Построение архитектуры безопасности для предотвращения сложных целенаправленных атак

Руслан Барбашин, CyberSecurity Account Manager
Ruslans_Barbasins@mcafee.com

Обо мне

<u>Образование</u>

- Rigas Tehniska Universitate, Латвия
- University of Salford, Великобритания
- Sales Institute of Ireland, Ирландия

<u>Карьера:</u>

1995 – 2000 инженер телекоммуникаций
2000 – 2017 Проджект менеджер, BDM

2010 - McAfee Ireland Ltd. / Intel (Intel Security)

7 лет в сфере ИБ

https://www.linkedin.com/in/ruslansbarbasins/

Our Brand Promise

We believe that no one person, product, or organization alone can secure the digital world.

It's why we rebuilt McAfee around the idea of working together: People working together. Products working together. Organizations and industries working together.

We aim to inspire collaboration among our customers, partners—even our competitors—to make the connected world a safer place.

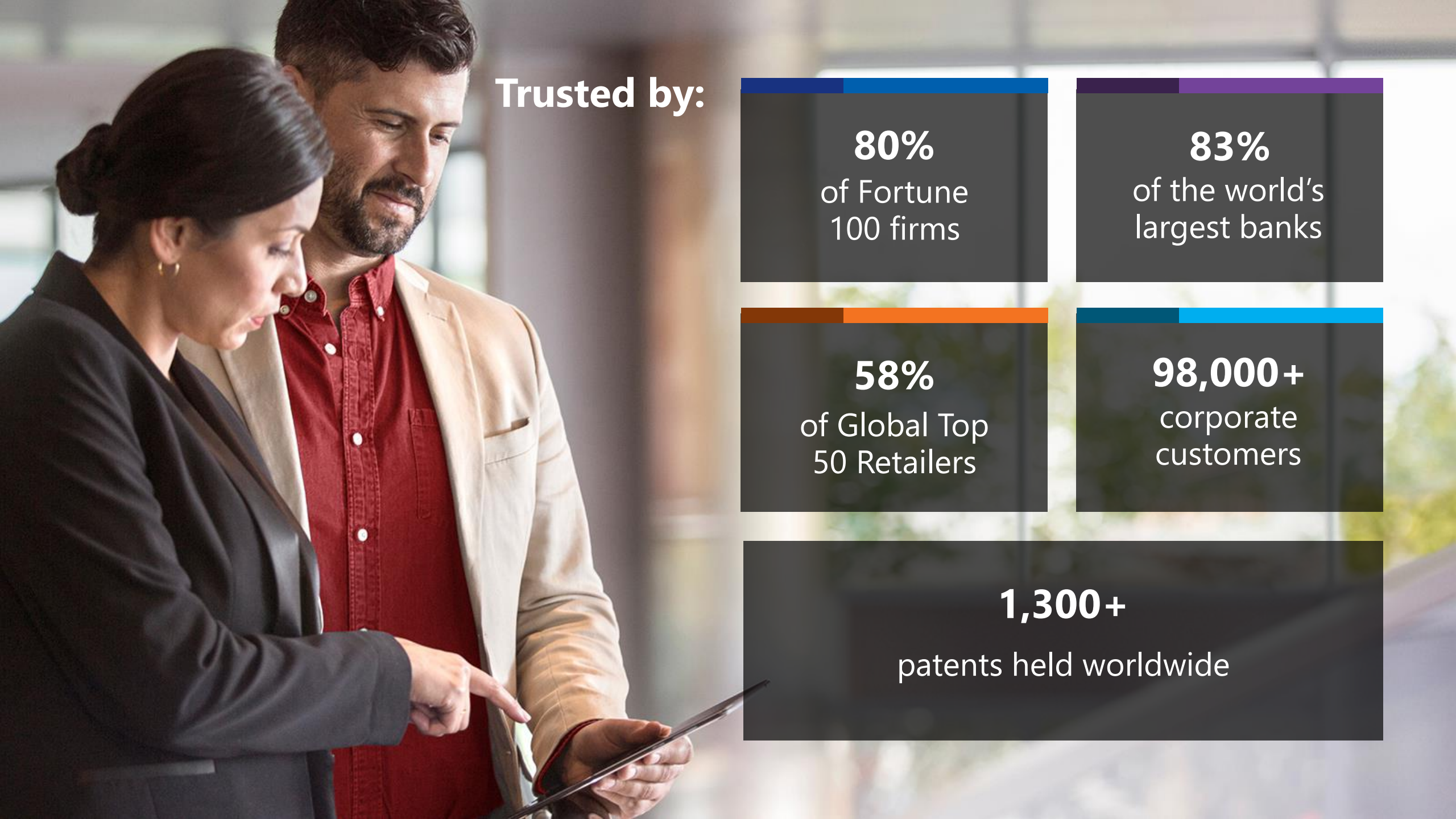
McAfee. Together is power.

McAfee. The device-to-cloud cybersecurity company.

- Open Ecosystem,
  Integrated Platform
- Modern Architecture
- Leading-edge Threat Security

The best of all cybersecurity worlds.
All on one leading-edge platform.

McAfee. The device-to-cloud cybersecurity company.



Trusted by:

80%
of Fortune 100 firms

83%
of the world's largest banks

58%
of Global Top 50 Retailers

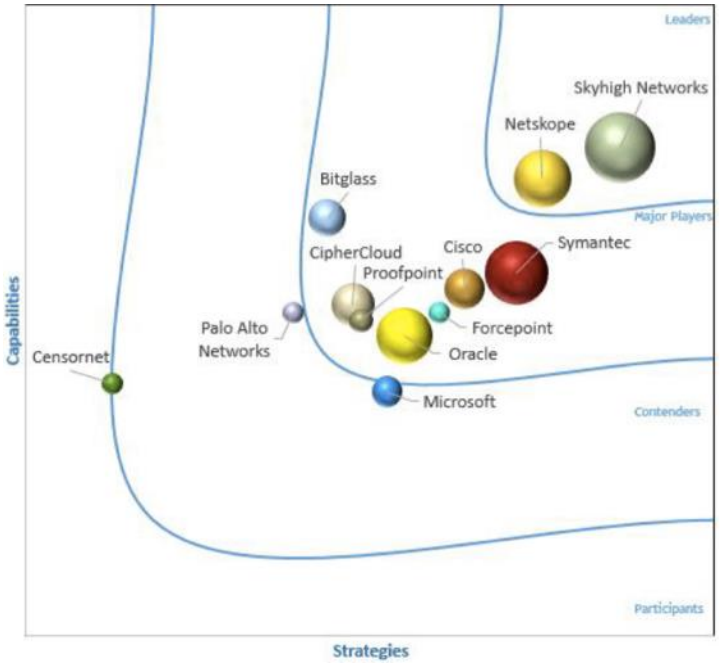
98,000+
corporate customers

1,300+
patents held worldwide

Skyhigh is the only CASB Triple Crown winner

Gartner®

IDC



FORRESTER®

McAfee™
Together is power.

The Evolution of Security Operations

Stuxnet – первое в истории кибер оружие (2009)

WIRED

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

SUBSCRIBE

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

SHARE

SHARE 4759

TWEET

PIN

COMMENT 245

EMAIL

KIM ZETTER SECURITY 11.03.14 6:30 AM

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

LATEST NEWS

FETISH

This Air Purifier Has Brains *and* Doesn't Look Like Garbage

23 HOURS

MEDIA

Never Miss a Thing: Sign Up for WIRED's Newsletter Now

23 HOURS

Атака на Saudi Aramco - 2012

8 MAY 2014 NEWS

Saudi Aramco Cyber Attacks a 'wake-up call', Former NSA Boss

Alexander said malware attacks on Saudi Aramco in 2012 were a "wake-up call for everybody" that could have severe repercussions for the safety of critical infrastructure networks

Former NSA boss Gen. Keith Alexander has claimed that the Shamoon malware attacks on Middle East energy company Saudi Aramco in 2012 were a "wake-up call for everybody" that could have severe repercussions for the safety of critical infrastructure networks.

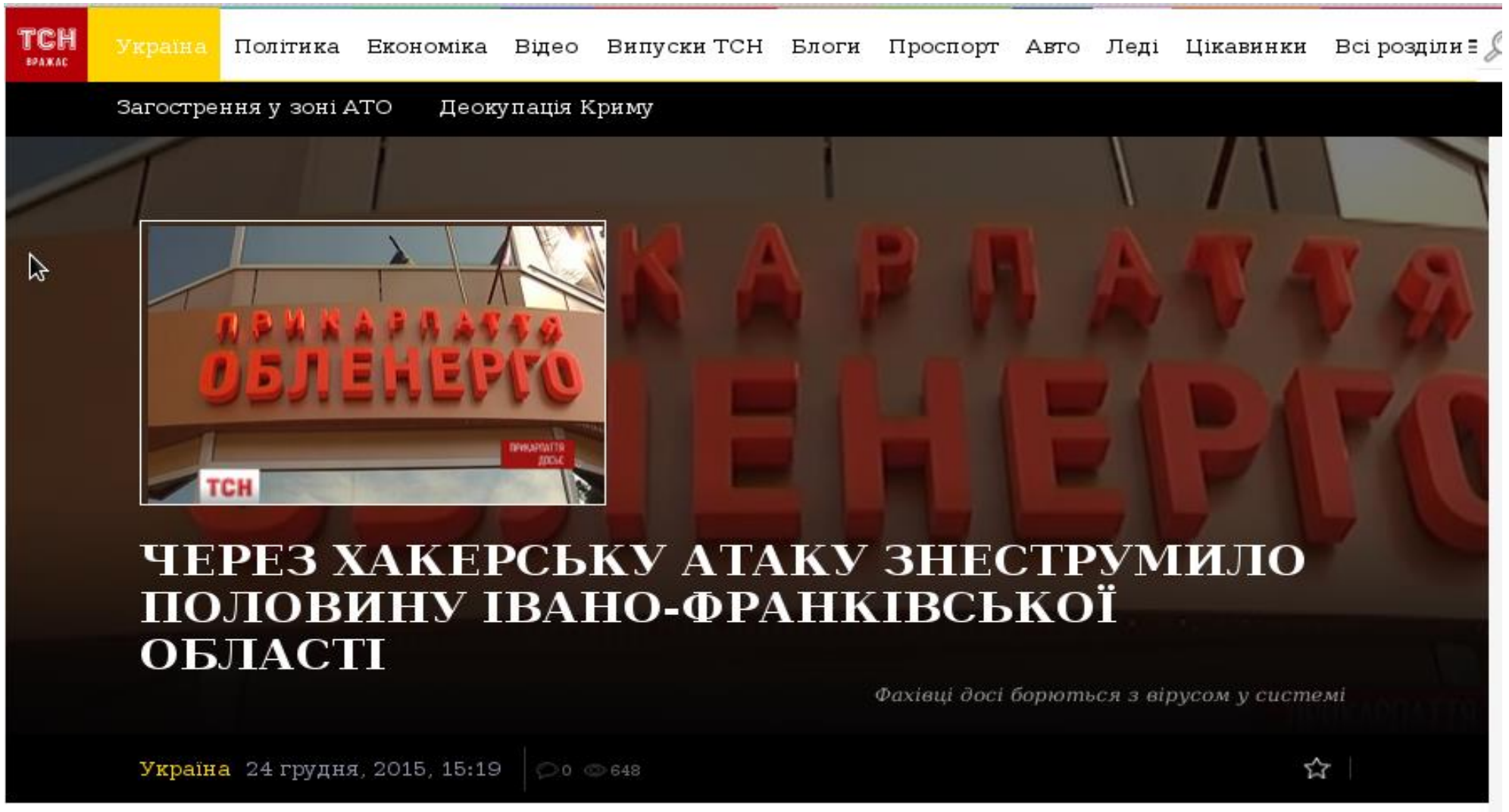
The longest serving director of the much-maligned US security agency made the remarks in a marathon two-hour interview with *Australian Financial Review*, which has published the 17,500-word transcript.

In response to a question asking whether Stuxnet is a "harbinger of a new age of cyber warfare", he argued that, in fact, the Aramco attack was perhaps more noteworthy.

"The new age was not necessarily Stuxnet. It was what happened to Saudi Aramco in August 2012. That's the

- 10% от мировой добычи нефти
- 35 000 компьютеров, тысячи серверов
- вся информация удалена с ЖД
- 5 месяцев до полного востановления!

Атака на энергетический сектор, Украина 2015



NotPETYA, Украина, 27 июля 2017

McAfee Global Threat Intelligence

McAfee GTI received on average 48 billion queries per day in Q4.

PowerShell malware

267%

Script-based threats are a growing concern. **PowerShell malware grew 267% in Q4**, reaching a total count of more than 47,000 samples.

57 million

McAfee GTI protections against risky URLs **fell to 57 million per day in Q4 from 99 million per day in Q3.**

84 million

McAfee GTI protections against risky IP addresses **rose to 84 million per day in Q4 from 48 million per day in Q3.**

Mobile malware

46%

Global infections of mobile devices fell by 0.2%; South America reported the highest rate, at 16%. **Total mobile malware grew 46% in the past four quarters to 24 million samples.**

Ransomware

59%

New ransomware samples increased in Q4, by 35%. **The total number of ransomware samples grew 59% in the past four quarters** to 14.8 million samples.

