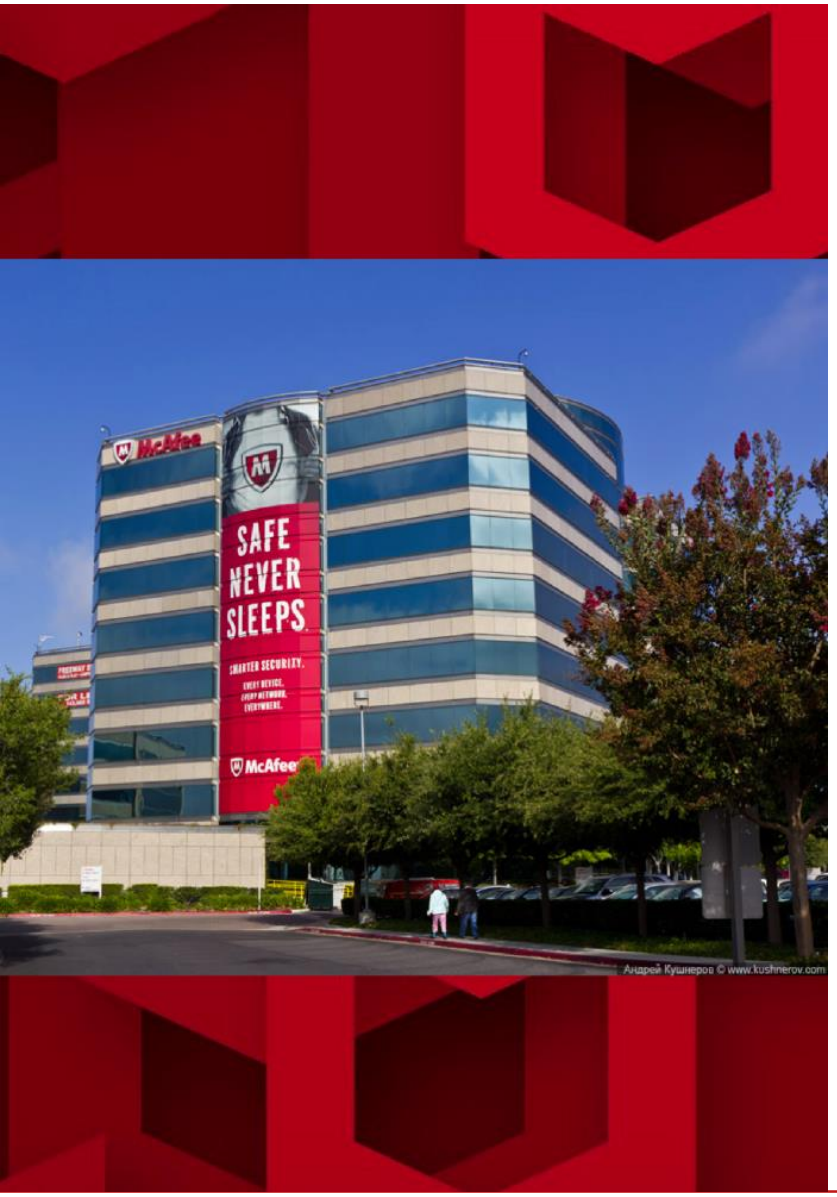
McAfee™
Together is power.

Комплексная архитектура информационной безопасности

Взгляд McAfee на современные подходы ИБ

Николай Метёлкин | Представитель McAfee

О компании McAfee



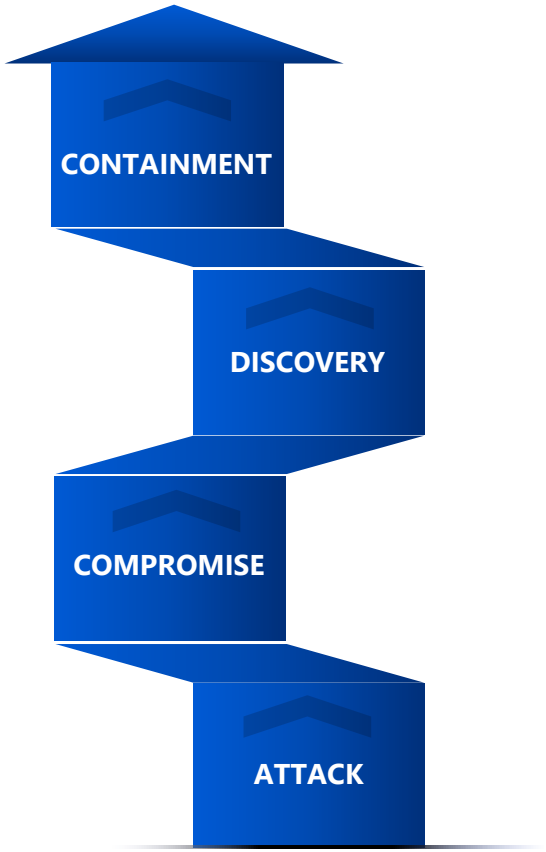
- Обеспечивает безопасность более 250 млн конечных точек
- Крупнейший в мире разработчик
- Только кибербезопасность
- McAfee GTI ежедневно появляется более 500 000 новых угроз
- В компании McAfee работает более 7 500 опытнейших специалистов по кибербезопасности
- Главный офис - Santa Clara, California

- Комплексность и эффективность
- Открытая платформа
- Портфолио
- Лидирующие позиции

