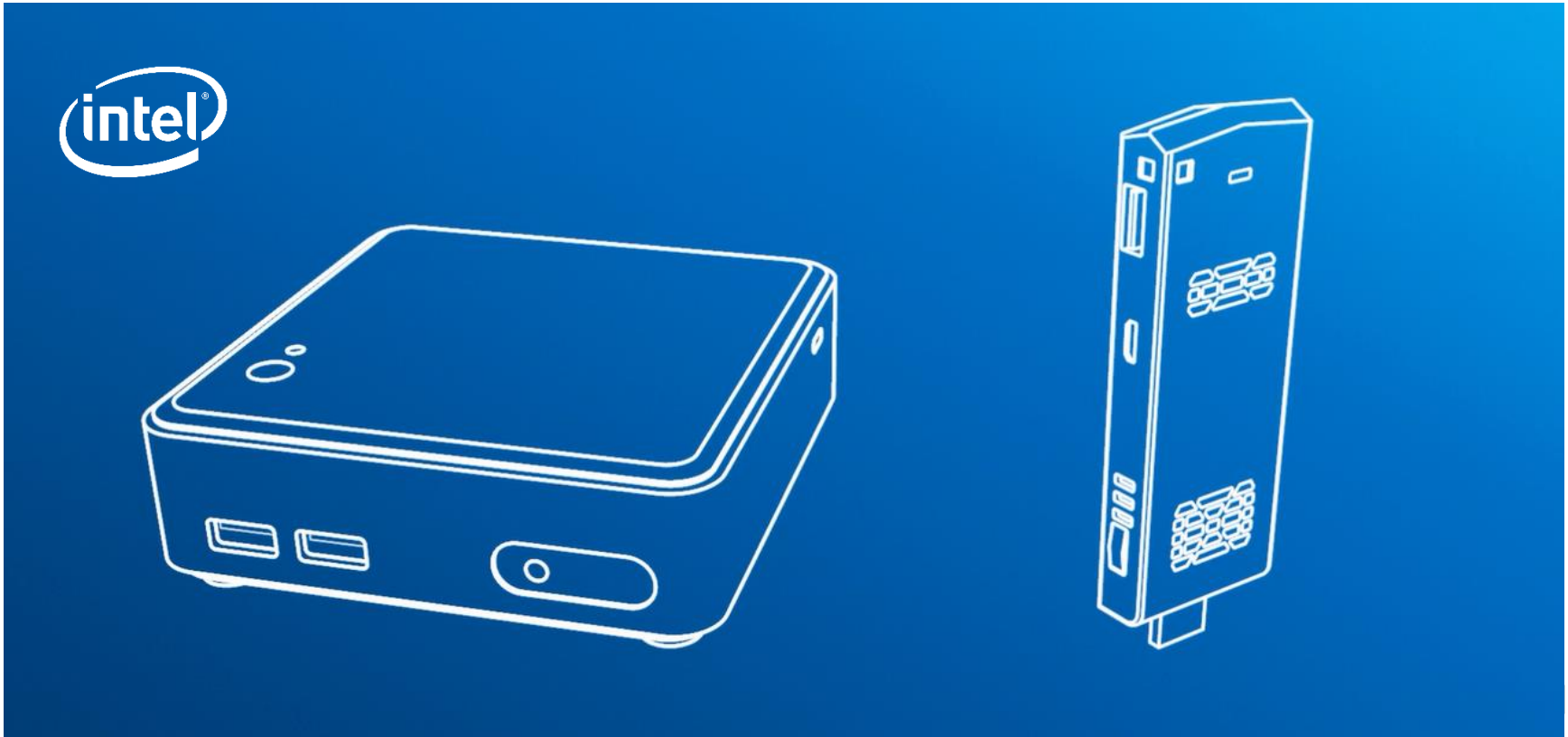
Аппаратно-программные комплексы защиты

Трансформация рабочих мест с Intel®

Компактные размеры. Возможность установки практически в любом удобном месте.