45 million

McAfee GTI protections against malicious files **increased to 45 million per day in Q4 from 40 million per day in Q3.**

Malware

36%

New malware samples increased in Q4 to an all-time high of 63 million, a 32% increase. **The total number of malware samples grew 36% in the past four quarters to almost 690 million samples.**

Дефицит кадров в сфере кибербезопасности на уровне эпидемии

Острая нехватка человеческих ресурсов там где НАДО принимать решения вживую

62%

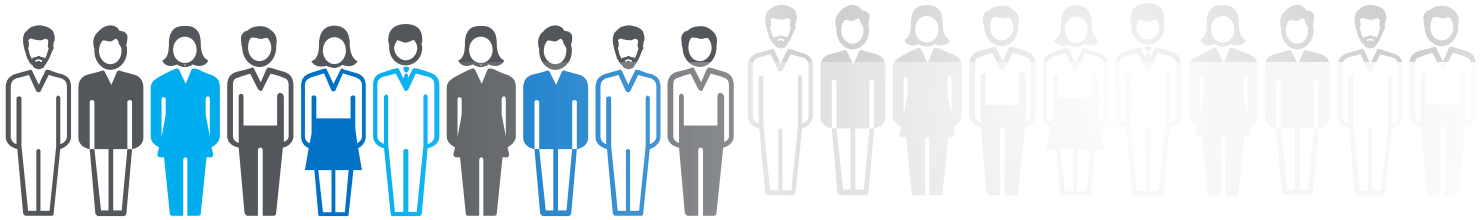
организации в настоящее время недоукомплектованы*

3-6 месяцев

Среднее время для поиска кандидата, при этом 10% позиции всегда открыты*

2 Млн.

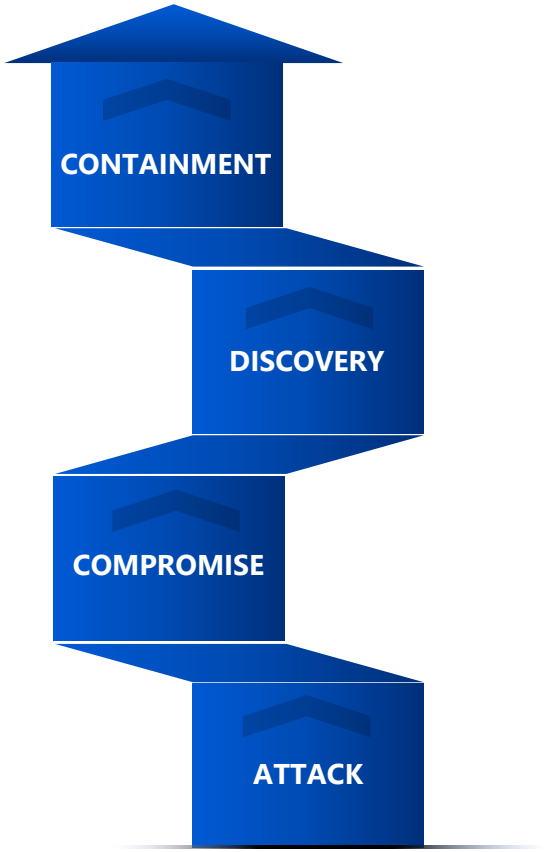
к 2020 году пронозируется нехватка квалифицированных специалистов**



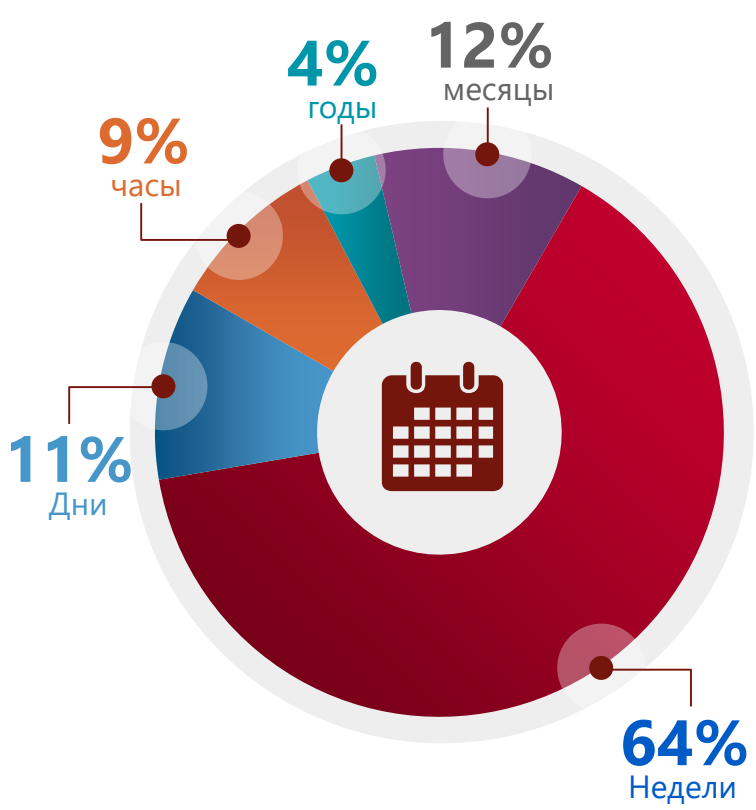
* State of Cybersecurity: Implications for 2015 – ISACA (Состояние Кибербезопасность: Последствия для 2015 года - ISACA)
** Epy 2015 (ISC)2 Global Information Workforce Study – Extrapolation (2015 (ISC) 2 Глобальная информационная Workforce Study – Экстраполяция)

Целенаправленные атаки – новая реальность

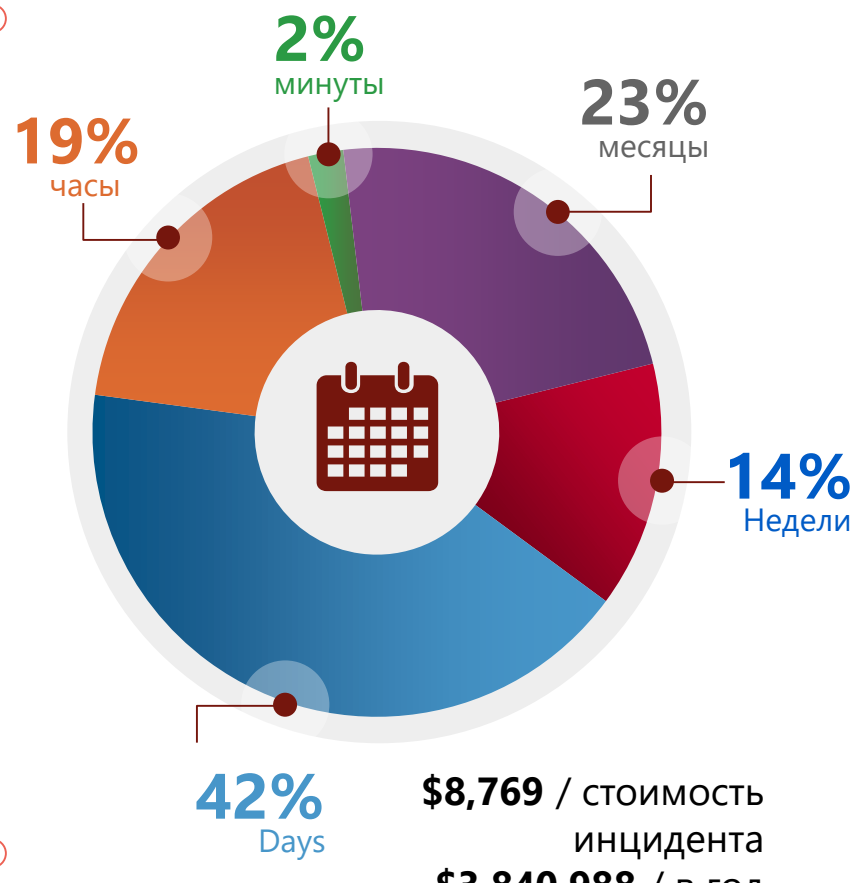
APT



Обнаружение



устранение



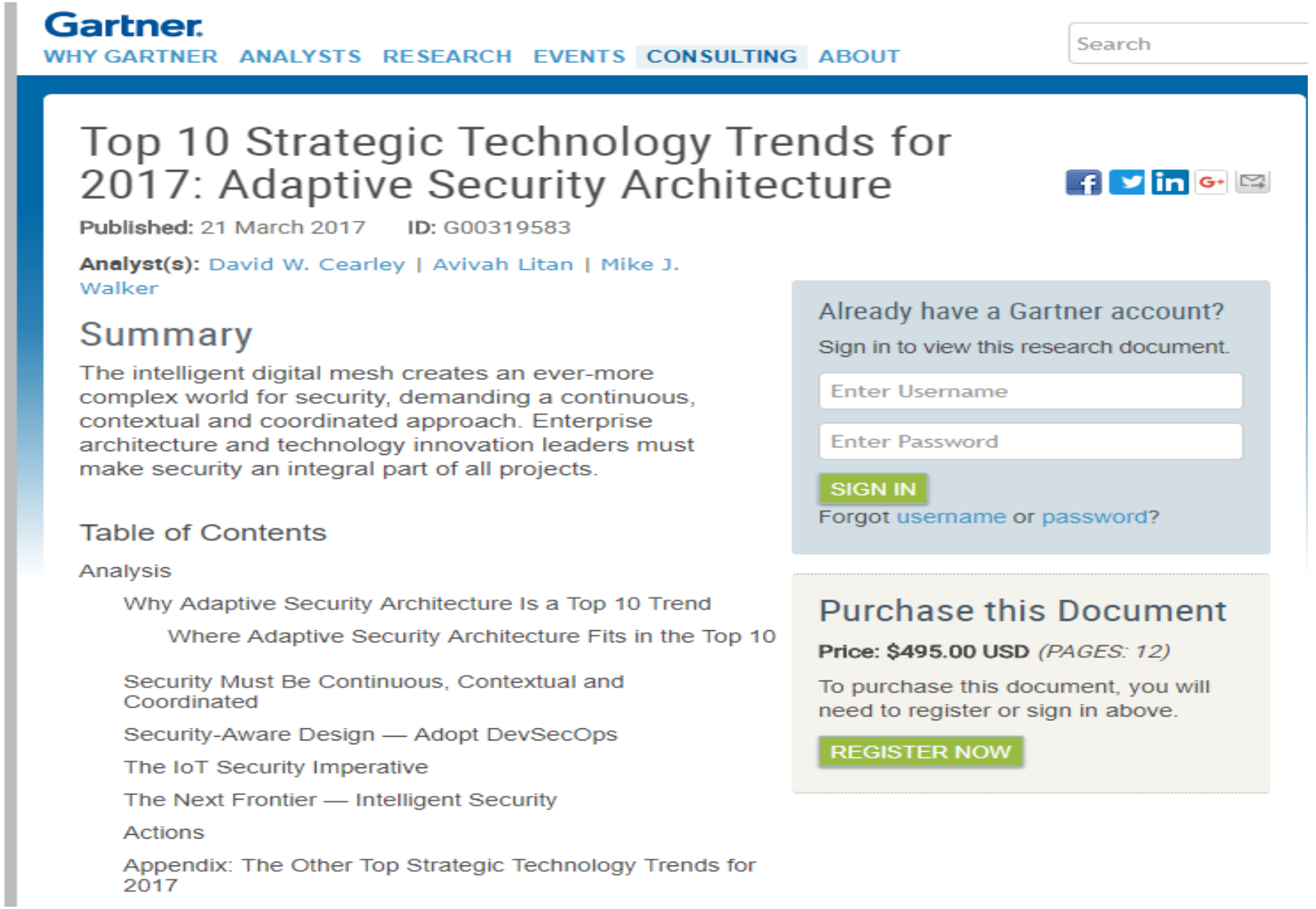
$8,769 / стоимость инцидента
$3,840,988 / в год

Sources: Verizon 2013 Data Breach Investigations Report. Securosis Malware Analysis Quant Metrics Model

“Безопасность это процесс, а не результат”

Bruce Schneier

Adaptive Security Architecture in TOP10 trends



Gartner.

WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

Search

Top 10 Strategic Technology Trends for 2017: Adaptive Security Architecture

Published: 21 March 2017 **ID:** G00319583

Analyst(s): David W. Cearley | Avivah Litan | Mike J. Walker

Summary

The intelligent digital mesh creates an ever-more complex world for security, demanding a continuous, contextual and coordinated approach. Enterprise architecture and technology innovation leaders must make security an integral part of all projects.

Table of Contents

Analysis

- Why Adaptive Security Architecture Is a Top 10 Trend
  - Where Adaptive Security Architecture Fits in the Top 10
- Security Must Be Continuous, Contextual and Coordinated
- Security-Aware Design — Adopt DevSecOps
- The IoT Security Imperative
- The Next Frontier — Intelligent Security
- Actions
- Appendix: The Other Top Strategic Technology Trends for 2017

Already have a Gartner account?

Sign in to view this research document.

Enter Username

Enter Password

SIGN IN

Forgot username or password?