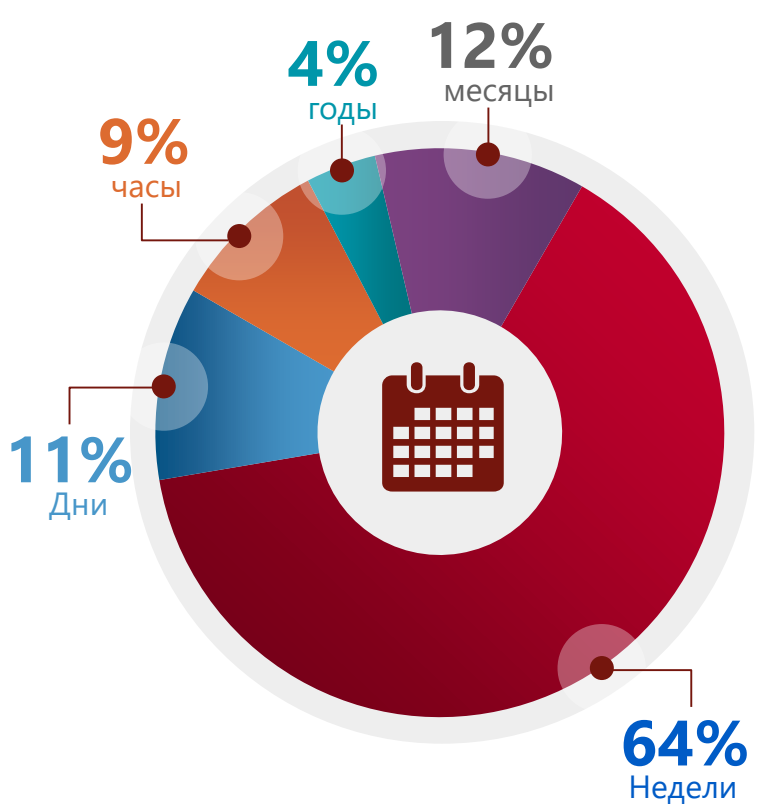
Проблематика

Целенаправленные атаки – новая реальность

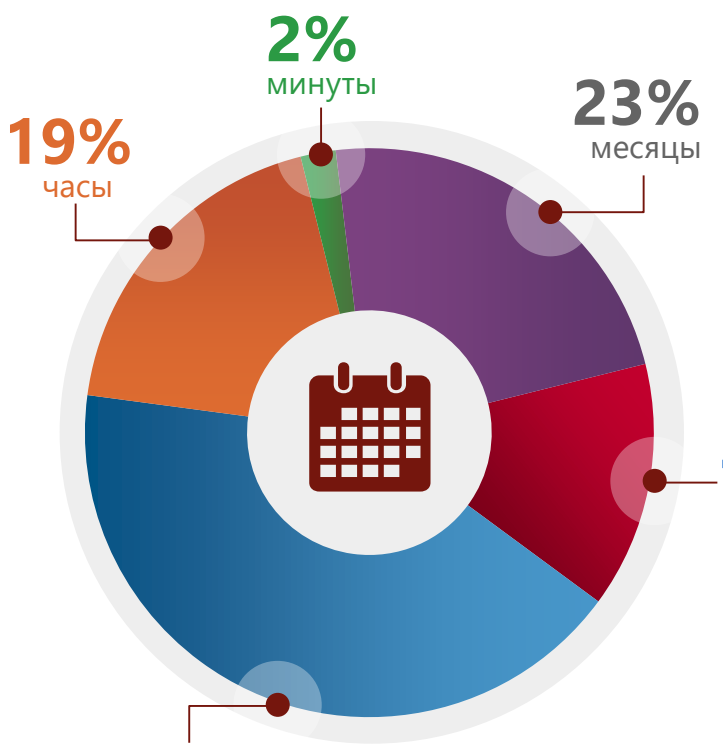
APT



Обнаружение



устранение



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

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

Проблематика

Целенаправленные атаки – новая реальность

АРХИТЕКТУРА

АВТОМАТИЗАЦИЯ

ИНТЕГРАЦИЯ

ТЕХНОЛОГИИ

ПРОЦЕССЫ

ЛЮДИ

Проблематика

Дефицит кадров в сфере кибербезопасности на уровне эпидемии

Нехватка профессионалов в области кибербезопасности влияет на возможности организаций управлять безопасностью своих все более усложняющихся информационных сетей.

82%

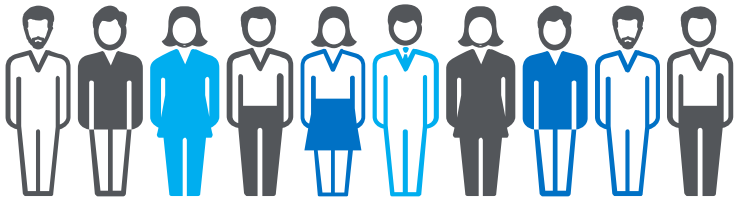
респондентов со всего мира сообщили о дефиците специалистов по кибербезопасности в своей организации *

71%

признали, что из-за недостатка кадров организации становятся более уязвимыми для злоумышленников. *

1,8 Млн.

