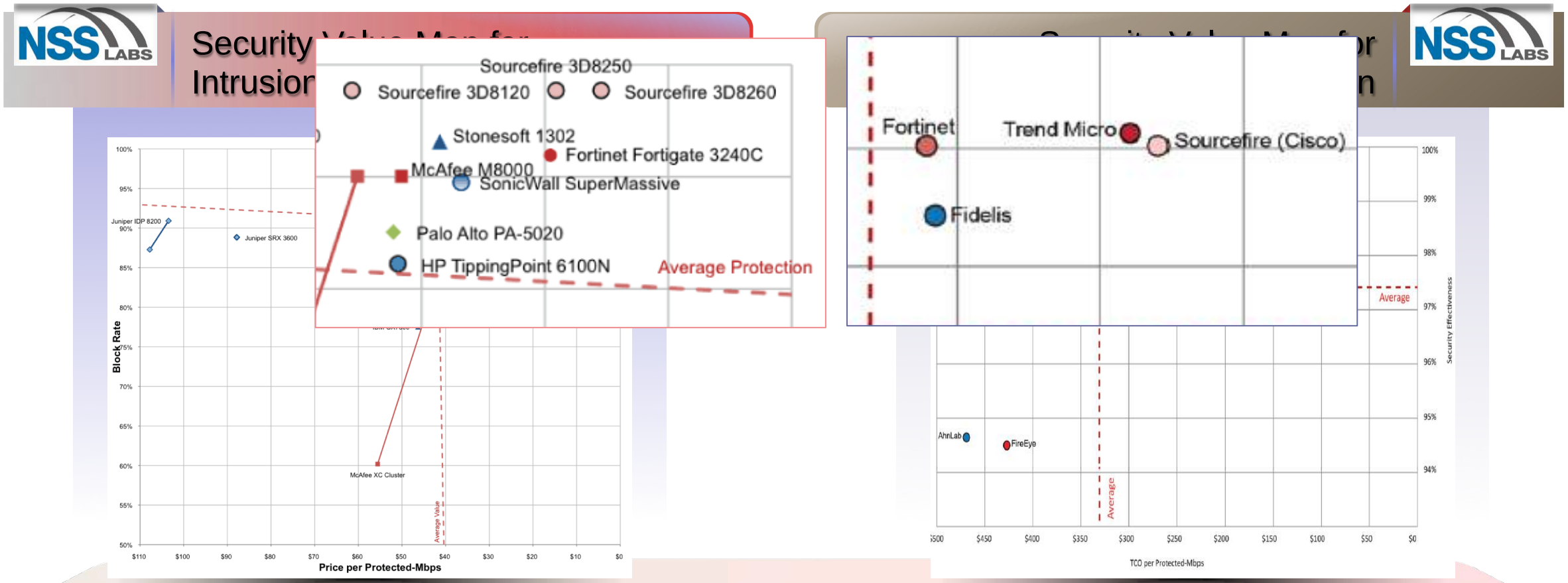
Сравнение Cisco ASA с функциями FirePOWER и прежних МСЭ нового поколения

Возможности	Cisco ASA с функциями FirePOWER	Прежние МСЭ нового поколения
Упреждающая защита на основе репутации	**На высшем уровне**	Не имеется
Автоматизация мониторинга, учета контекста и интеллектуальной безопасности	**На высшем уровне**	Не имеется
Репутация файлов, отслеживание активности файлов, ретроспективный анализ	**На высшем уровне**	Не имеется
Индикаторы компрометации	**На высшем уровне**	Не имеется
СОВ нового поколения	**На высшем уровне**	**Имеется**[1]
Мониторинг и контроль приложений	**На высшем уровне**	**Имеется**
Политика допустимого применения/Фильтрация URL-адресов	**На высшем уровне**	**Имеется**
Удаленный доступ по VPN	**На высшем уровне**	Не на уровне предприятия
Межсетевое экранирование с отслеживанием состояния, высокая доступность, кластеризация	**На высшем уровне**	**Имеется**[2]