Purchase this Document

Price: $495.00 USD *(PAGES: 12)*

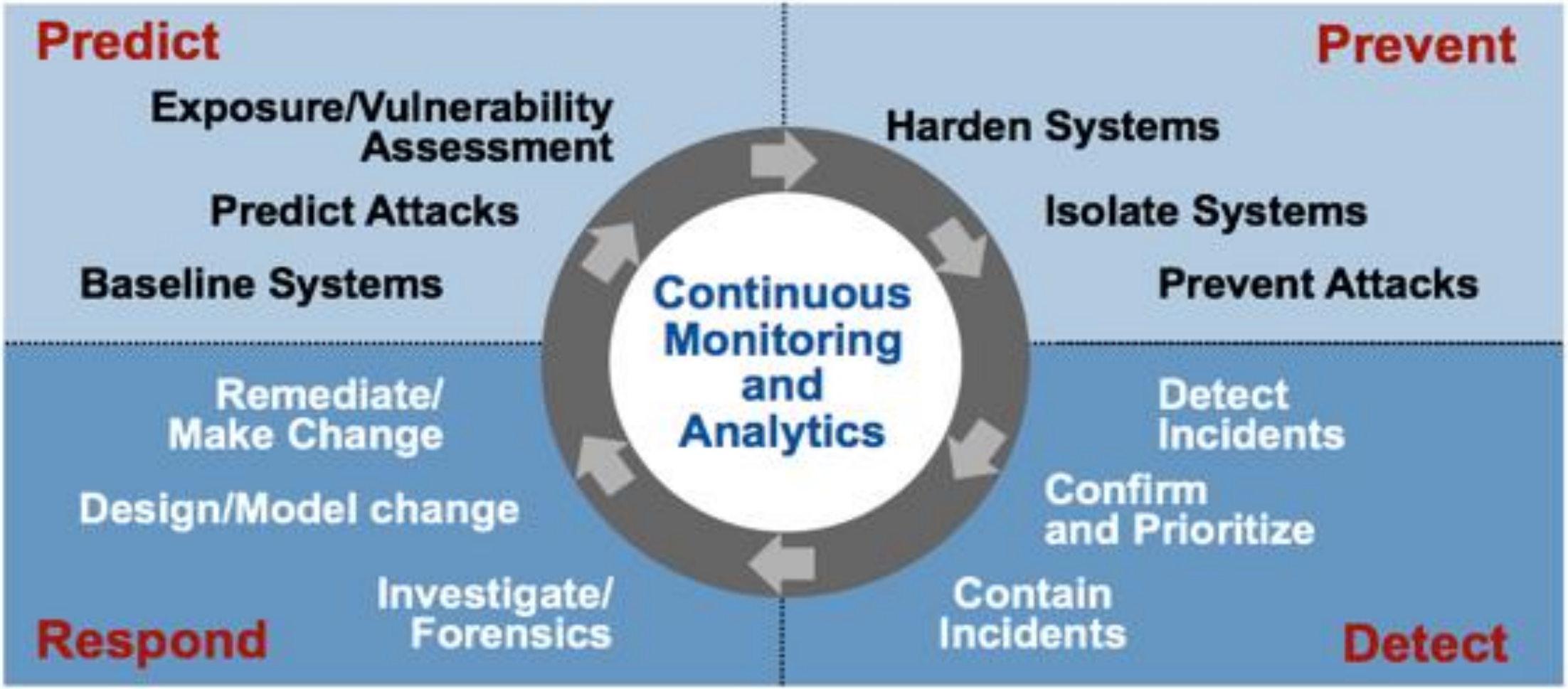
To purchase this document, you will need to register or sign in above.

REGISTER NOW

Краткие выводы от Gartner:

- Существующих технологий защиты недостаточно для противостояния современным целенаправленным атакам.
- Большинство организаций до сих пор инвестируют средства только в технологии защиты.
- ***Технологии защиты, предотвращения атак, детектирования и расследования/устранения от различных производителей не интегрированы друг с другом, что приводит к дополнительному хаосу, увеличивает затраты и снижает эффективность ИБ.***
- ИБ не хватает постоянной видимости происходящего для детектирования целенаправленных атак.
- Корпоративные системы находятся под постоянными и не прекращающимися атаками, поэтому понятие «Incident Response» больше не подходит.

The Adaptive Security Architecture: Twelve Critical Capabilities of Security



Gartner

Рекомендации от Gartner:

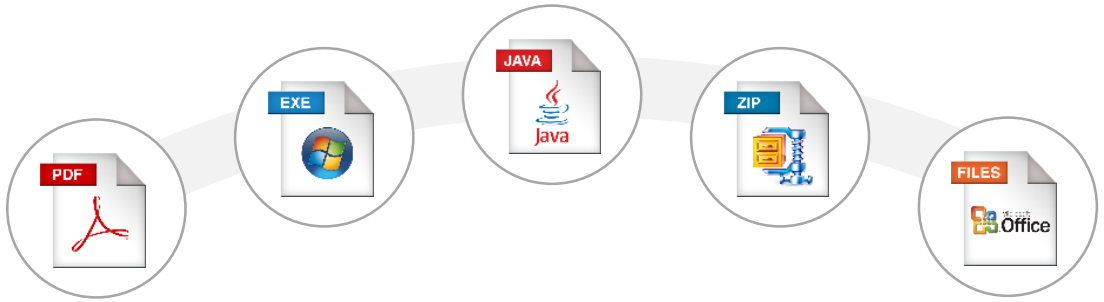
- Поменять понятие «Incident Response» на «Continuous Response», где предполагается, что системы постоянно скомпрометированы и им необходим непрерывный мониторинг и восстановление.
- Создание Адаптивной Архитектуры Безопасности для защиты от целенаправленных атак, используя 12 критических функций от Gartner.
- Направить больше инвестиции на системы обнаружения и быстрого реагирования, и уменьшить на защиту и предотвращение.
- **Отдавать предпочтения производителям, которые предлагают контекстно-ориентированные платформы для сетевой безопасности, безопасности рабочих станций и приложений, а также интегрированный подход к анализу, предотвращению, обнаружению и реагированию на атаки.**
- Развивать Security Operation Center (SOC), который позволяет осуществлять постоянный мониторинг и предотвращение атак.
- Осуществлять полный мониторинг на всех уровнях ИТ: сетевых пакетов, сетевых потоков, активности ОС, контента, поведения пользователей.

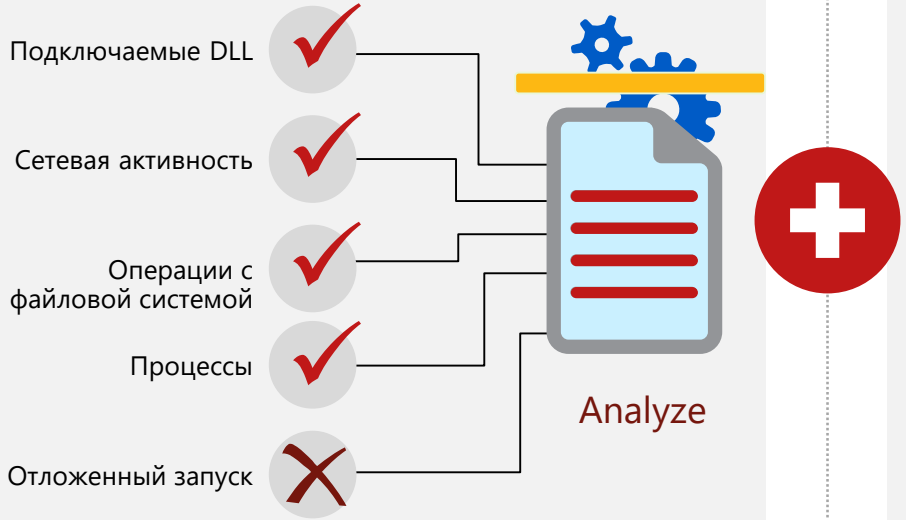
Экосистема McAfee

Обнаружение сложных атак McAfee Advanced Threat Defense

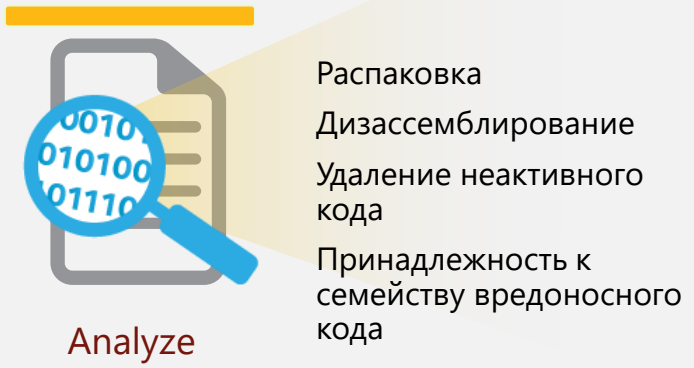
Идентификация: статический и динамический анализ угроз

В стандартном и пользовательском окружении





Динамический анализ

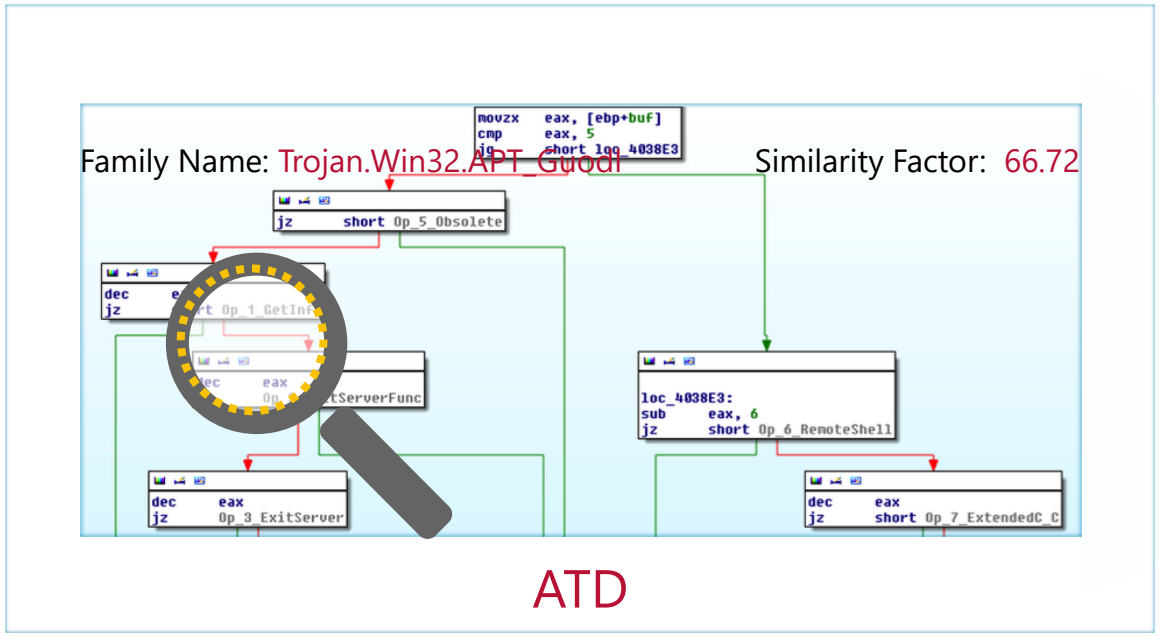


Статический анализ

Некоторые угрозы «обходят» динамический анализ

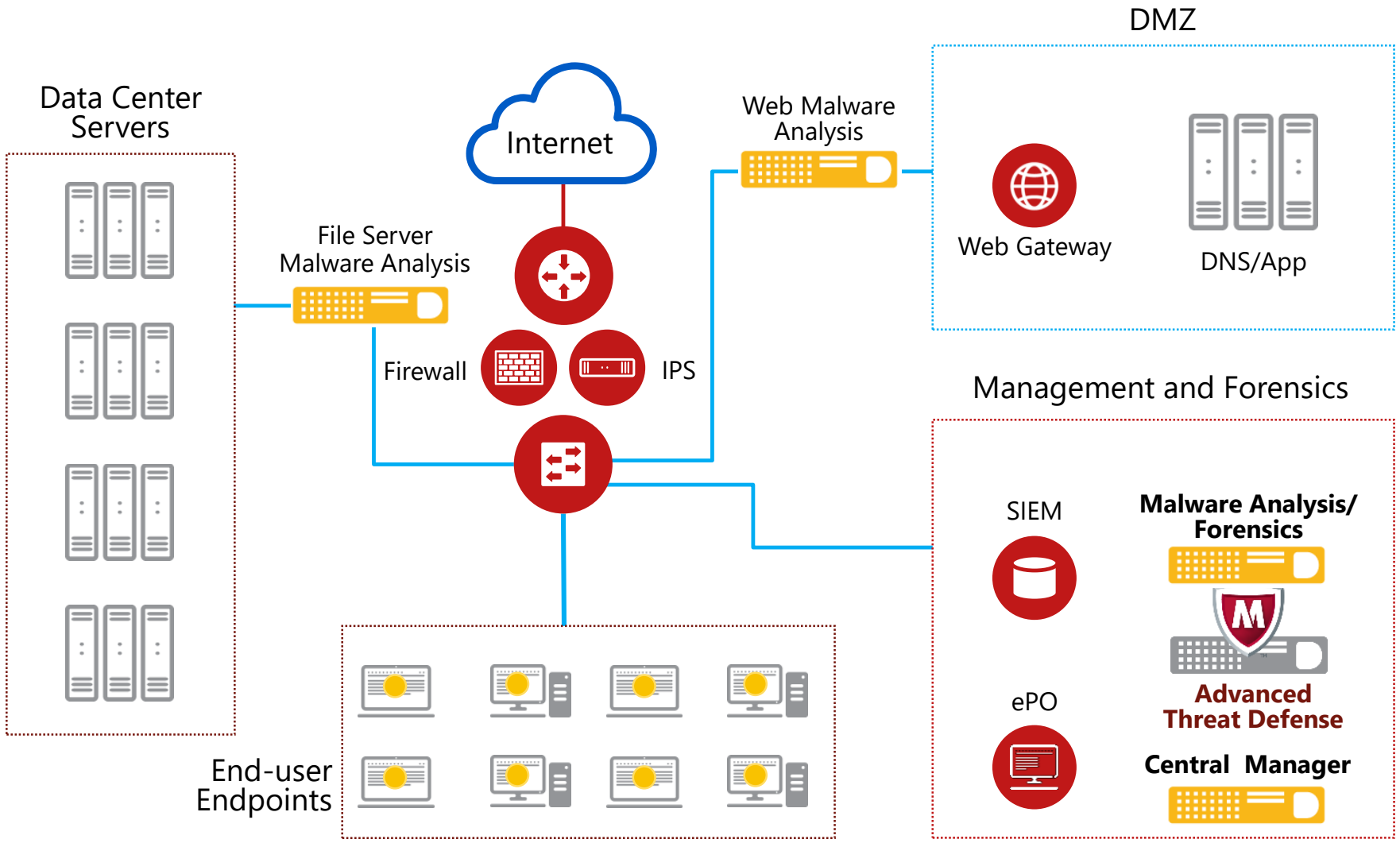
В этих случаях помогает статический анализ кода