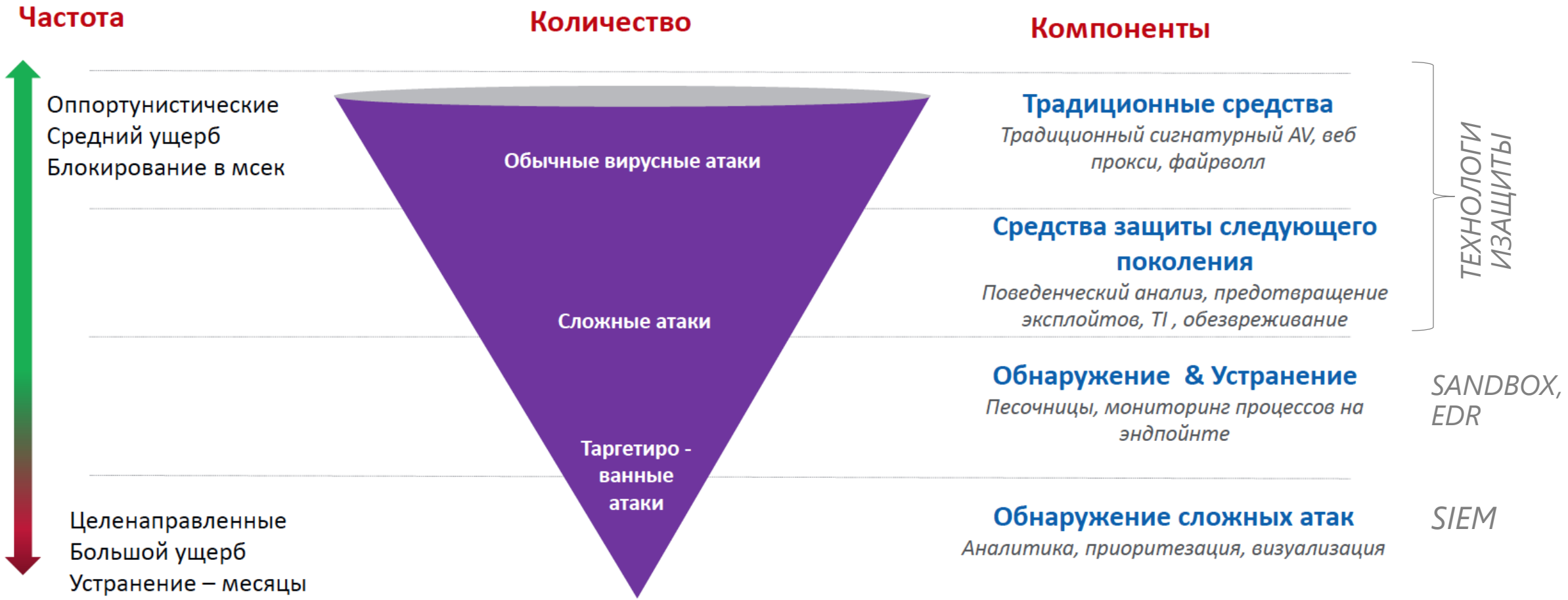
к 2022 году нехватка специалистов может достичь 1,8 миллиона человек **



- * Исследование McAfee и Центра стратегических и международных исследований (CSIS — Center for Strategic and International Studies), Hacking the Skills Shortage (Нехватка специалистов как уязвимость)
- ** Global Information Security Workforce Study, проведенный организацией (ISC)2

Стратегические инвестиции: взгляд на угрозы

Соответствие вложений сложности атаки



Позиция McAfee соответствует рекомендациям ведущих аналитиков

Verizon Report Recommendations

- Eliminate unnecessary data
- Collect, analyze, share
  - Incident data
  - Threat intelligence
- Focus on better and faster detection
- Evaluate threat landscape


What can we do about it?

Eliminate unnecessary data; keep tabs on what's left.

Ensure essential controls are met; regularly check that they remain so.

Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness.

Collect, analyze, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defense and detection.

Without deemphasizing prevention, focus on better and faster dete through a blend of people, proc and technology.

Regularly measure things like "r of compromised systems" and " time to detection" in networks. them to drive security practice

Evaluate the threat landscape t prioritize a treatment strategy. buy into a "one-size fits all" app to security.

If you're a target of espionage, underestimate the tenacity of adversary. Nor should you undere the intelligence and tools at your

Picking over the remains of breach picture of our current state, but it's have said before—we have the toc ones and using them in the right wa

To that end, we're convinced of t of understanding your enemy. If is your business, then there's a na controls on which you can focu commodity, you've got your work

knowing the attack patterns (and sharing them) can make that work more fruitful. Take steps to better understand your threat landscape and deal with it accordingly. See the Conclusion for tips on threat-centric control prioritization.

We strongly recommend readers consider the detection of failures (in a reasonable time frame) as a success. The security industry has long been overly focused on prevention