Intel® Compute Stick

Мини-ПК – Основные преимущества

ЭКОНОМИЯ МЕСТА

Windows

ВТОРАЯ ЖИЗНЬ ВАШЕГО ТВ

Совместим с любыми HDMI телевизорами/мониторами

ПРИВЫЧНОЕ УПРАВЛЕНИЕ

Просто подключи беспроводную клавиатуру и мышь

ЭКОНОМИЧНЫЙ

Потребление ниже чем у обычного ПК

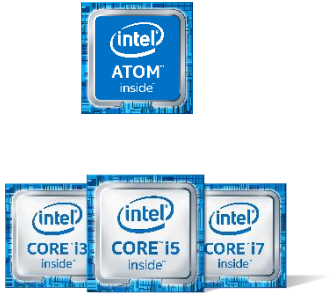
ПРОСТОй

Просто подключите и приступайте к работе

Intel® NUC

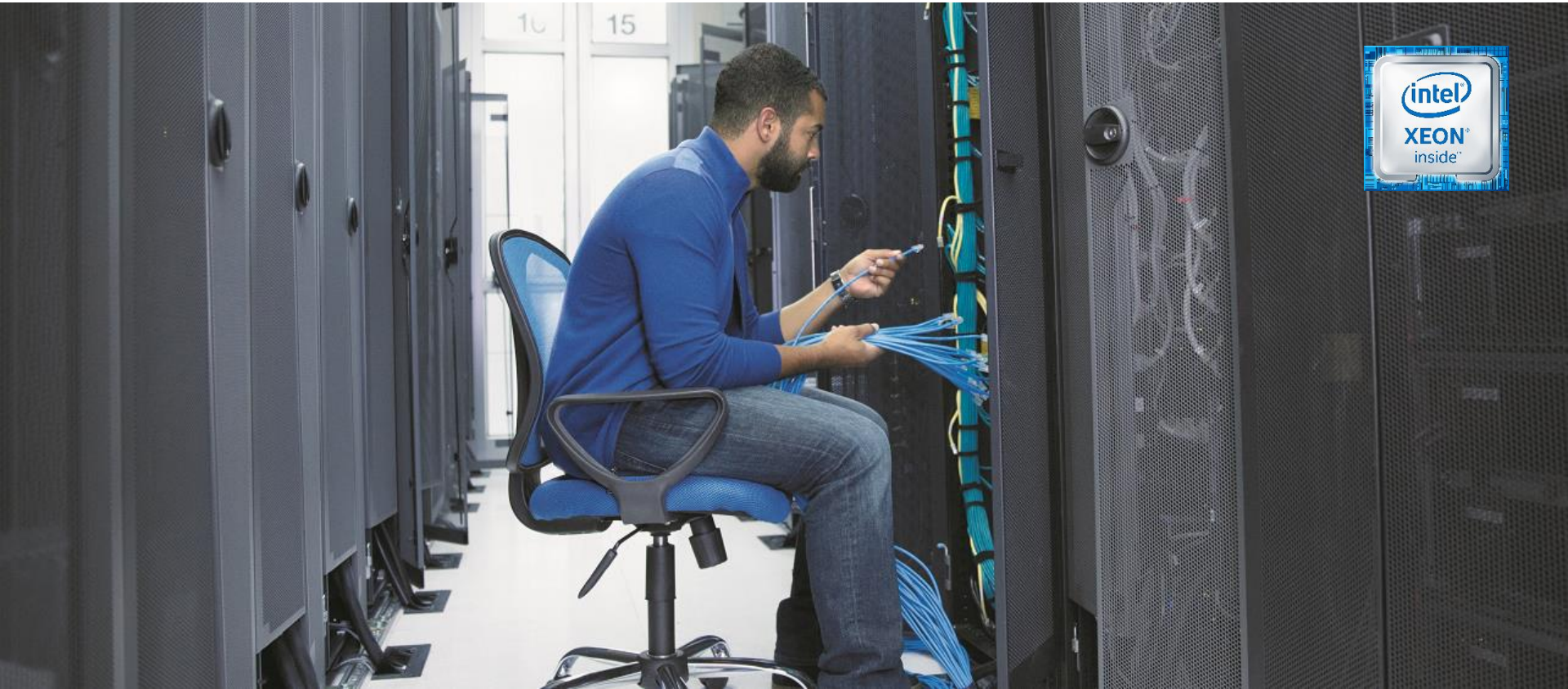
Компактный, но в то же время мощный ПК

- Мультимедиа ПК для дома
- Офисные ПК
- Цифровые вывески, электронные табло
- Интеллектуальная торговля
- Электронные киоски продаж



Серверные решения Intel®

Семейство процессоров Intel® Xeon®



intel Security

Как защитить «гибридную» инфраструктуру?

Безопасное облако. Для тех, кто строит, для тех кто использует

Дата центры меняются!

Дата центры должны предоставлять больше и больше услуг. Быстрее, чем раньше

200%

Затраты на услуги Public Cloud удвоятся с 2015 по 2020[1]

78%

от вычислений будут обрабатываться в облаках к 2018[3]

40%

Всех данных будут храниться или обрабатываться в облаках к 2020[2]

54%

Совокупный среднегодовой темп роста инвестиций (CAGR) SDN* и NFV** к 2020[4]

*Software-Defined Network
**Network Function Virtualization

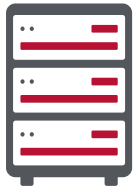
1. IDC, *Worldwide Public Cloud Services Spending Forecast to Double by 2019,* January 2016
2. IDC, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in Far East. Dec. 2012
3. Cisco Global Cloud Index: Forecast and Methodology, 2013-2018.
4. SNS Research, 2015-2020, Dec.2015