Advanced Threat Defense сканирует образец
Может быть не зафиксировано вредоносного поведения (отложенный запуск, VM Evasions)
Распаковка и классификация кода позволяют выявить вредоносный контент внутри



Централизованная установка

Уменьшение себестоимости и производительность



Широкий выбор

Любой набор по производительности и возможности инсталляции

Программно-аппаратный комплекс

Advanced Threat Defense

ATD-3100
ATD-6100

- Все данные остаются в организации
- 2 модели разной производительности
- Большой функционал для расследования

Виртуальная машина

Virtual Advanced Threat Defense

x8

- Весь функционал ATD + гибкость внедрения
- Для Дата Центров, филиалов и
- OpEx vs CapEx

+ Интеграция с MS Exchange, Cisco ESS
+ STIX/TAXII

Анализ WannaCry в McAfee Advance Threat Defense

Behavior Classification

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	Very High
Spreading	Very High
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	High
Exploiting, Shellcode	High
Networking	Low
Data spying, Sniffing, Keylogging, Ebanking Fraud	Low
Persistence, Installation Boot Survival	Unverified

Dynamic Analysis

Action	Severity
Injected code into processes using Dynamic Forking method	Very High
Injected into a different process memory and changes the access protection of the committed pages	High
Collecting credentials from different sources	Medium
Wrote (injected) data to an area of a foreign process memory	Medium
Downloaded data from a webserver	Low
Queried information of pages within the virtual address space of another process	Low

GTI Web/URL Reputation

Connected Sites: 2

URL	Port	Reputation	Category Name	Risk Group	Functional Group
82.165.142.107	80	High Risk	---	---	---
87.106.75.19	80	High Risk	---	---	---

Processes Analyzed

Name	Reason	Severity
xwn56asj6.exe	loaded by MATD Analyzer & dropped by xwn56asj6.exe	Very High
grammarquota.exe	executed by xwn56asj6.exe	Very High

Анализ NotPetya в McAfee Advance Threat Defense

Engine Analysis

Engine	Threat Name	Severity
GTI File Reputation	---	Very High
GTI URL Reputation		
Gateway Anti-Malware	Artemis!ADD1777EF790	Very High
Anti-Malware	---	Unverified
YARA	---	Unverified
Custom Rules		
Sandbox	Malware.Dynamic	Very High
Final		Very High

Sample is malicious: final severity level 5

Dynamic Analysis

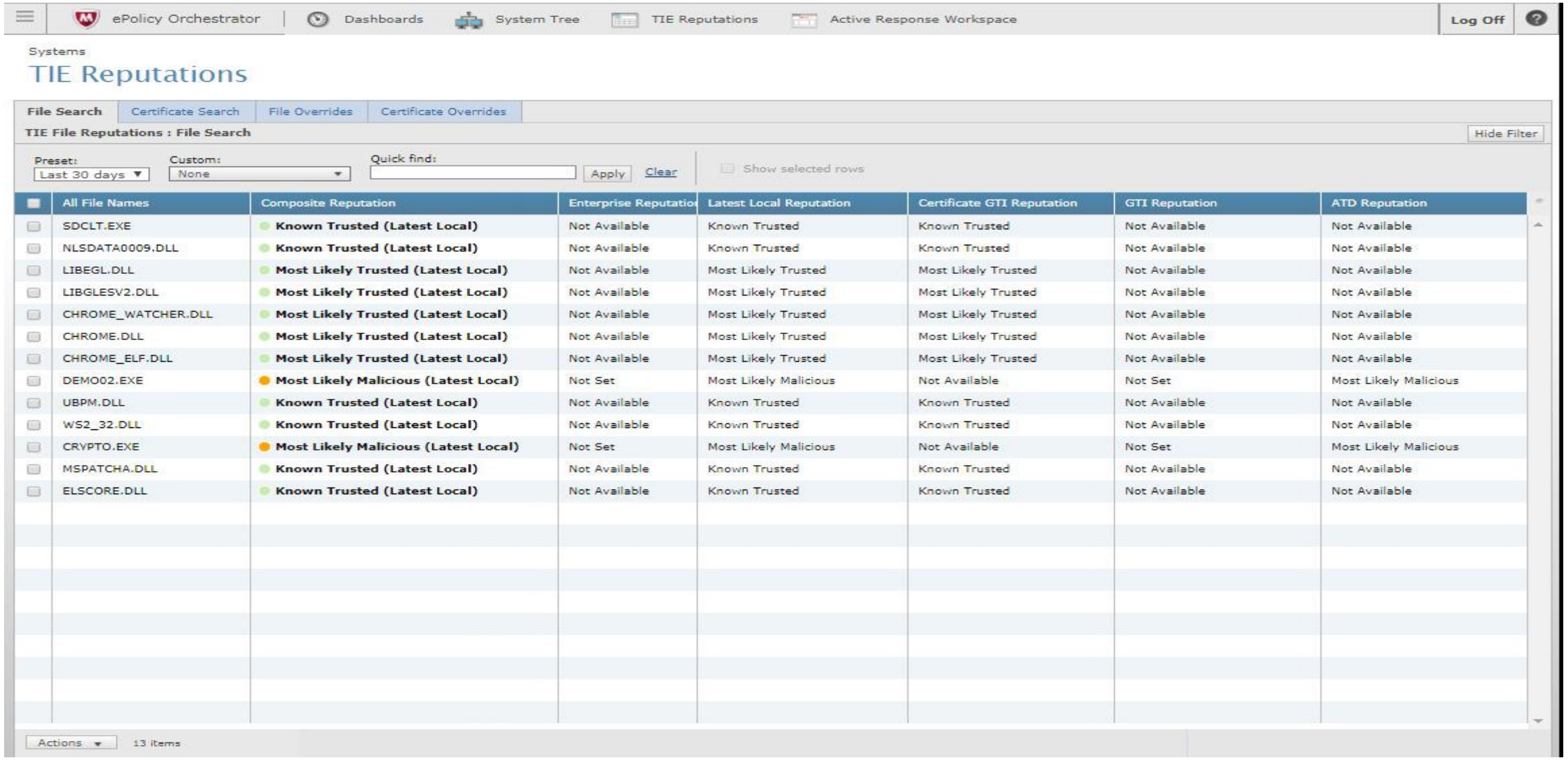
Action	Severity
OverWrites MBR and behaves like ransomware	Very High
OverWrites MBR sector and hijacks operating system booting	High
Dropped malicious files in standard Windows executable names	High
Gathered physical access to the hard drive	Low
Modified time attribute of the specified file after its creation	Low
Allowed the process to perform system-level actions that were not enabled previously	Low
Created named mutex object	Low
Created new PE file	Informational

Behavior Classification

Persistence, Installation Boot Survival	Very High
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	Very High
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	High
Spreading	High