IDC Lab Validation Report

MCAFEE INTEGRATED THREAT DEFENSE SOLUTION

Essential Capabilities for Analyzing and Protecting Against Advanced Threats

By Rob Ayoub, CISSP, IDC Security Products Team

Sponsored by McAfee | March 2017

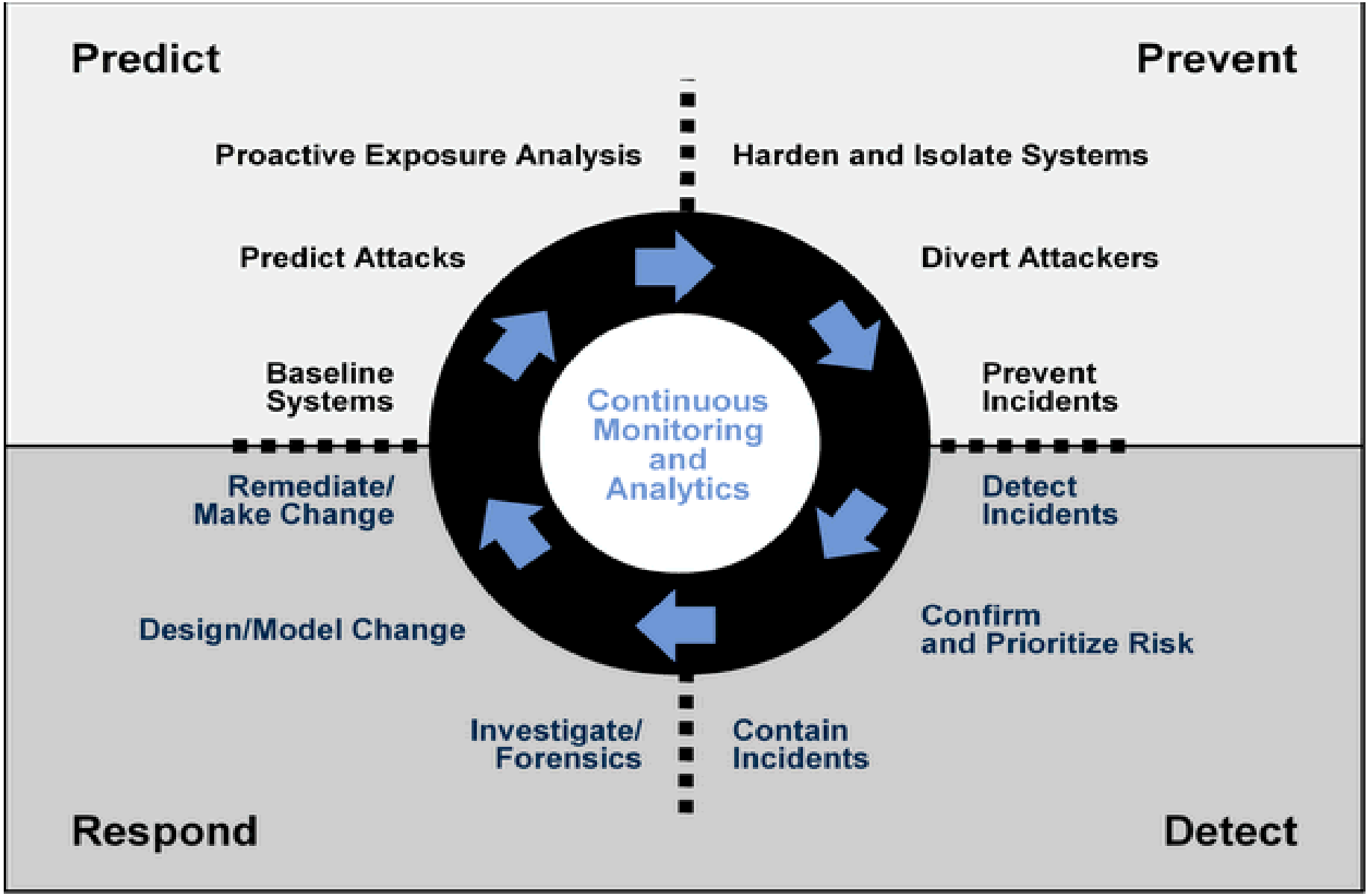
IDC Analyze the Future


Gartner

WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

The Five Characteristics of an Intelligence-Driven Security Operations Center

Архитектура Адаптивной безопасности



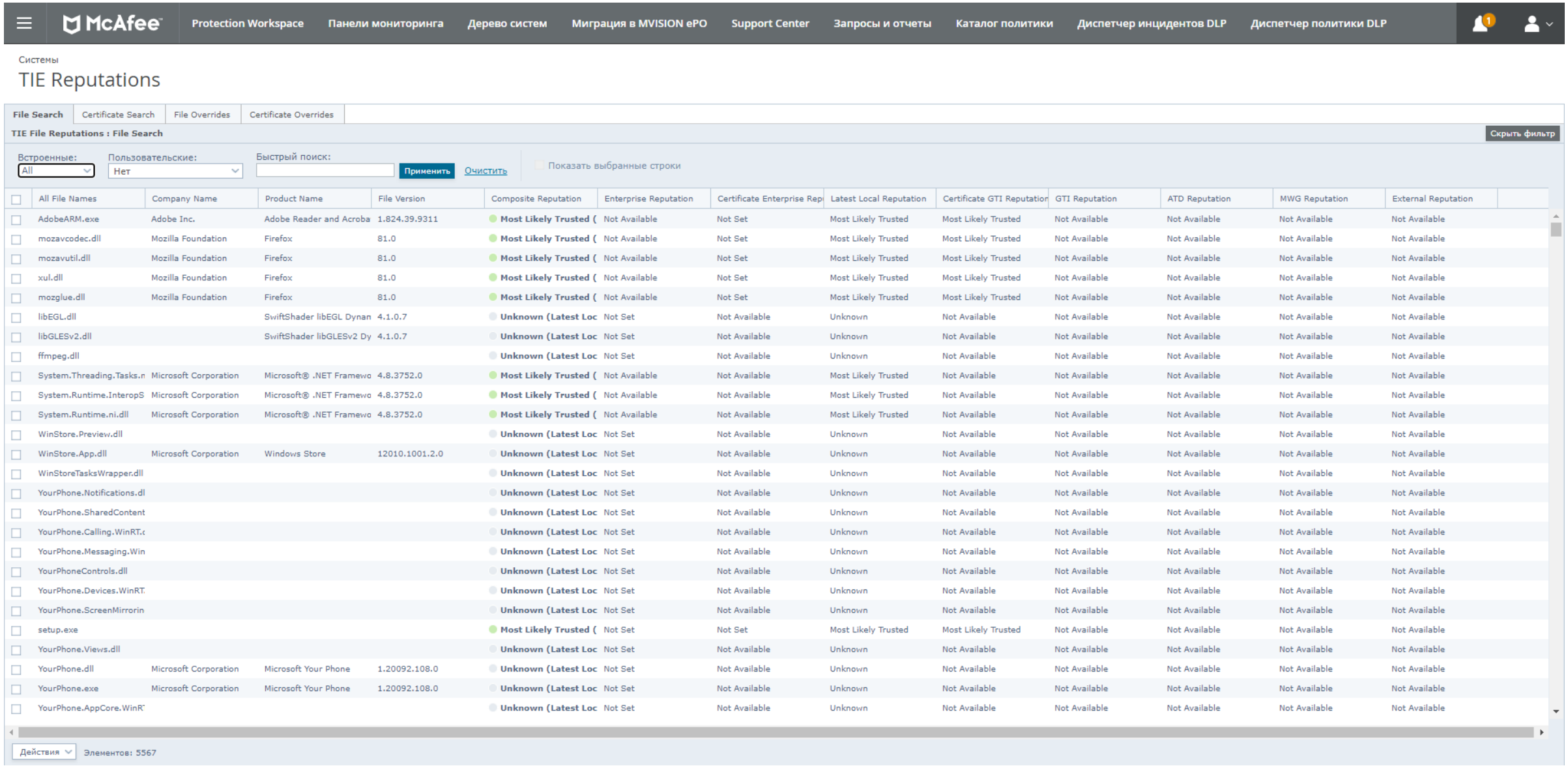
Экосистема McAfee – комплексная архитектура

Сертификация (ДССЗЗІ) продуктов McAfee в Украине

- ЗАЩИТА РАБОЧИХ СТАНЦИЙ
- ЗАЩИТА СЕРВЕРОВ
- РЕШЕНИЕ КЛАССА «ПЕСОЧНИЦА» (SANDBOX)