1- Обычно для 1-го поколения СОВ. 2 - Возможности высокой доступности зависят от производителя МСЭ нового поколения

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Лучшая эффективность защиты



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Подтверждение качества защиты

NGIPS—Perimeter

NEW! NGFW 2014

	Cisco FirePOWER 8350	Cisco ASA with FirePOWER Services (5525-X)	Cisco ASA with FirePOWER Services (5585-X)	Fortinet FortiGate	Check Point
Security Effectiveness	Highest % Tested	Highest % Tested	Highest % Tested		
Real World Throughput	Better than claim and others	Better than claim and others	Better than claim and others		
Evasion Resistance	100%	100%	100%		
Management	Superior	Superior	Superior		
TCO (per Mbps Protected)	Lowest	Lowest	Lowest		

	Cisco Sourcefire FirePOWER 8260	Fortinet FortiGate 3240C	Check Point 12600	McAfee NSP M-8000	Dell SonicWALL SuperMassive	Palo Alto Networks PA-5020	HP Security TP-6100N	Stonesoft IPS-1302	Juniper SRX 3600	IBM Security GX7800
Protection	98.90%	96%	98.3%	95%	94.8%	92.5%	91.1%	96.6%	88.8%	77.5 %
Real World IPS Throughput	34Gbps (20 Gbps)	6.3 Gbps (8 Gbps)	2.7 Gbps (6 Gbps)	12.3 Gbps	16.3 Gbps	2.3 Gbps (5 Gbps)	10 Gbps (8 Gbps)	2.3 Gbps (2 Gbps)	3.7 Gbps (10 Gbps)	11.4 Gbps
Concurrent Connections	60M	5.5 M	1							
TCO (per Mbps Protected)	$15	$19								

Breach Detection (AMP)

	Cisco Sourcefire Advanced Malware Protection (AMP)	Fortinet FortiSandbox 3000D	FireEye Web MPS 4310 / Email MPS 5300	Trend Micro Deep Discovery Inspector 1000	Fidelis XPS Direct 1000	AhnLab MDS
Protection	99.0%	99.0%	94.5%	99.1%	98.4%	94.7%
Real World Throughput	1Gbps	1 Gbps	667Mbps	1 Gbps	1 Gbps	1 Gbps
Stability / Reliability	100%	100%	100%	100%	100%	100%
Maximum TCP Connections/Second	15,000,000	14,000,000	5,500,00	15,000,000	11,000,000	3,750,000
TCO (per Mbps Protected)	$232	$309	$428	$240	$307	$469
New TCP Connections/second	225K	225K	25K	200K	50K	40K
Product Rating	Recommended	Recommended	Caution	Recommended	Recommended	Caution

	Cisco FirePOWER 8250/8290	Fortinet FortiGate 3600C	Check Point 12600	Dell SonicWALL SuperMassive
Security Effectiveness	97.7%	97.1%	98.5%	97.3%
Real World NGFW Throughput	13Gbps (10 Gbps) 52Gbps (40Gbps)	7.5 Gbps (14 Gbps)	4.2 Gbps (5 Gbps)	16.3 Gbps (20 Gbps)
TCP Conns/sec	1.17M	81.5K	53K	220K
TCO (per Mbps Protected)	$18	$22	$28	$27

NGFW 2013

	Cisco Sourcefire FirePOWER 8290-2			
Protection	99.4%	98.2%	86.3%	99.6%
Anti-Evasion	100%	100%	100%	100%
Real World IPS Throughput (claimed)	136Gbps (80 Gbps)	59.3 Gbps (120 Gbps)	31.6Gbps (40Gbps)	47.5 Gbps (40 Gbps)
Concurrent Connections	240M	120M	60M	44M
Connections per Second	2.1M	80K	18K	60K
TCO (per Mbps Protected)	$13.55	$39.02	$55.13	$11.94
New Connections/second (Real-world Traffic Mix)	160K	66K	40K	58K
Product Rating	Recommended	Neutral	Caution	Recommended