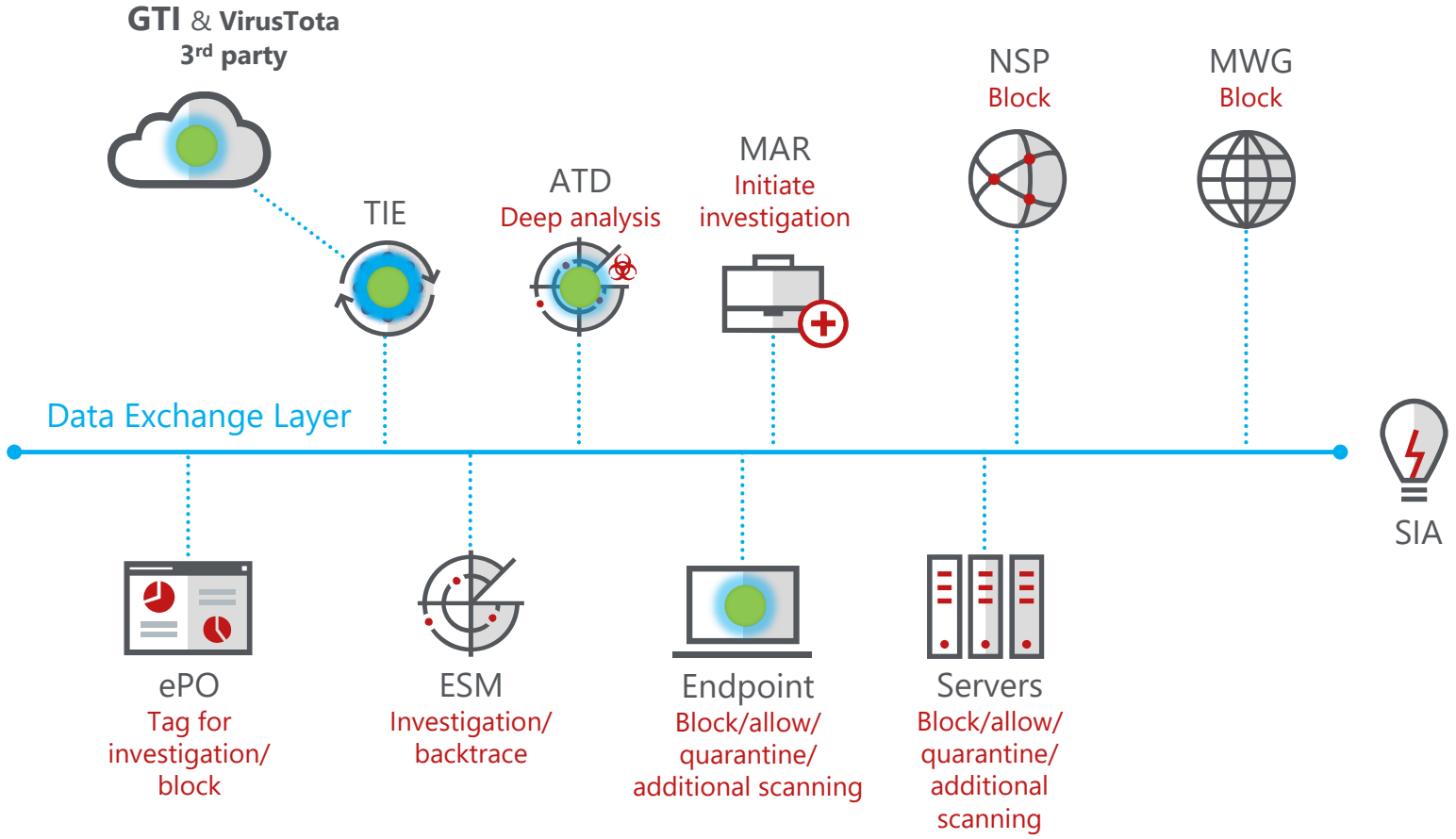
McAfee Threat Intelligence Exchange DXL

McAfee Threat Intelligence Exchange



McAfee Adaptive Security Architecture

Share reputation intelligence instantly across the entire ecosystem



Extreme® Connect Beyond the Network

RAPID7

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

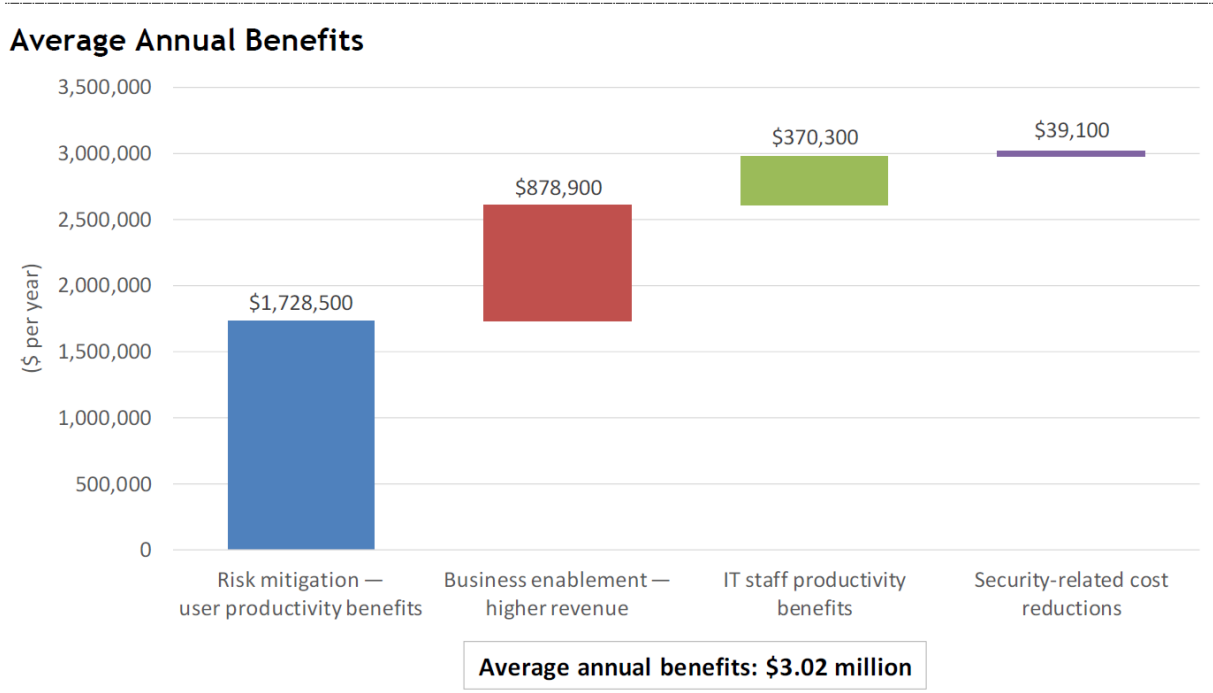
JUNIPER NETWORKS

IDC ExpertROI Spotlight Top 100 US FDIC Bank

"Мы можем обнаружить атаку в течении 60 секунд, провести анализ и ликвидировать атаку в течении 5 минут"

Решения: Endpoint, SIEM, TIE, GTI, ATD, DLP

FIGURE 1



Source: IDC, 2017

- Экономия средств **$3.02 M** в год
- **ROI 208%** в течении 4 лет
- Период окупаемости **20** месяцев
- На **90%** быстрее расследование инцидентов
- На **77%** меньше инцидентов с причиненным ущербом
- На **98%** меньше времени снижение продуктивности из-за инцидентов ИБ
- **$5-10 миллионов** дополнительная прибыль
- Мониторинг всех компонентов на **1-2** консолях

Source: http://idcdocserv.com/US42210917

Phase 2: Security Innovation Alliance Partners

SIA Partners

Connected Today

- Advanced Cyber Security
- aruba, a Hewlett Packard Enterprise company — POC
- Avecto
- boldonjames
- Check Point Software Technologies Ltd.
- CICADA Security Technology
- FORCEPOINT
- HUAWEI — POC
- RAPID7
- TITUS
- TYCHON
- TRAPX SECURITY

In Testing or Development Today

- Attivo Networks
- Autonomic Software
- Guidance Software
- GURUCUL
- Infoblox — Control Your Network
- INTERSET
- Lumeta
- MobileIron
- NIKSUN
- proofpoint
- THREATCONNECT

In Design

- ayehu
- BeyondTrust — Visibility. Knowledge. Action.
- BUFFERZONE
- CISCO
- CYPHORT
- DFLABS — Cyber Incidents Under Control
- Extreme — Connect Beyond the Network
- ForeScout
- JUNIPER NETWORKS
- Phantom
- sas
- tenable network security
- vmware airwatch
- THALES

DXL Integration Use Cases

SIA Partners

Check Point SOFTWARE TECHNOLOGIES LTD.	▪ SandBlast integration with DXL, TIE and ePO ▪ Publishing Topics: File Reputation, IOC, Threat Event Data, Mobile ▪ Subscribing Topics: IOC, File Reputation Updates
aruba a Hewlett Packard Enterprise company	▪ ClearPass integration with DXL and ePO ▪ Publishing Topics: IOC Information, New Asset Discovery Information ▪ Subscribing Topics: IOC information, Threat Event
RAPID7	▪ Nexpose integration with DXL, TIE and ePO ▪ Publishing Topics: IOC, Vulnerability, New Asset Discovery Information ▪ Subscribing Topics: IOC, File Reputation, Threat Event, Vulnerabilities
TRAPX SECURITY	▪ Deception Grid integration with DXL, TIE and ePO ▪ Publishing Topics: File Reputation, IOC, Threat Event Data ▪ Subscribing Topics: IOC, File Reputation, Threat Event

DXL Integration Use Cases

Элементы для защиты конечных точек

McAfee Complete Endpoint Protection - Business

Самая совершенная защита для среднего бизнеса*

Наиполнейший набор опций с продвинутой защитой, шифрованием данных, динамическим сдерживанием приложений и машинным обучением для защиты от сложных атак, с дополнительным модулем EDR для быстрого реагирования и восстановления, и ePolicy Orchestrator для централизованного управления и отчетности.

Основа защиты

- Web Control
- Firewall
- Threat Prevention
- Data Protection
- Application Control
- Dynamic Application Containment
- Machine Learning

Дополнительный модуль EDR

- McAfee Active Response (MAR)
- McAfee Threat Intelligence Exchange (TIE)

Развертывание, управление, отчетность

- ePolicy Orchestrator

True Centralized management with a single pane of glass

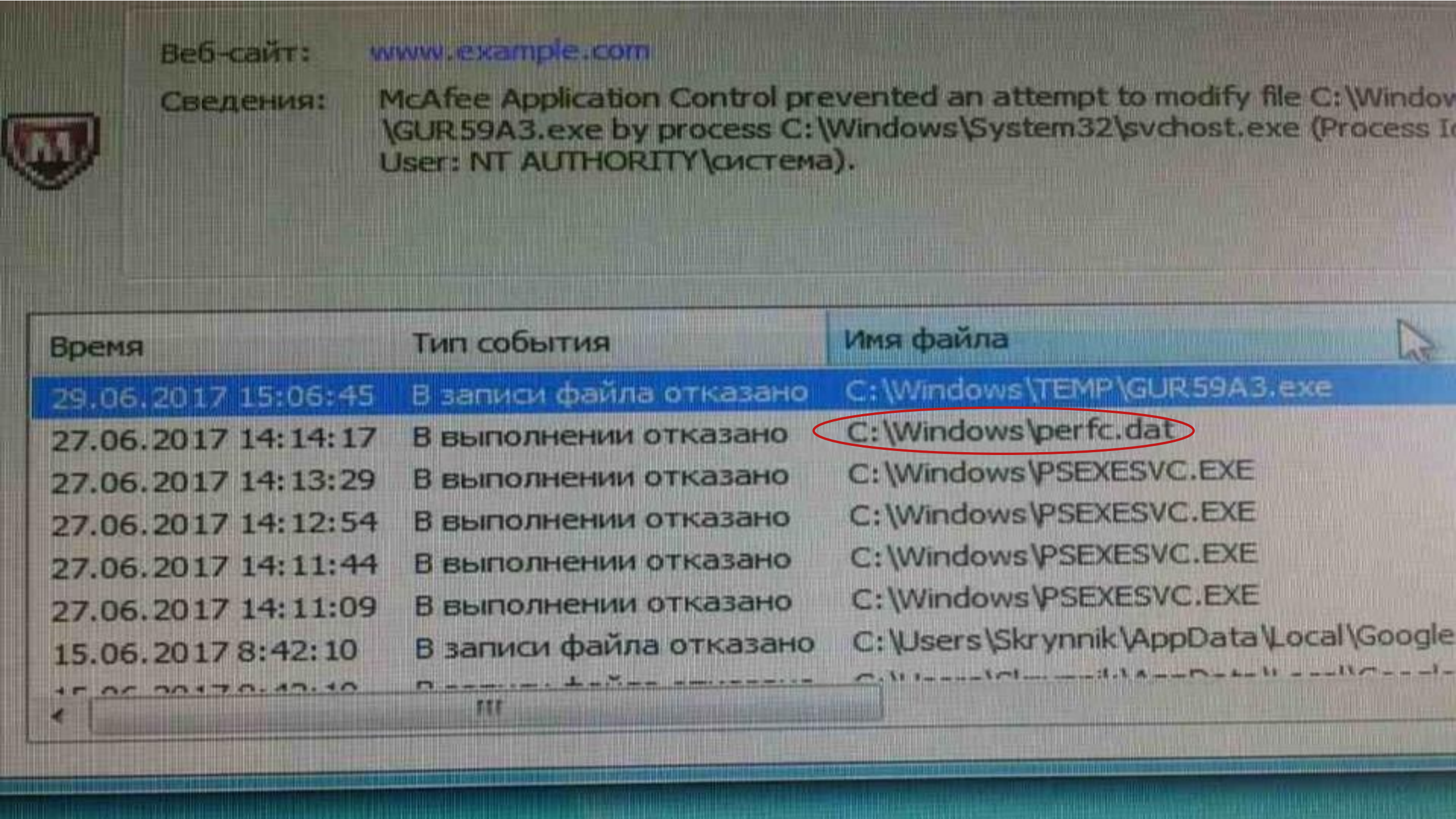
*Limit 2000 nodes, added in Q2 '17: (Dynamic Application Containment, Real Protect, Application Control), CEB Customers are now eligible for discount on optional EDR

McAfee Application Control
защита на основе динамических белых списков

McAfee Application Control
защита на основе динамических белых списков

Белый список создается при инсталляции и включает в себя приложения, драйверы, библиотеки и скрипты

1. Попытка запуска приложения
   - Исполняемый файл / компонент ОС
2. MAC сверяет его с белым списком
3. Если приложение не в белом списке – оно не запускается.
   - Попытка журналируется



Веб-сайт: www.example.com

Сведения: McAfee Application Control prevented an attempt to modify file C:\Windo
\GUR59A3.exe by process C:\Windows\System32\svchost.exe (Process I
User: NT AUTHORITY\система).

Время	Тип события	Имя файла
29.06.2017 15:06:45	В записи файла отказано	C:\Windows\TEMP\GUR59A3.exe
27.06.2017 14:14:17	В выполнении отказано	C:\Windows\perfc.dat
27.06.2017 14:13:29	В выполнении отказано	C:\Windows\PSEXESVC.EXE
27.06.2017 14:12:54	В выполнении отказано	C:\Windows\PSEXESVC.EXE
27.06.2017 14:11:44	В выполнении отказано	C:\Windows\PSEXESVC.EXE
27.06.2017 14:11:09	В выполнении отказано	C:\Windows\PSEXESVC.EXE
15.06.2017 8:42:10	В записи файла отказано	C:\Users\Skrynnik\AppData\Local\Google

Детектирование угроз 0-дня, Защита от Пациент-0

Обнаружение скрытых атак и минимизация последствий

Обмен репутациоонными данными
Локальные, глобальные, или 3 стороны

Статический
Анализ подозрительных атрибутов перед запуском

Сдерживание
Блокировка подозрительных активностей

Динамический
Поведенческий анализ в режиме реального времени

- **Обнаружение** – больше атак, чем сигнатурный или статический анализ
- Автоматическое обновление модели угроз через **машинное обучение**
- Остановить **вредоносные изменения** и изолировать сеть от инфекции
- Найти **скрытые атаки** при сравнении вредоносных атрибутов

Новые возможности адаптивной защиты

Dynamic Application Containment

- Контроль неизвестного «серого» ПО с возможностью отката
- Защита “нулевого пациента”
- Для борьбы с вредоносными файлами, опознающими запуск в «песочнице»
- Работает в режиме оффлайн

Real Protect - машинное обучение

- Наиболее эффективное выявление вредоносных средств “нулевого дня”
- Использует для классификации локальную копию аналитической модели или/и обращается к облаку

Тесты NSS Labs

McAfee Endpoint Security version 10.5

100%

Tested Evasions Blocked

0%

False Positives

99%

Overall Security Effectiveness

Endpoint Security (ENS) 10.5 + DAC + RealProtect

Security Effectiveness		98.98%	
False positives (detection accuracy)		0.0%	
Malware	Block rate	Additional detection rate	Security Effectiveness
HTTP	100.0%	0.0%	100.0%
HTTPS	100.0%	0.0%	100.0%
Email (IMAP4/POP3)	100.0%	0.0%	100.0%
P2P applications	100.0%	0.0%	100.0%
Local intelligence evaluation	100.0%	0.0%	100.0%
Exploits	Block rate	Additional detection rate	Security Effectiveness
Exploits	100.0%	0.0%	100.0%
Blended threats	92.9%	0.0%	92.9%
Evasions	Block rate	Additional detection rate	Security Effectiveness
Evasions	100.0%	0.0%	100.0%

Какое решение для защиты выбрать?