- ЗАЩИТА ВЕБ ТРАФИКА (Web Gateway)
- РЕШЕНИЕ КЛАССА EDR (Endpoint Detect and Response)
- УПРАВЛЕНИЕ СОБЫТИЯМИ БЕЗОПАСНОСТИ (SIEM)
- ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ И АТАК (IPS)
- ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ (DLP)
- ЗАЩИТА БАЗ ДАННЫХ
- ЛОКАЛЬНЫЙ СЕРВЕР (БАЗА) РЕПУТАЦИЙ

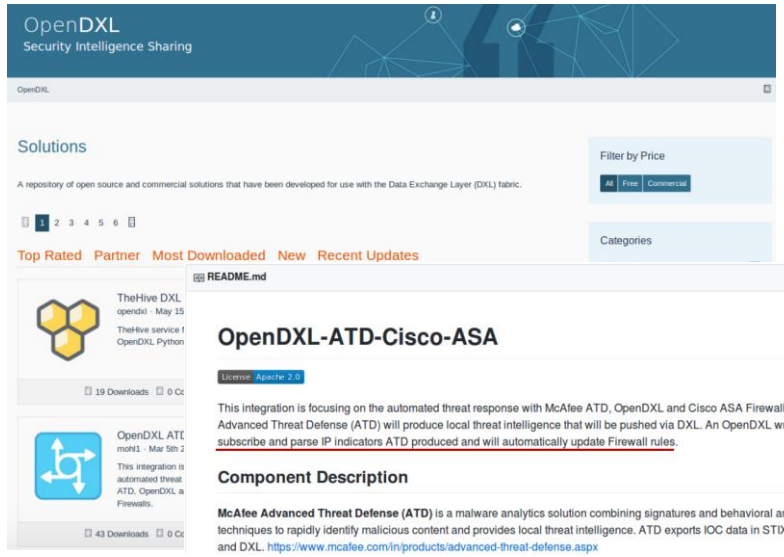
McAfee Insights

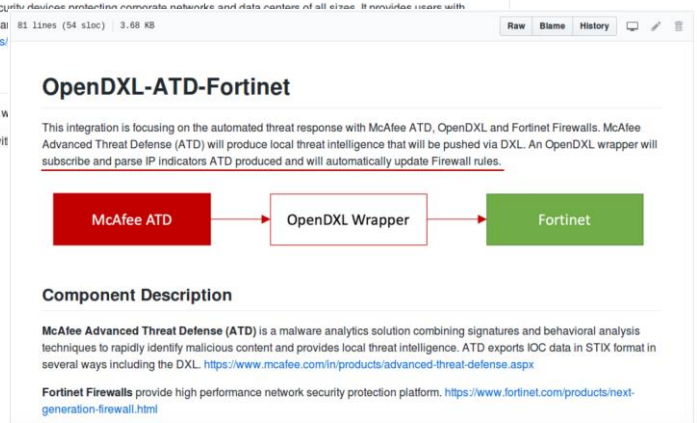
Threat Intelligence Exchange



Открытая платформа (Open DXL)

- Работа шины на передачу/получение
- Возможность интеграции с другими решениями ИБ
- Обмен IOC между решениями разных производителей
- MQTT, TLS 1.2, PKI, двухсторонняя связь





Check Point SOFTWARE TECHNOLOGIES LTD.