Безопасность DC тоже должна измениться

Увеличение площади атаки приводит к большему количеству взломов

60%

Взломов, приведших к компрометации, были осуществлены в течении минут[1]



40%

Атак направлены на сервера[3]

82%+

Компаний не знают объём неконтролируемого IT в организации[2]

75%

Сервис-провайдеров сталкивались с атаками на HTTP и DNS[4]

Средняя стоимость утечки данных (в мире): $3.79M — рост на 23% с 2013[5]

Sources:

1. Verizon 2015 Data Breach Investigations Report
2. Cloud Adoption Practices & Priorities Survey, January 2015.
3. *Verizon 2013 State of the Enterprise Cloud Report*
4. Arbor Networks Application-Layer Attacks report, 2014
5. Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis, 2015*

Важнейшие цели IT для безопасности

Наглядность состояния безопасности по всей инфраструктуре

- Полная видимость для рабочих нагрузок и данных, как внутри корпоративного центра обработки данных, так и в публичном облаке
- Уверенность, что бизнес защищен и соответствует требованиям проверяющих

Обнаруживать взломы и нарушения опасные для бизнеса

- Способность обнаруживать даже сложные направленные атаки
- Управляемость уровнями рисков в соответствии с угрозами по всей компании
- Обнаруживать угрозы раньше и устранять их быстрее

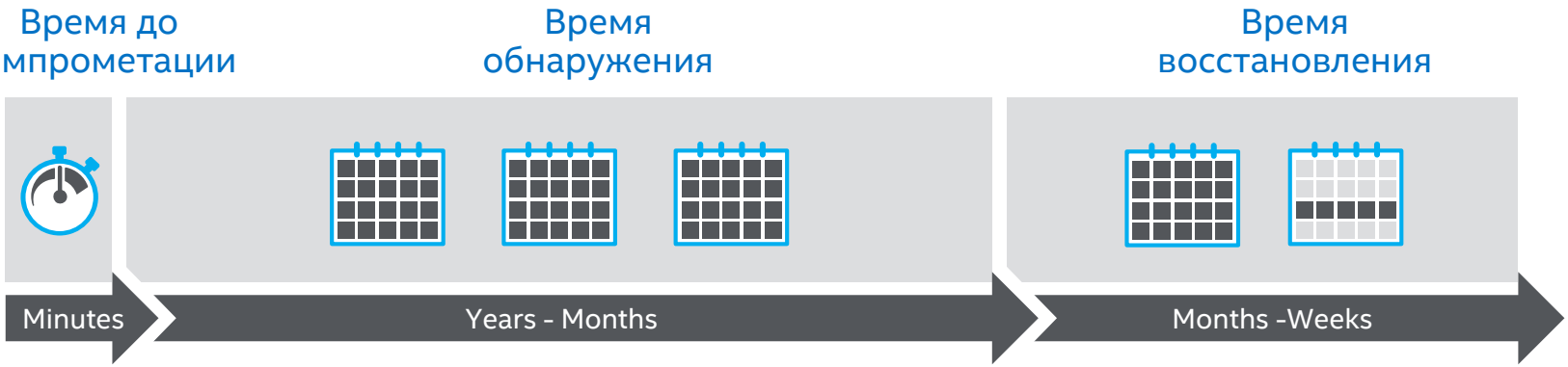
Восстановить любой ущерб который может быть нанесён