	Системы с фиксированными функциями	Сервера	Десктопы	Динамические десктопы
				
	⬅ STATIC			DYNAMIC ➡
Первичный Antimalware	MAC	MAC	MAC	ENS
Вторичный Antimalware		ODS	ENS	

McAfee Active Response (EDR)

McAfee Active Response

Detect, Contain and Eliminate Advanced Threats

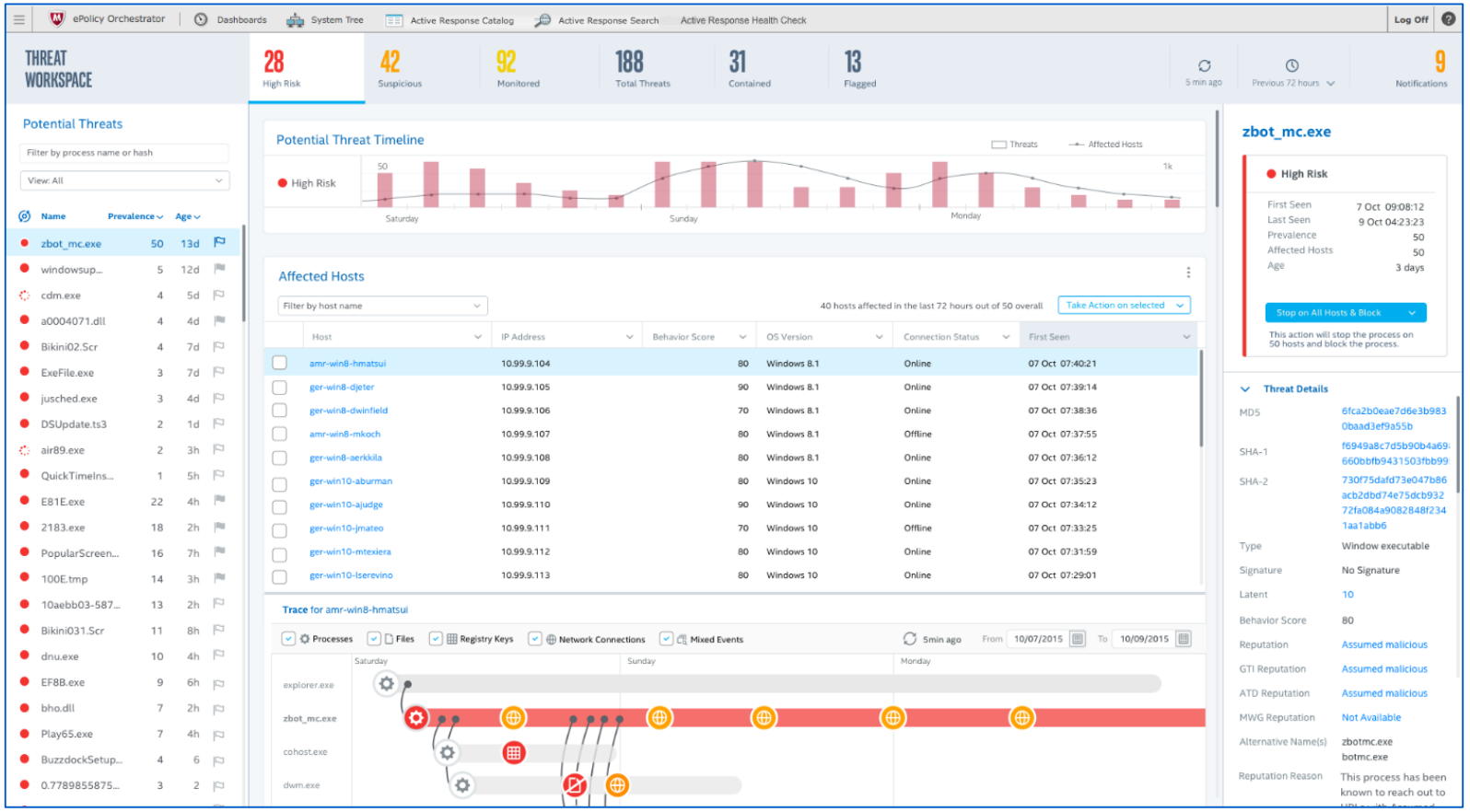
- Постоянный мониторинг критичных событий и изменений
- Постоянный сбор событий для визуализации всех файлов
- Установка триггеров для автоматических действий
- Эффективное управление, обнаружение и устранение

Молниеносная «охота» за вредоносным кодом

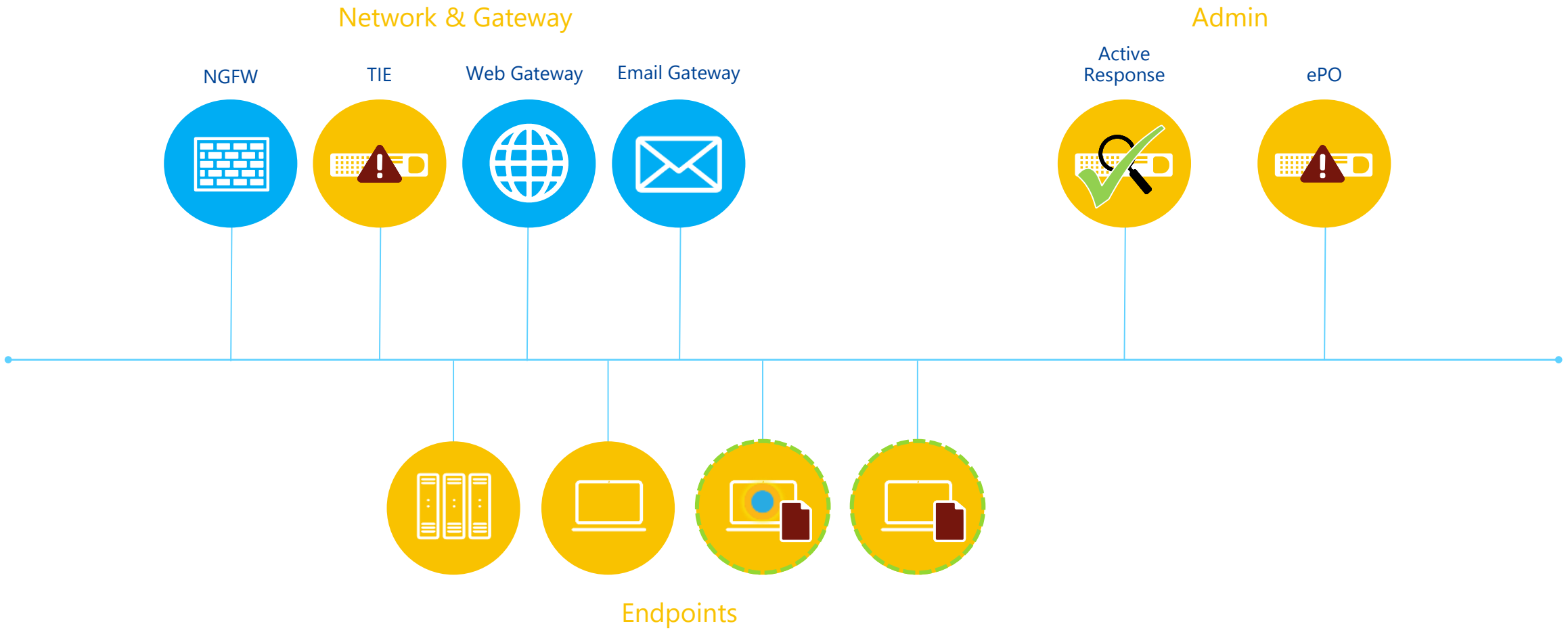
Найти и обезвредить в считанные секунды, - не дни или месяцы!

Простой дашборд для анализа и действий

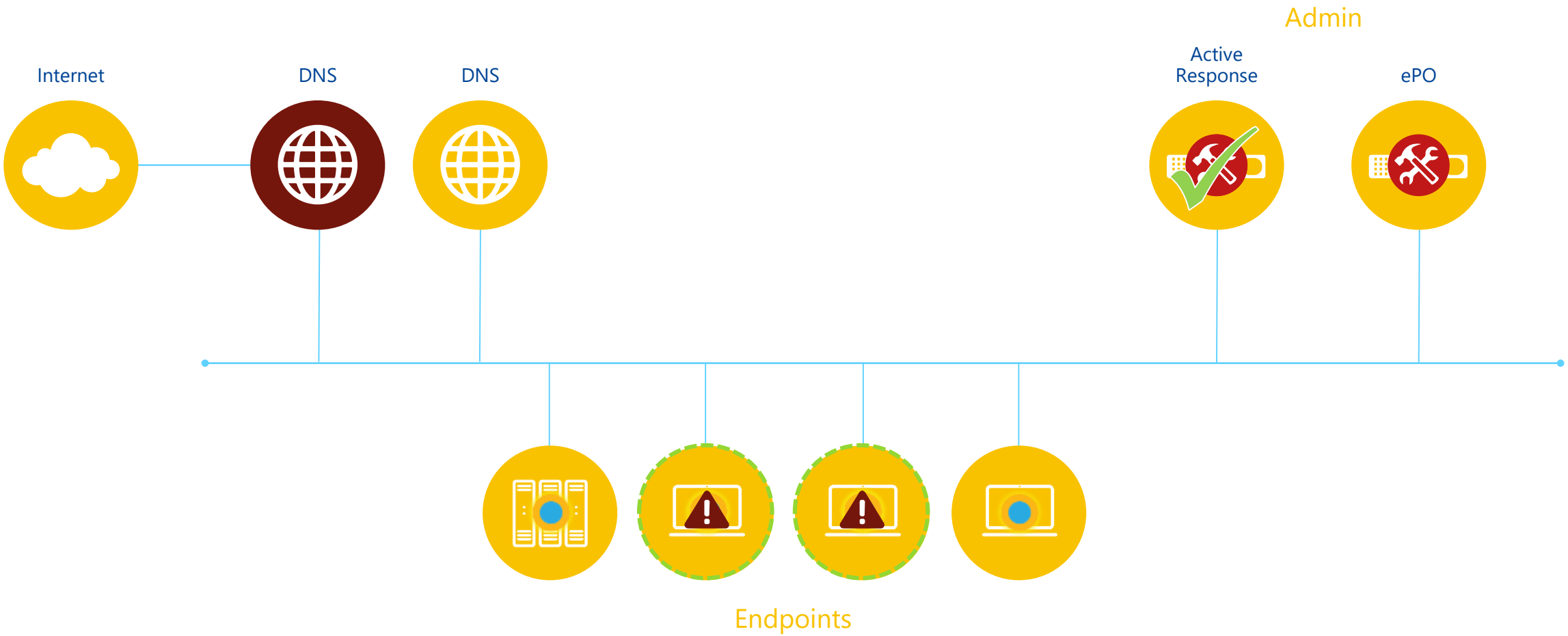
- Автоматическая категоризация подозрительных событий
- Визуализация трендов угроз
- Вывод угроз с наивысшим приоритетом в зависимости от времени возникновения
- Корреляция атак запущенных на хосте
- Идентификация «живых», затаившихся или удалённых вредоносного кода
- Применение мгновенной реакции для обезвреживания вредоносного кода