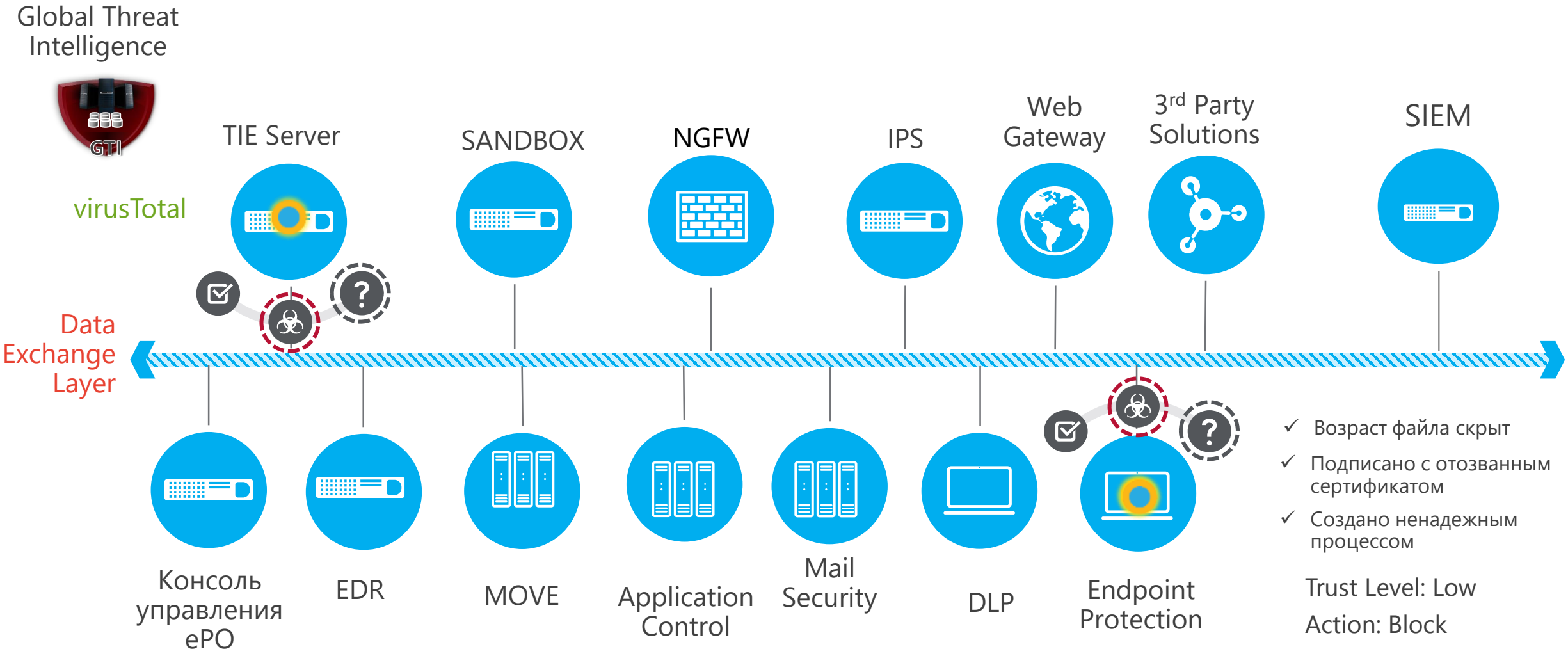
RAPID7 aruba NETWORKS CISCO FORTINET

TITUS proofpoint FORCEPOINT POWERED BY Raytheon paloalto NETWORKS

Партнеры SIA (Security Innovation Alliance)

Крупнейшая в индустрии интеграционная платформа – McAfee SIA – более 130 партнеров