- Реагировать быстро и эффективно, ограничивать возможный ущерб

IT безопасность теперь волнует и ТОП менеджеров

CIOs и CISOs находятся под давлением руководства

Существующая реальность

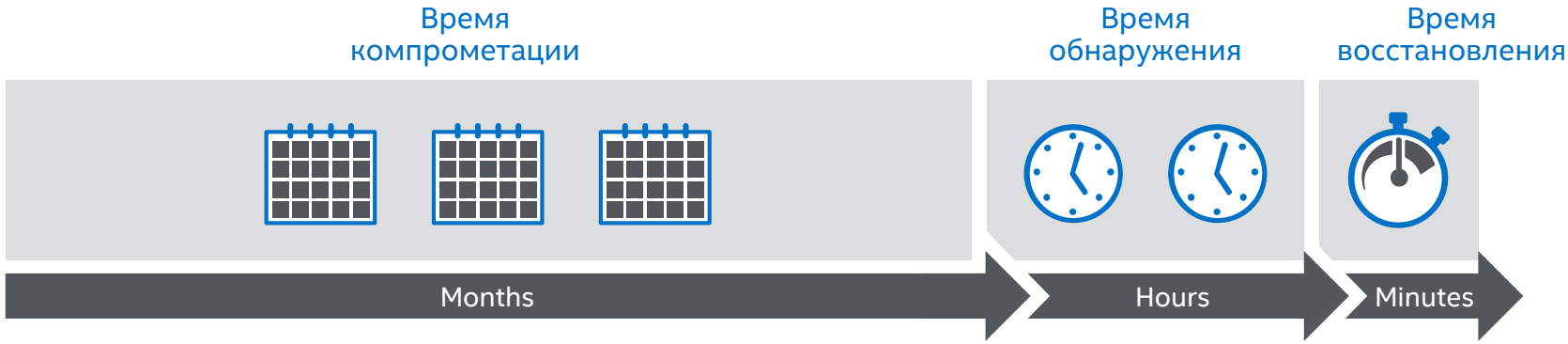


Недостаточные усилия по предотвращению

Группы IT безопасности разбиты

Катастрофические последствия $$$

Правильный подход. Результаты для Бизнеса



Достаточные усилия по предотвращению

Оптимизированные команды IT безопасности

Минимальный ущерб

Основные вызовы перед IT для безопасности «Гибридных облаков»

Отсутствие наглядности по всем вычислительным ресурсам на территории и за пределами

- Использование публичных и приватных облаков, так называемый «Shadow IT» делают наглядность использования ресурсов невозможной, а аудит затруднённым.
- У контролирующих и проверяющих органов возникнут вопросы. Нужно быть готовым

Трудности в обнаружении взломов и восстановлении урона

- IT сложно понять и спрогнозировать как угрозы становятся взломами

Отсутствие единого управления и отчётности по всей инфраструктуре и данным

- Облачная инфраструктура, которая не находится в собственности или в ведении бизнеса
- Нагрузки и корпоративные данные в публичном облаке

Решение Intel Security

McAfee Network Security Platform

- IPS для физических и виртуальных сетей software-defined infrastructure (SDI)

McAfee Server Security Suites

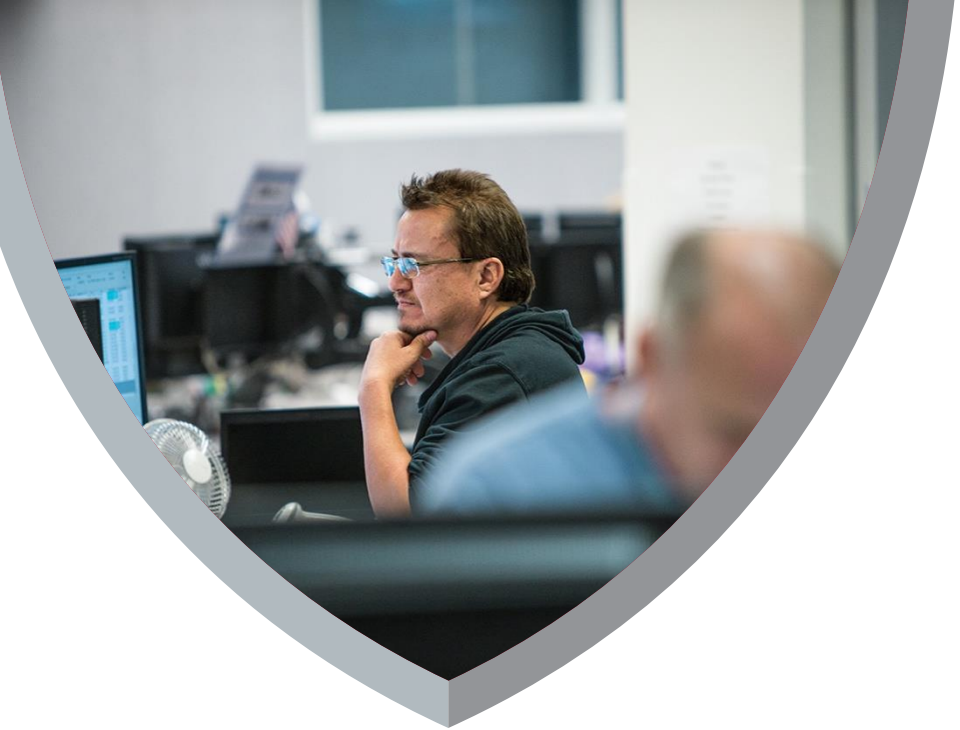
- Защита серверов. Физических, виртуальных и в облаке.