NGIPS – Data Center

NSS LABS

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Варианты исполнения Cisco ASA with FirePOWER

FirePOWER Services for 5500-X (ПО)

ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X

FirePOWER Services for 5585-X (модуль)

ASA 5585-X

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Модульная функциональность

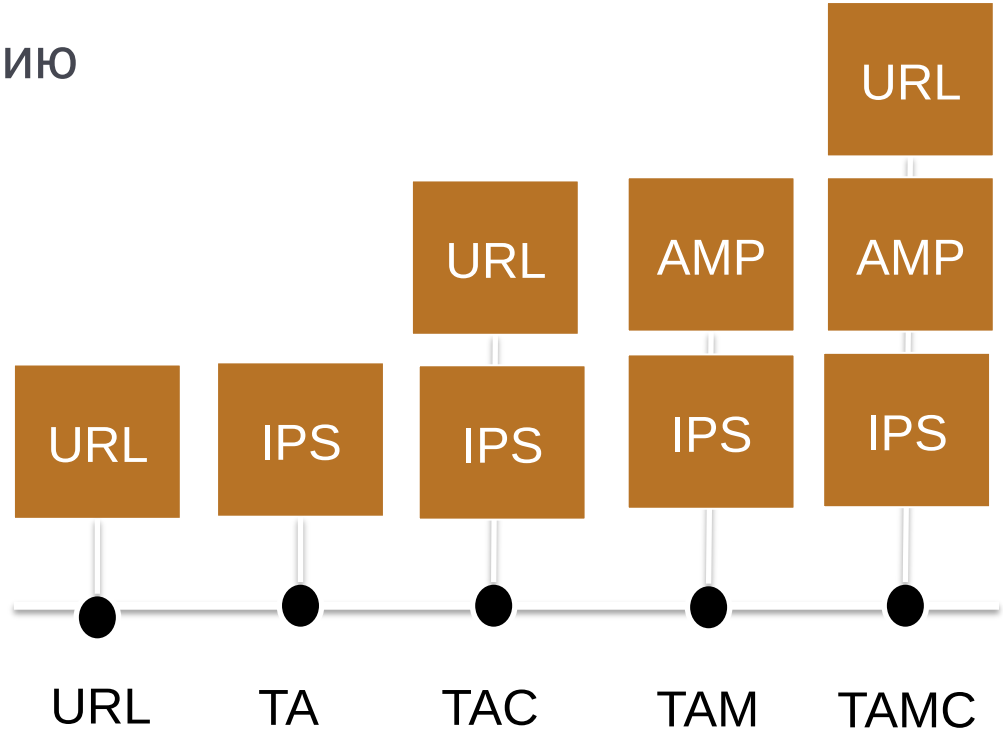
5 вариантов заказа защитных функций

Подписка на 1 или 3 года (включая обновления)

Функция AVC (NGFW) включена по умолчанию

- Активирует функции FirePOWER Services
- Постоянная и поставляется вместе с устройством