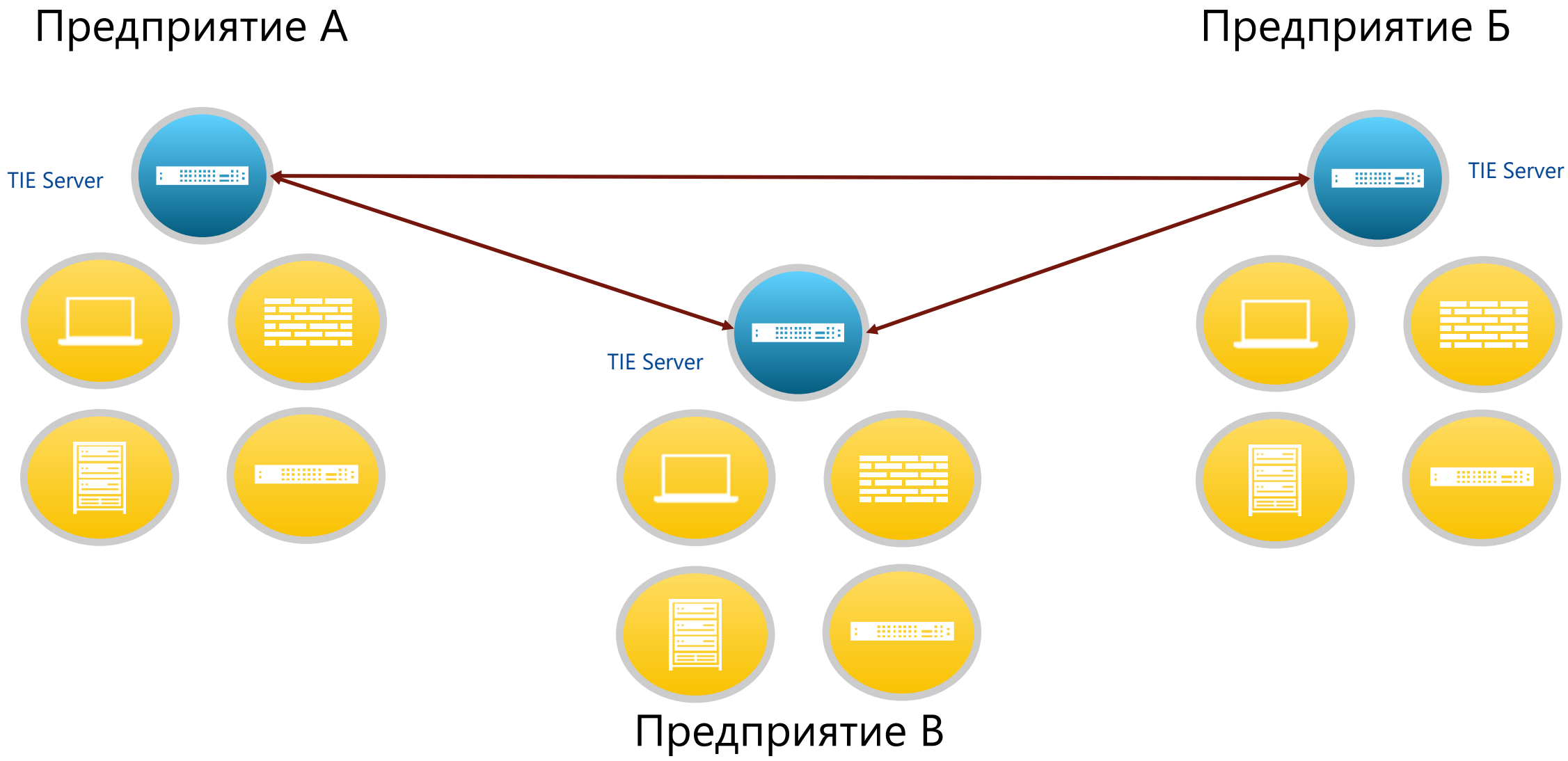
DXL – уникальное преимущество



Мгновенный обмен аналитическими данными об угрозе и анализ на связь в прошлом

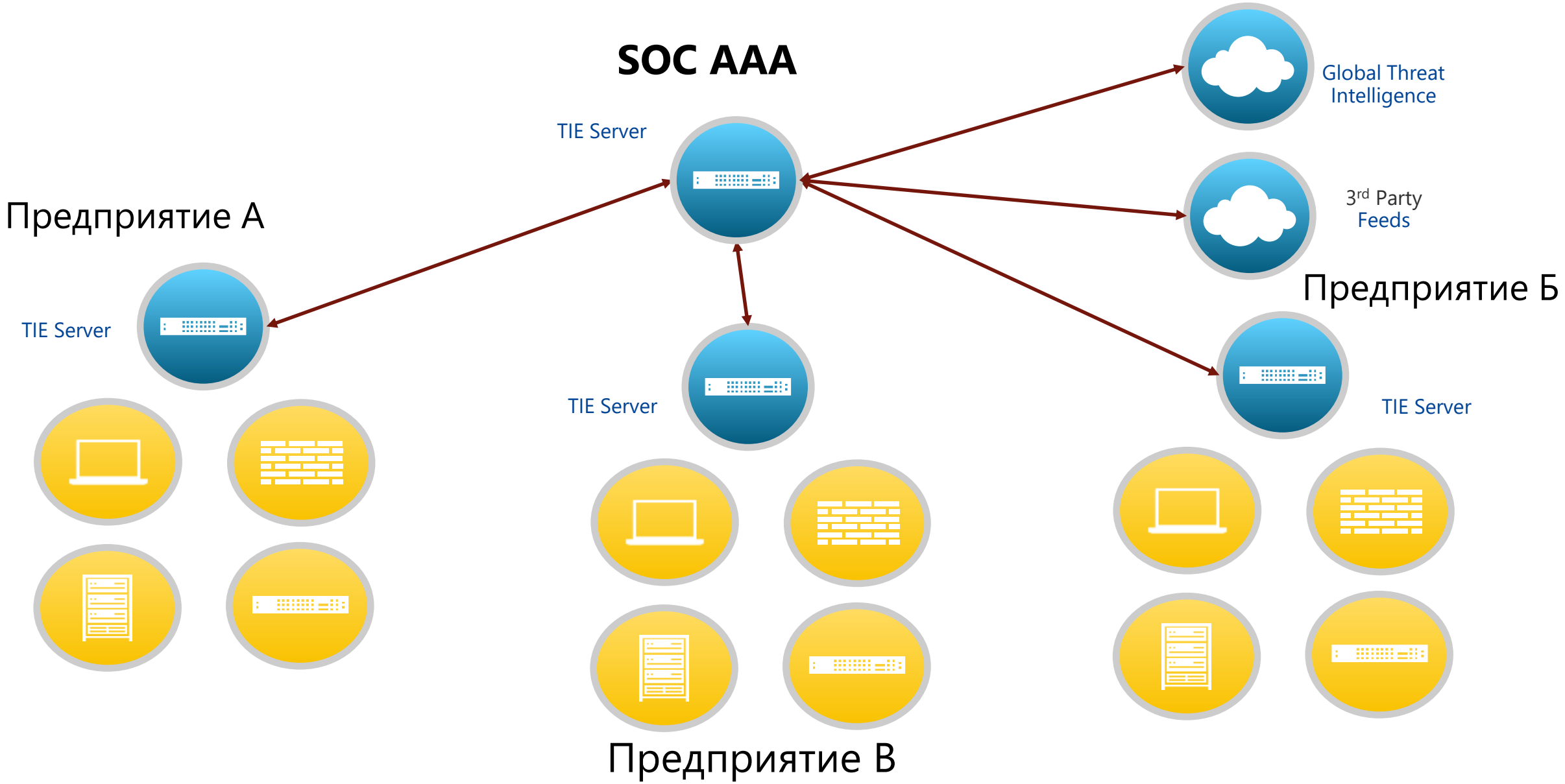
Обмен информацией о угрозах в режиме реального времени