Database Security

- Защищает базы данных от угроз внешних, внутренних и системных

Threat Intelligence Exchange (TIE)

- Включает адаптивное обнаружения угроз в режиме реального времени

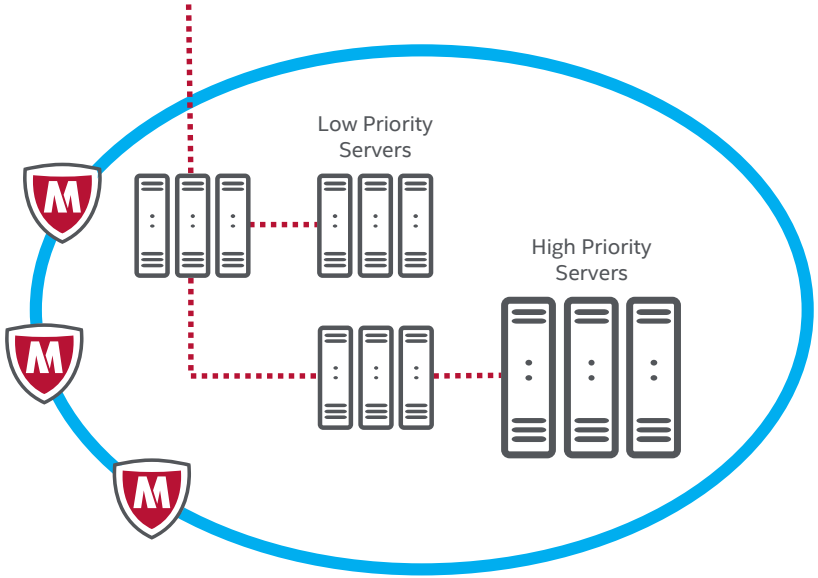


Network Security Platform

Классическая безопасность периметра одна не останавливает взломы

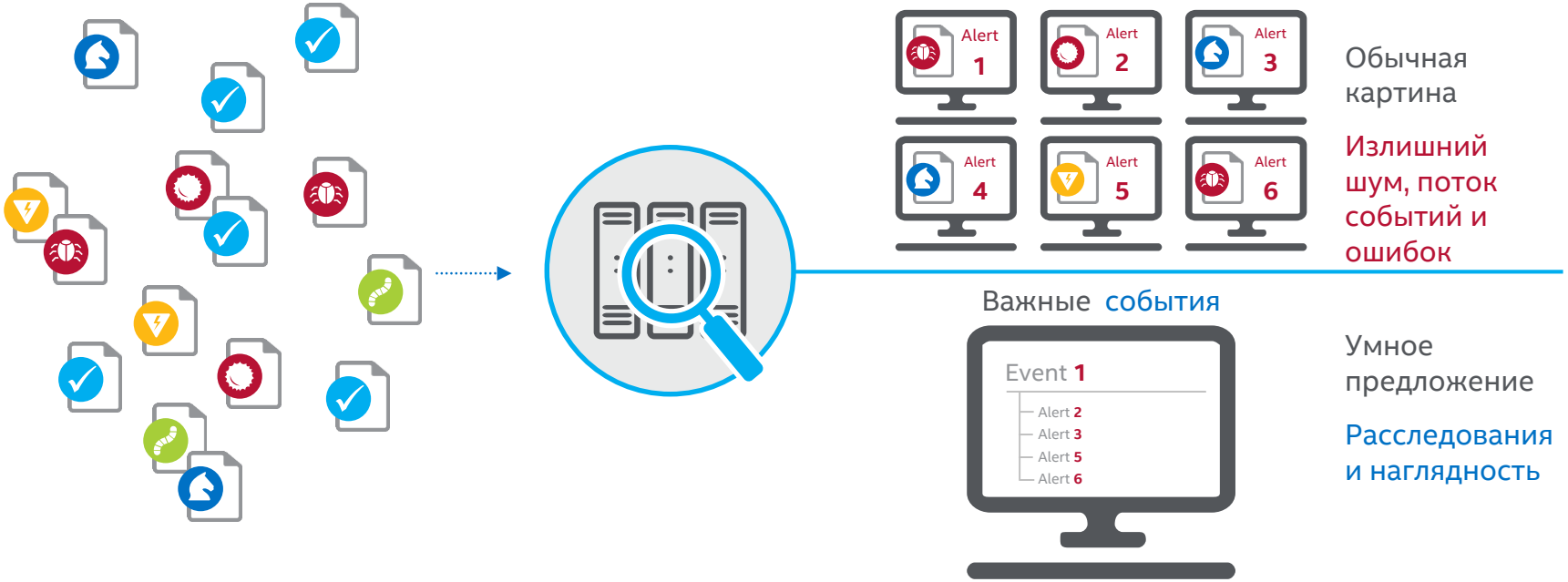
Внутренний контроль часто недостаточен

- Сильная защита периметра как правило стандартна
- Сложные угрозы находят сервера с низким приоритетом
- Угрозы распространяются с сервера на сервер