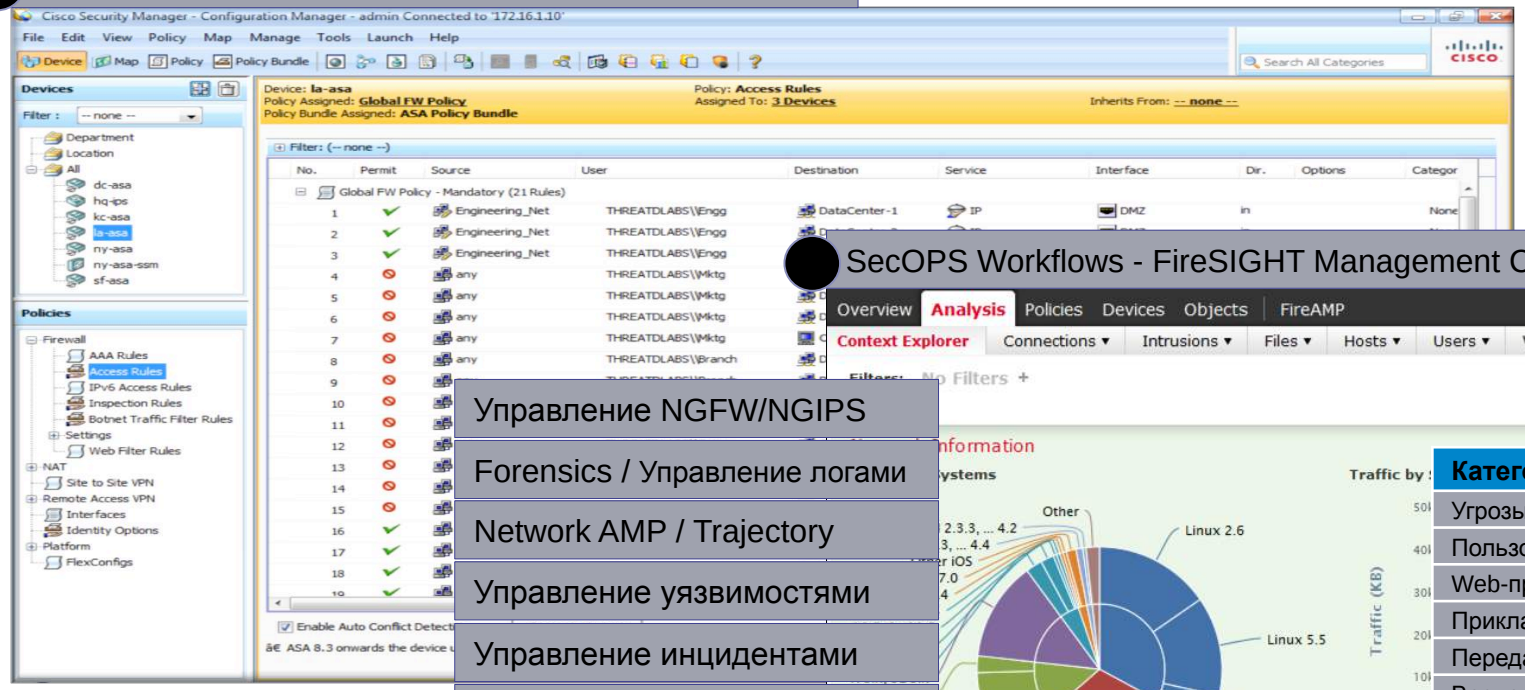
Обновления AVC включены в SMARTnet



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

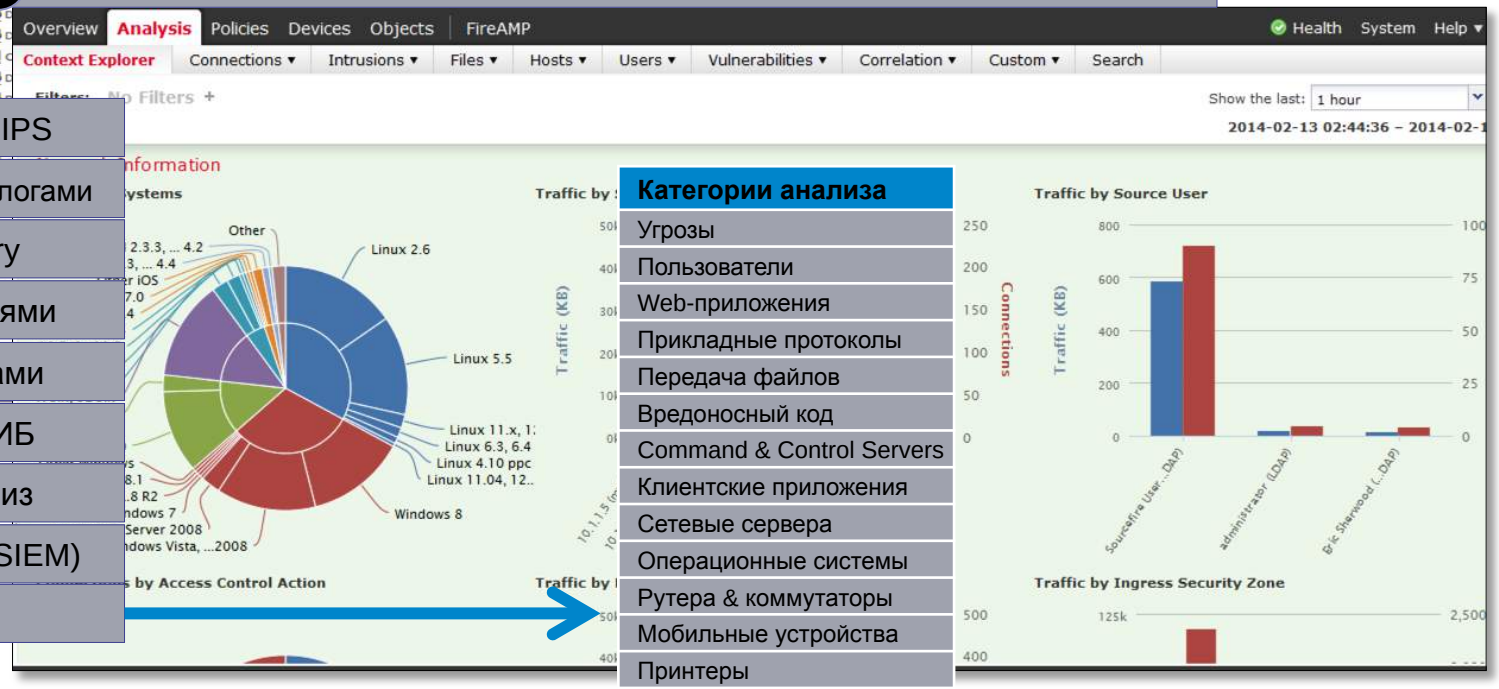
Управление Cisco Security

- NetOPS Workflows - CSM 4.6/7 или ASDM-ASA-On-Box



FireAMP Connector
(Managed by FMC)

- SecOPS Workflows - FireSIGHT Management Center



- Управление NGFW/NGIPS
- Forensics / Управление логами
- Network AMP / Trajectory
- Управление уязвимостями
- Управление инцидентами
- Адаптивная политика ИБ
- Ретроспективный анализ
- Корреляция событий (SIEM)
- Распознавание

Категории анализа

- Угрозы
- Пользователи
- Web-приложения
- Прикладные протоколы
- Передача файлов
- Вредоносный код
- Command & Control Servers
- Клиентские приложения