Адаптивная защита – от обнаружения до защиты за миллисекунды



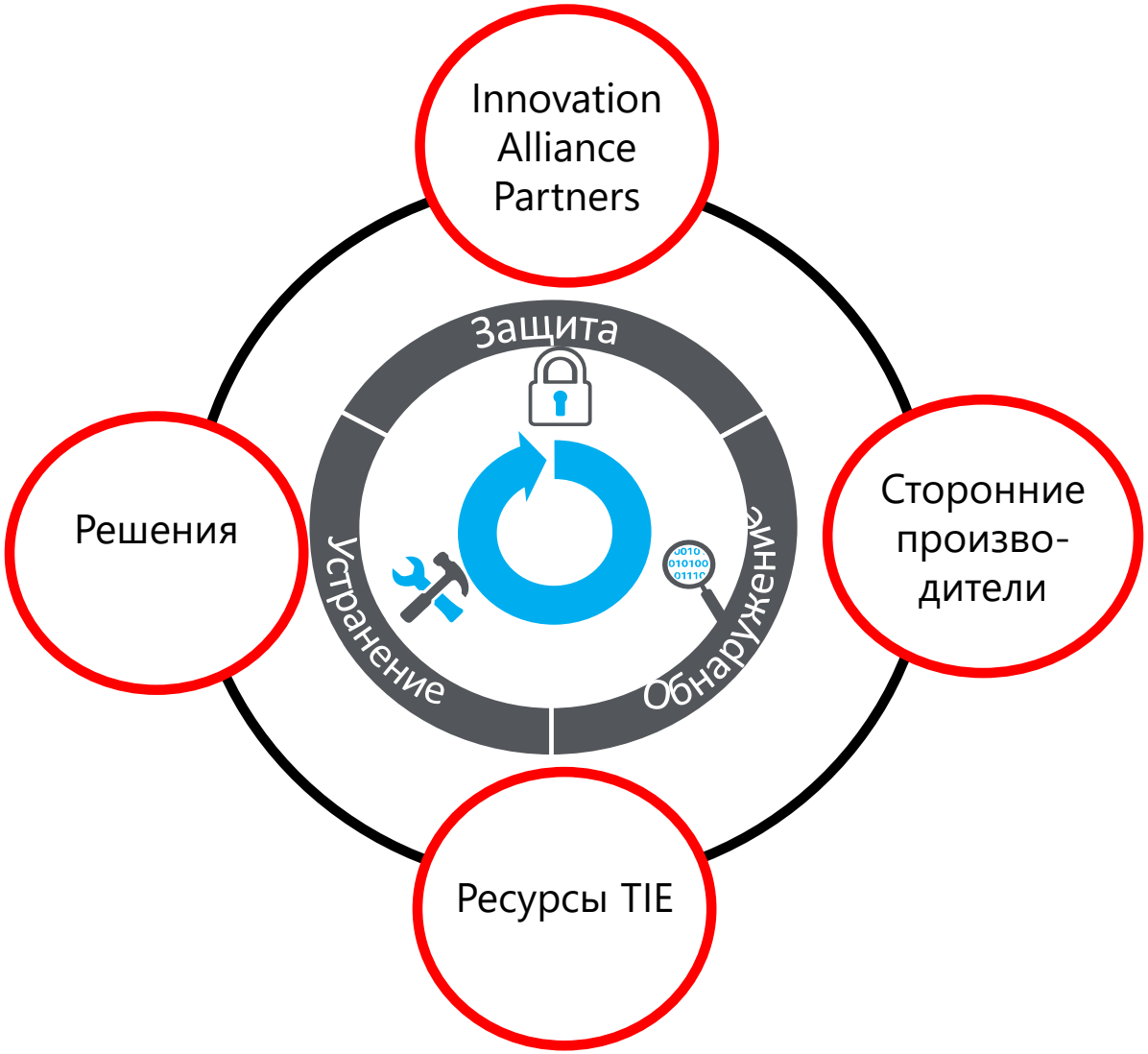
Обмен информацией о угрозах в режиме реального времени

Адаптивная защита – от обнаружения до защиты за миллисекунды



Преимущества единой экосистемы

- Снижение нагрузки на ИБ благодаря централизованному управлению
- Повышение эффективности по отражению сложных и целенаправленных атак
- Автоматизация процессов ИБ
- Снижение расходов на эксплуатацию
- Снижение репутационных и финансовых рисков



Благодарю за внимание!