Определение взломов быстрее

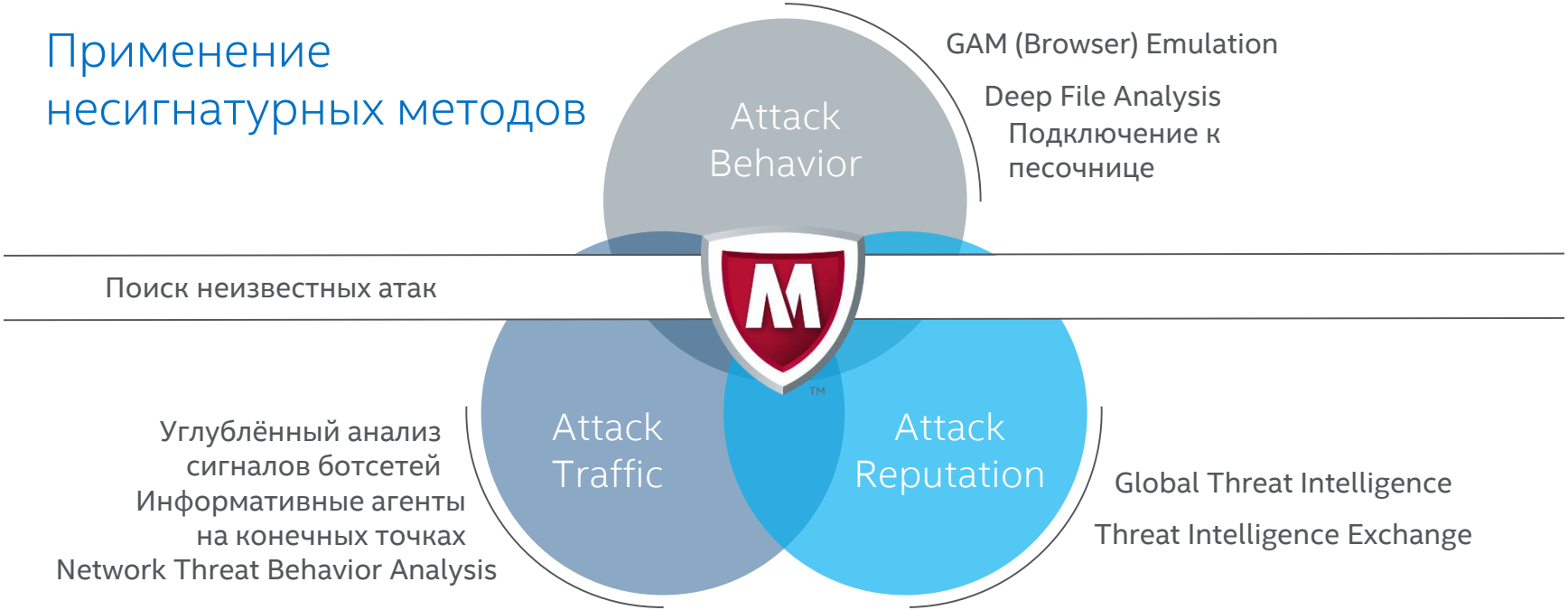
Реальные процессы



Как защитить Data Center периметр

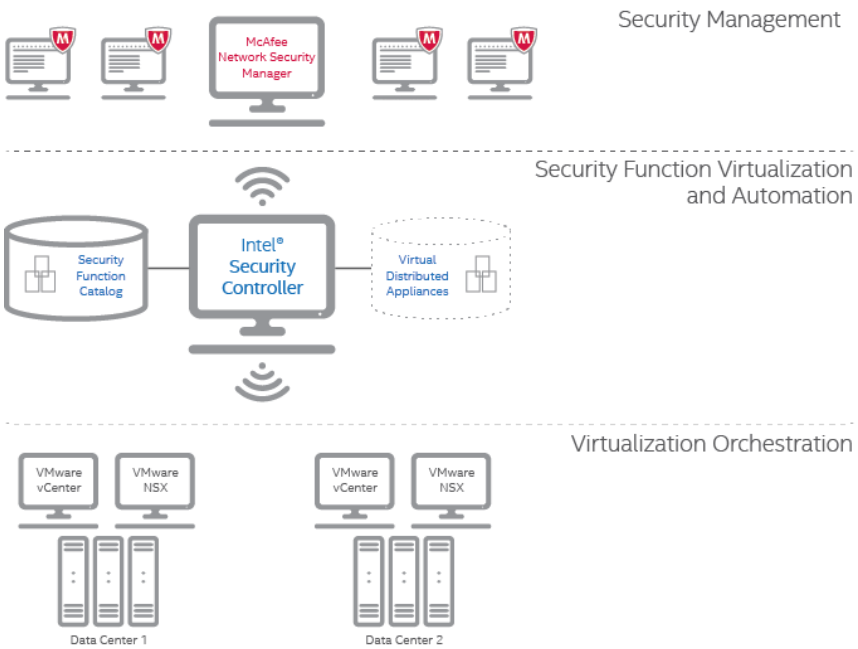
Network Security Platform (NSP)