- Сетевые сервера
- Операционные системы
- Рутера & коммутаторы
- Мобильные устройства
- Принтеры
- VoIP-телефоны
- Виртуальные машины

© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Cisco ASA с функциями FirePOWER

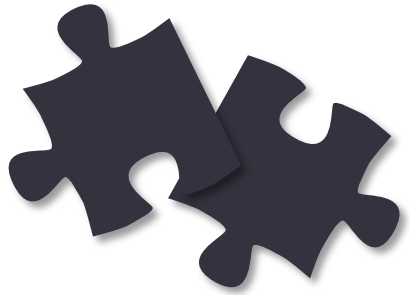
Первый в отрасли МСЭ нового поколения, смотрящий шире и глубже

Непревзойденная прозрачность

- Полная осведомленность о сетевом контексте для устранения уязвимостей

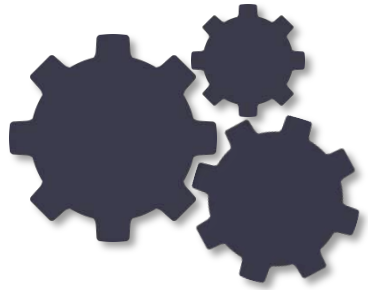
Комплексная защита от угроз

- Лучшая в своем классе многоуровневая защита в одном устройстве



Автоматизация

- Простота управления, динамическое реагирование и восстановление



© Cisco и(или) ее аффилированные лица, 2014 г. Все права защищены.

Благодарю за внимание

cisco