Пример 1
Поиск не запущеных вредоносных файлов



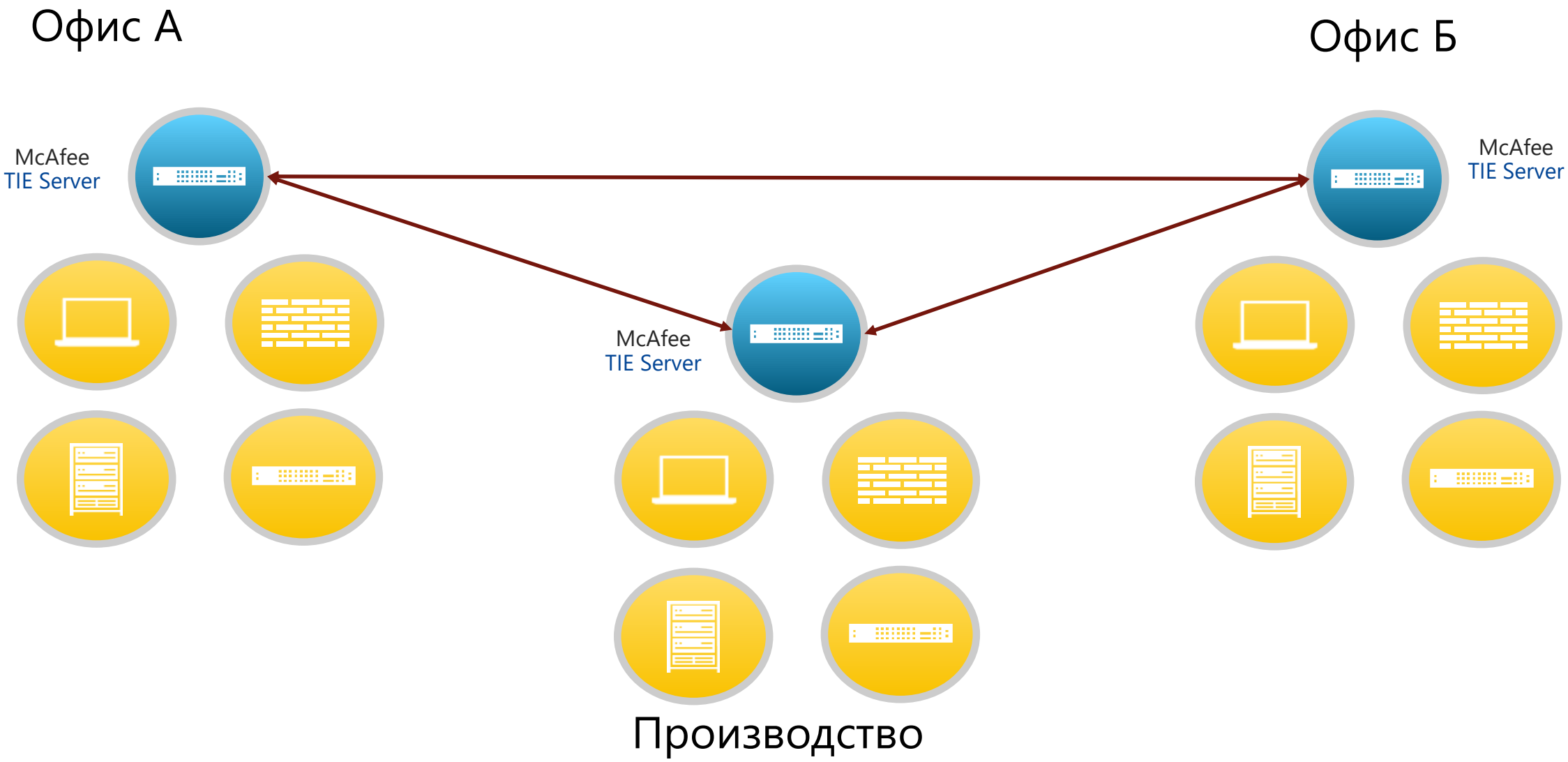
Пример 3
Мониторинг сетевой активности



Защита корпорации

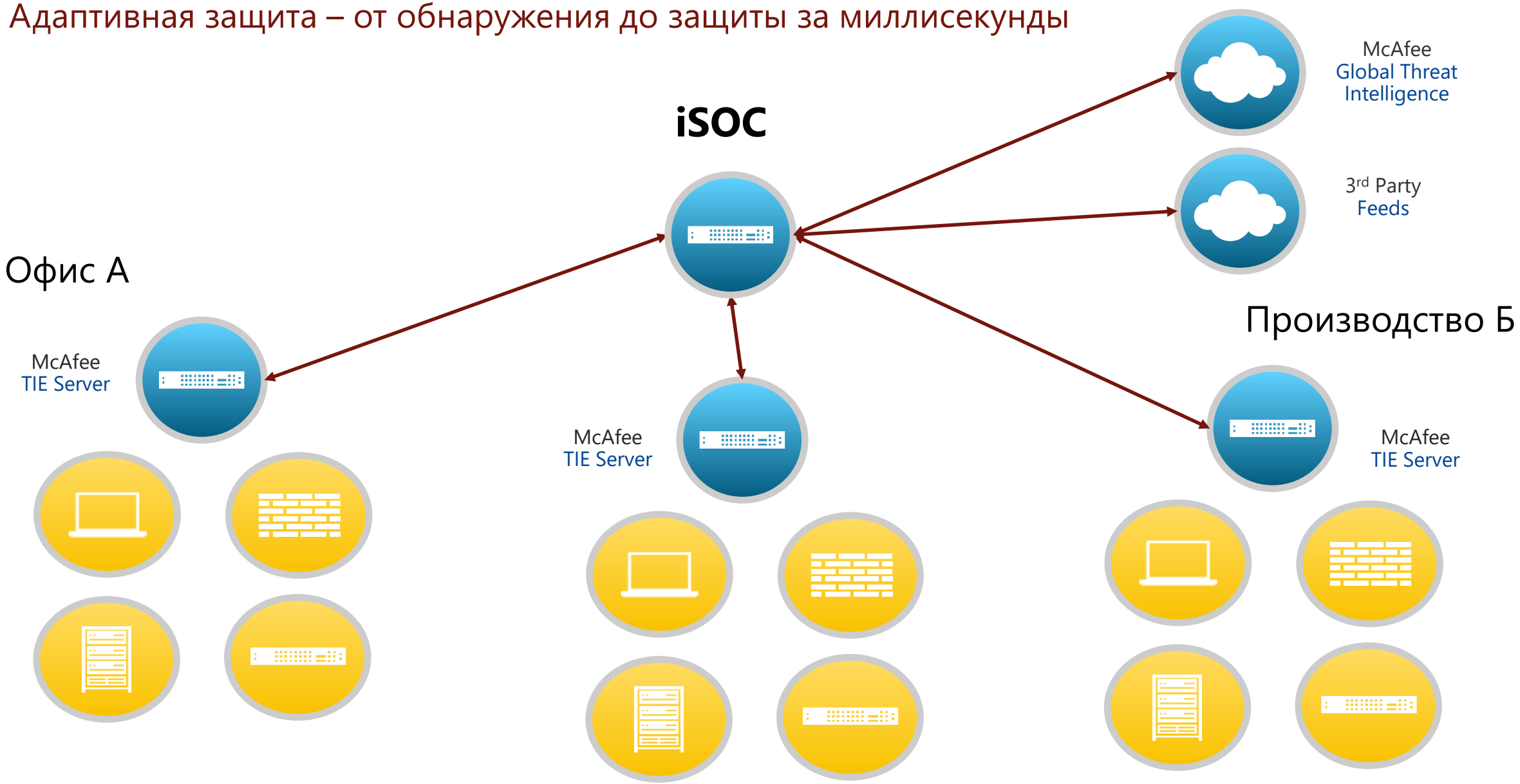
Защита корпорации

Адаптивная защита – от обнаружения до защиты за миллисекунды



Защита для всего государства

Адаптивная защита – от обнаружения до защиты за миллисекунды



Solution Architecture

Advanced Threat Intel Use Case

Threat Intelligence and Orchestration Platforms

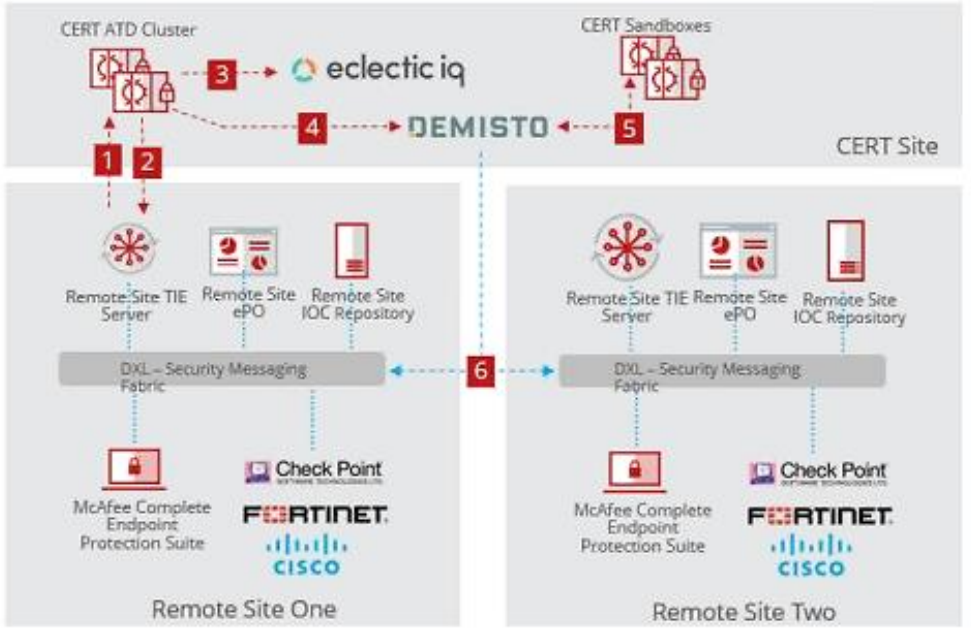
- Open Source and Commercial
- Used to extend Sec Ops solutions
- Improve the value of our Endpoint solutions

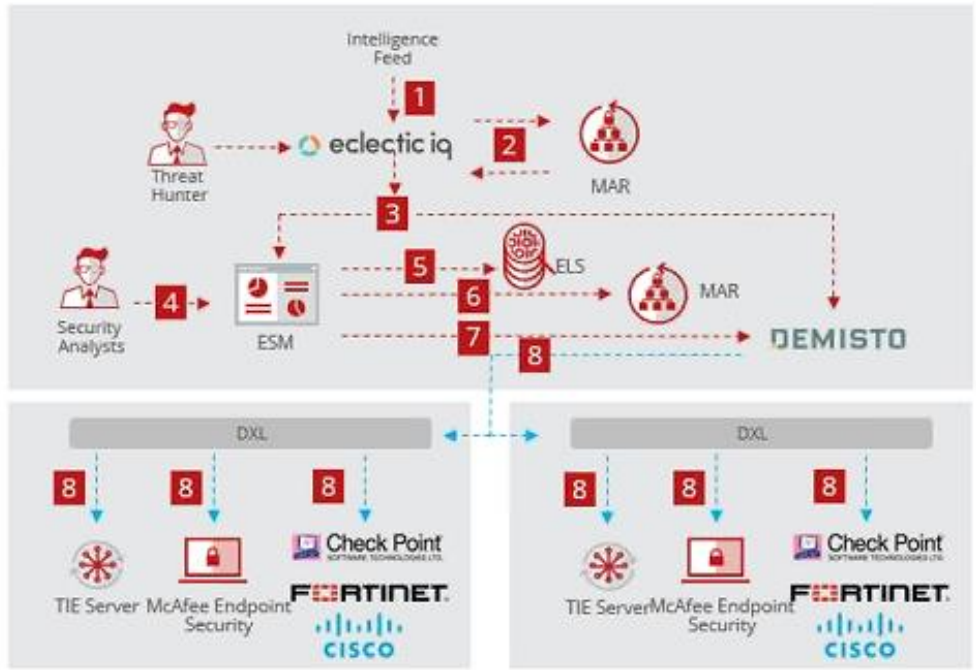
Multi-Agency Threat Intel Sharing

- National CERT
- Large Government or Enterprise customers
- MSSP

External Asset Locations

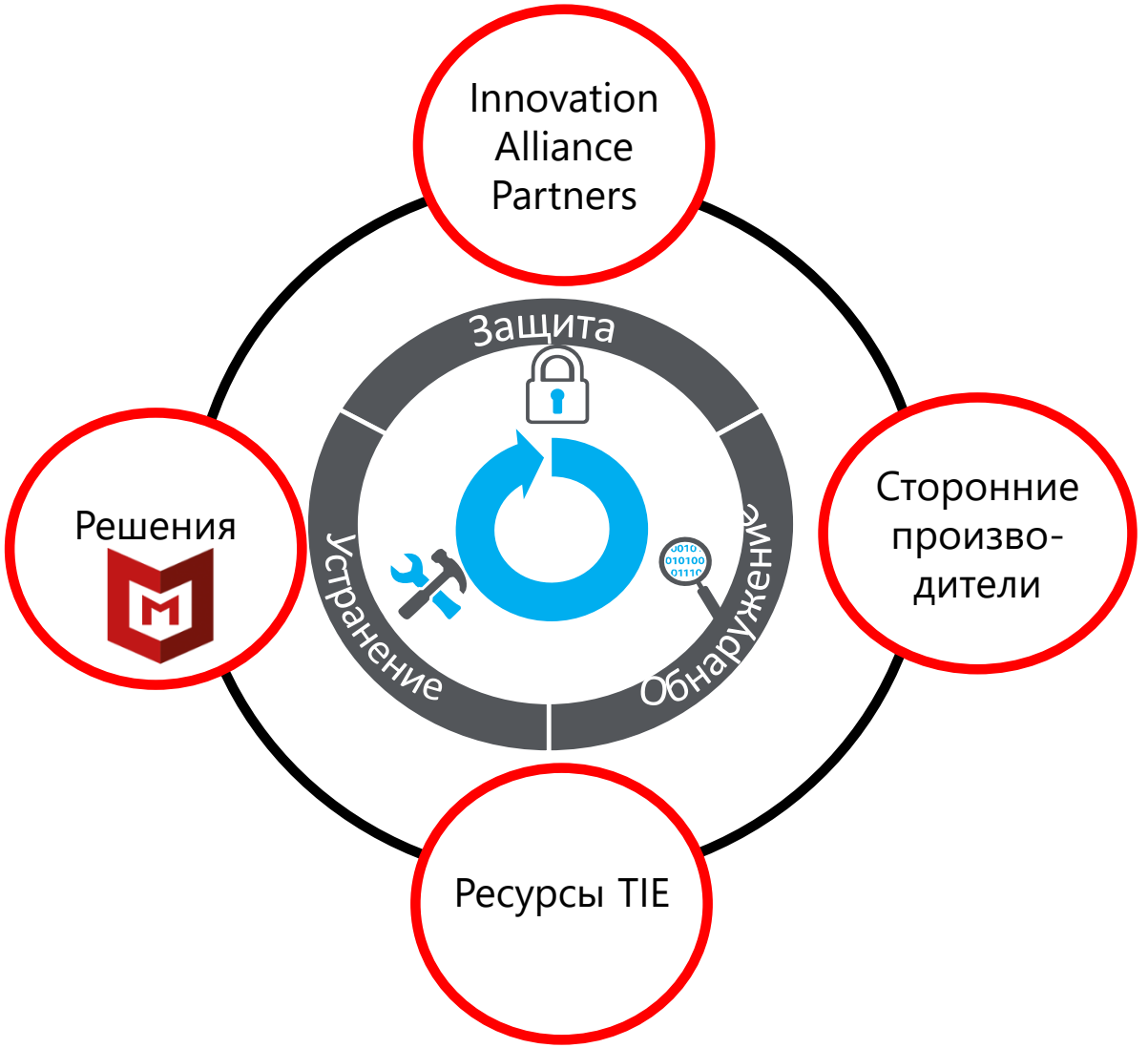
https://github.com/mohlcyber/OpenDXL-ATD-Demisto