Применение несигнатурных методов



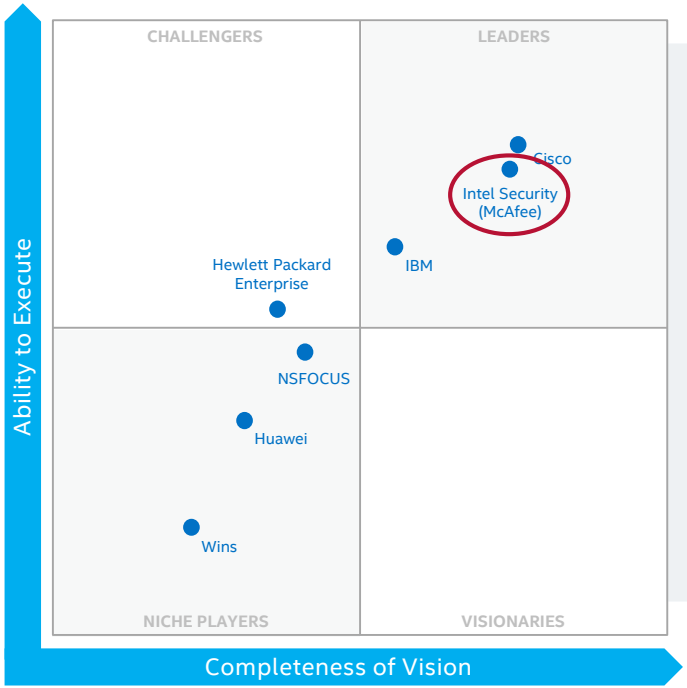
Защита VMware NSX Data Centers с помощью Next-Generation IPS

Intel Security и VMware анонсировали интегрированное решение для автоматизации и ускорения Advanced Security Services



- Полная интеграция с Vmware vCenter с поддержкой сегментации, профилей безопасности, политик и групп.
- Защита внутреннего VM-трафика в рамках VMware NSX data center. Или нескольких датацентров.
- Первый IPS, оптимизированный для архитектуры Intel с использованием технологии Intel® Xeon ™ для Intel® HyperScan и комплект Intel® Data Plane Development (Intel DPDK)

Дружите с лидерами в Network Security



9 Раз без перерыва размещён в квадранте лидеров GARTNER:

“ **Множество применяемых несигнатурных технологий** даёт несомненное преимущество над сигнатурными IPS технологиями.”

“ Клиенты оценивают **управляемость и лёгкость использования** как чрезвычайно хорошую.”

“ **Указан как главный конкурент** согласно опросу конкурентов.”

Gartner 2015 IPS Magic Quadrant

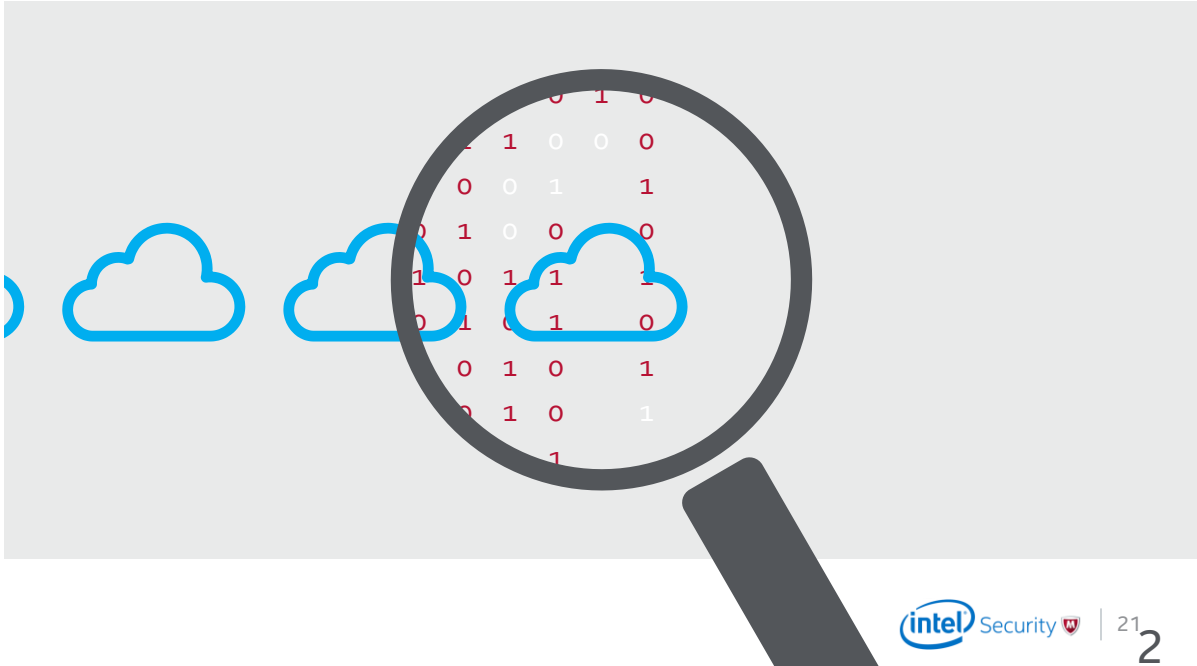
Server Security

Три проблемы для безопасности в «облаке»