Видение экосистемы «Адаптивная Архитектура Безопасности»

Новая эра в безопасности, где все компоненты объединяются, чтобы работать как единая сплоченная система, независимо от поставщика или базовой архитектуры



Стратегические инвестиции: взгляд на угрозы

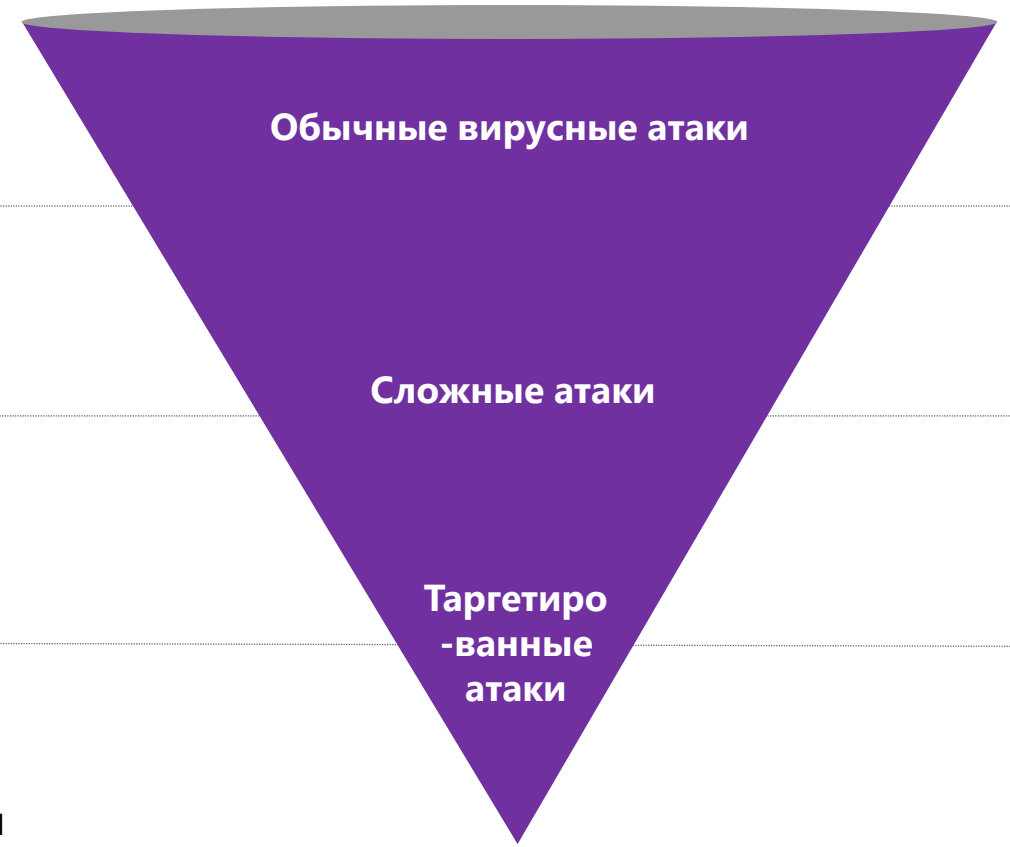
Соответствие вложений и сложности атаки

Частота

Оппортунистические
Средний ущерб
Блокирование в мсек

Целенаправленные
Большой ущерб
Устранение – месяцы

Количество



Компоненты

Традиционные средства
Традиционный сигнатурный AV, веб прокси, файрволл

Средства защиты следующего поколения
Поведенческий анализ, предотвращение эксплойтов, TI , обезвреживание

Обнаружение & Устранение
Песочницы, мониторинг процессов на эндпойнте

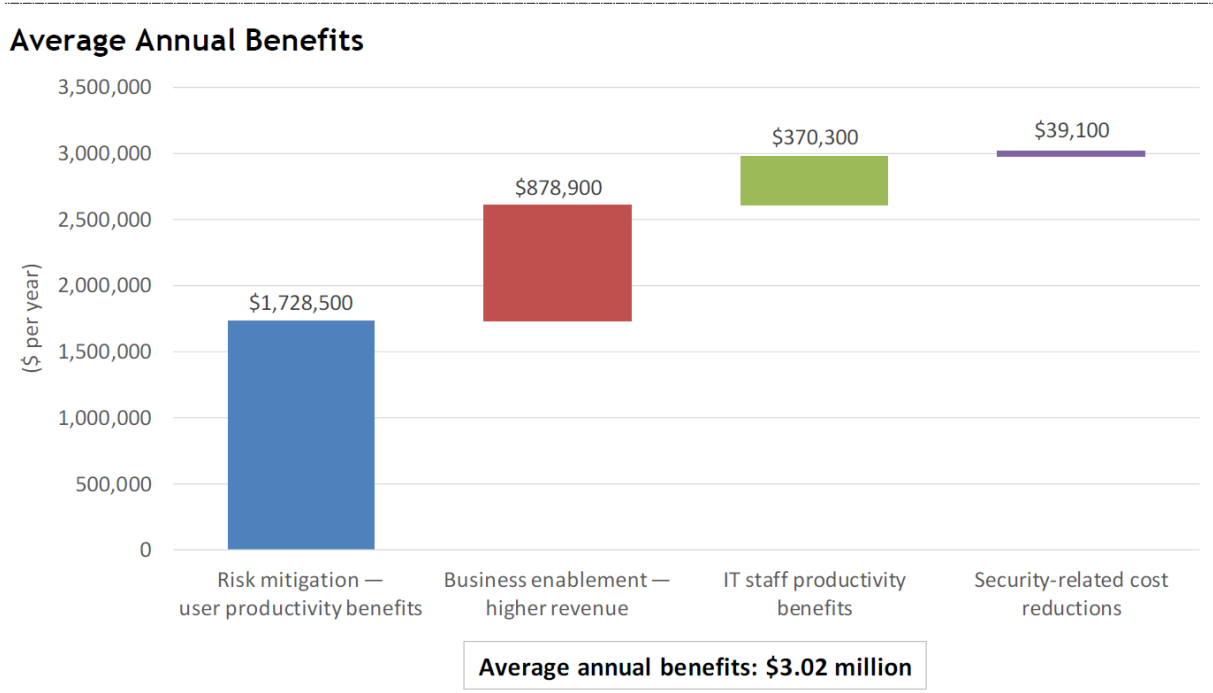
Обнаружение сложных атак
Аналитика, приоритезация, визуализация

IDC ExpertROI Spotlight Top 100 US FDIC Bank

"Мы можем обнаружить атаку в течении 60 секунд, провести анализ и ликвидировать атаку в течении 5 минут"

Решения: Endpoint, SIEM, TIE, GTI, ATD, DLP

FIGURE 1



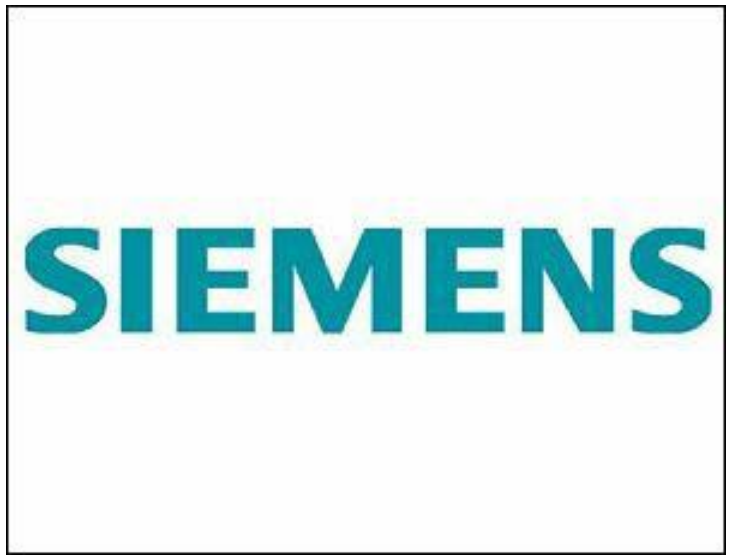
Source: IDC, 2017

- Экономия средств **$3.02 M** в год
- **ROI 208%** в течении 4 лет
- Период окупаемости **20** месяцев
- На **90%** быстрее расследование инцидентов
- На **77%** меньше инцидентов с причиненным ущербом
- На **98%** меньше времени снижение продуктивности из-за инцидентов ИБ
- **$5-10 миллионов** дополнительная прибыль
- Мониторинг всех компонентов на **1-2** консолях

Source: http://idcdocserv.com/US42210917

McAfee™
Together is power.

Защита SCADA/ICS



SCADA/ICS PARTNERSHIP

McAfee Solution Components

Essential Products

SIEMENS

Endpoint Security

ePolicy Orchestrator
Endpoint Security
Integrity Control
Device Control

SECURITY INFORMATION AND EVENT MANAGEMENT

Enterprise Security Manager

NETWORK SECURITY

Network Security Platform
Application Data Monitor

Two-way integration between McAfee components and SIA partners

Air-gap implementation for isolated systems

Support for industrial products and protocols

Flexible and expandable solutions

Virtual appliances

The Problem:
Why is Reducing Mean Time To Respond So Difficult

High Cost for More Data

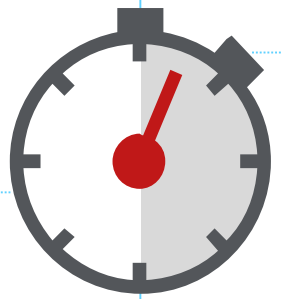
77% add 1TB+ / mo.

$$$$ to ingest more data & scale

Inefficient Manual Investigation

66% need better training for hunting

Scare expertise – Time to investigate – Inconsistent outcomes



Closed Architecture

63% of SOCs spend 10hrs/mo. customizing

Not designed to ingest at scale – poor APIs

Poor Detection Efficacy

100k+ alerts / week

False positives – Missed attacks – Triage efficiency

The Objective:
Security Operations at 30,000 Feet…. Simple Right?

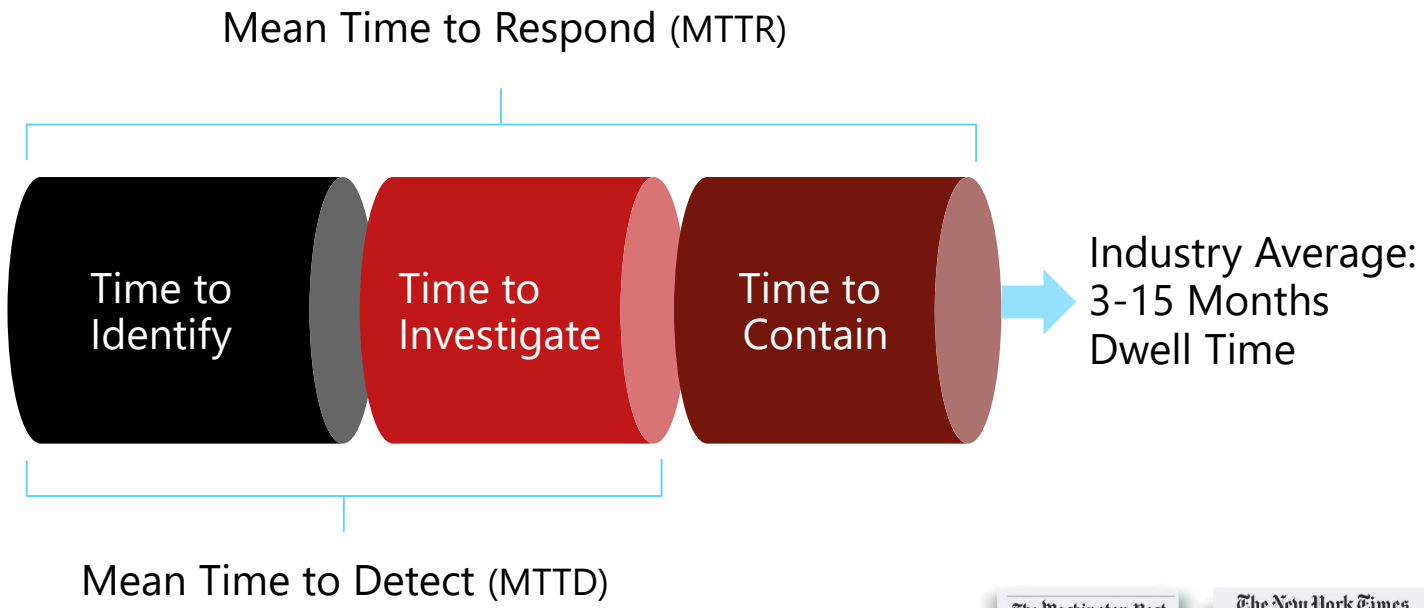
Organizations do this…

Collect and parse
relevant security data

Discover evidence
of missed attacks and determine what to pursue

Investigate to disposition
and coordinate response

…with the goal of reducing this…



…to avoid this