1. Наглядность/Понятность

Отсутствие понимания что же внутри облака

- Теневой IT: пользователи ходят в облака напрямую
- Старые VM в заброшенном состоянии или стали «зомби»
- Безопасность не может идти в ногу с авто-масштабированием веб-приложений



Три проблемы для безопасности в «облаке»

2. Защита

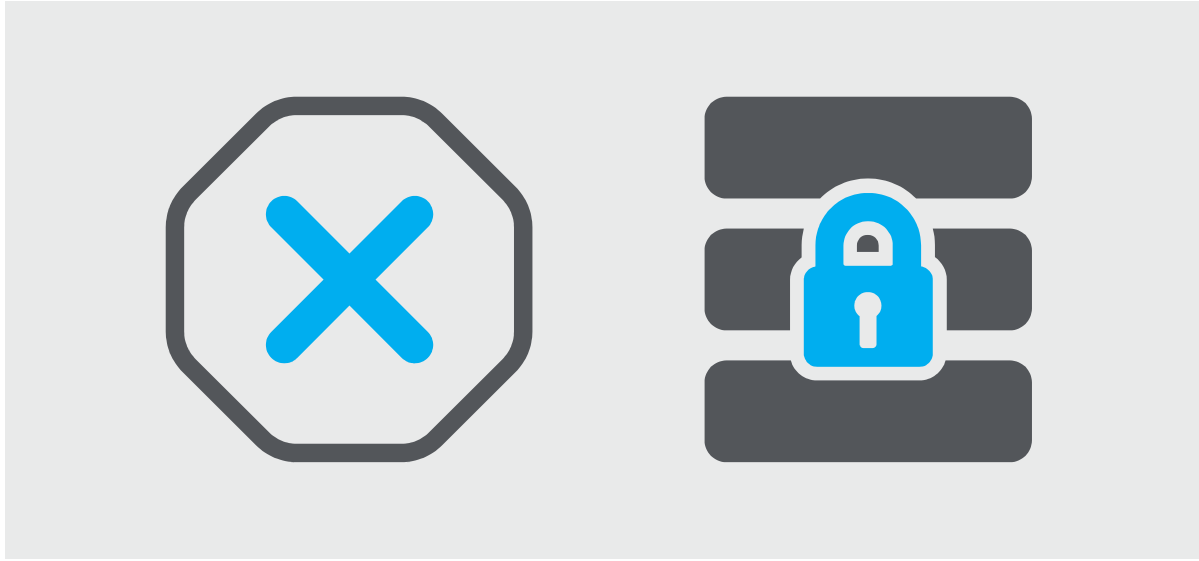
Нужно усовершенствованное средство предотвращения угроз и защиты данных

Предотвращение угроз

- Network Security не спасает
- Постоянные атаки ботнетами

Приватность данных

- Шифрование является главным требованием безопасности в публичном облаке
- Защита от несанкционированного доступа



Защита от несанкционированного доступа

3. Управляемость

Сложность управления двумя отдельными системами

- Большие затраты
- Ограниченные ресурсы
- Сложность

McAfee Public Cloud Server Security Suite

- Наглядность для всей среды
- Надёжная защита
- Централизованное управление

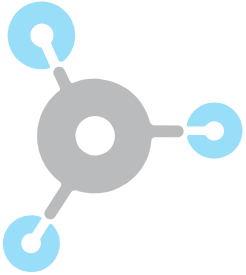
McAfee Public Cloud Server Security Suite

Наглядность

Работает непосредственно на серверах в облаке и в организации

Protection

Same world-class technologies as physical server solutions



Management

Single pane of glass for automated management

Коннектора к «облакам» в McAfee ePO

Cloud Connectors for McAfee ePO

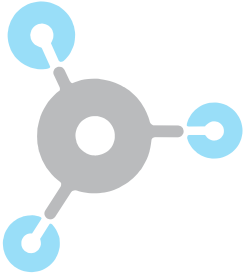
McAfee Public Cloud Server Security Suite

Visibility

Immediate insights into cloud-based and on-premise servers

Защита

Те же технологии как для защиты физических серверов



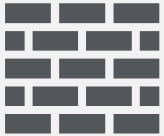
Management

Single pane of glass for automated management

Хорошего качества Антивирус, Firewall, IPS и защита данных для Windows & Linux

Защита как для Windows так и Linux

ANTI-VIRUS



FIREWALL

INTRUSION PREVENTION

APPLICATION WHITELISTING

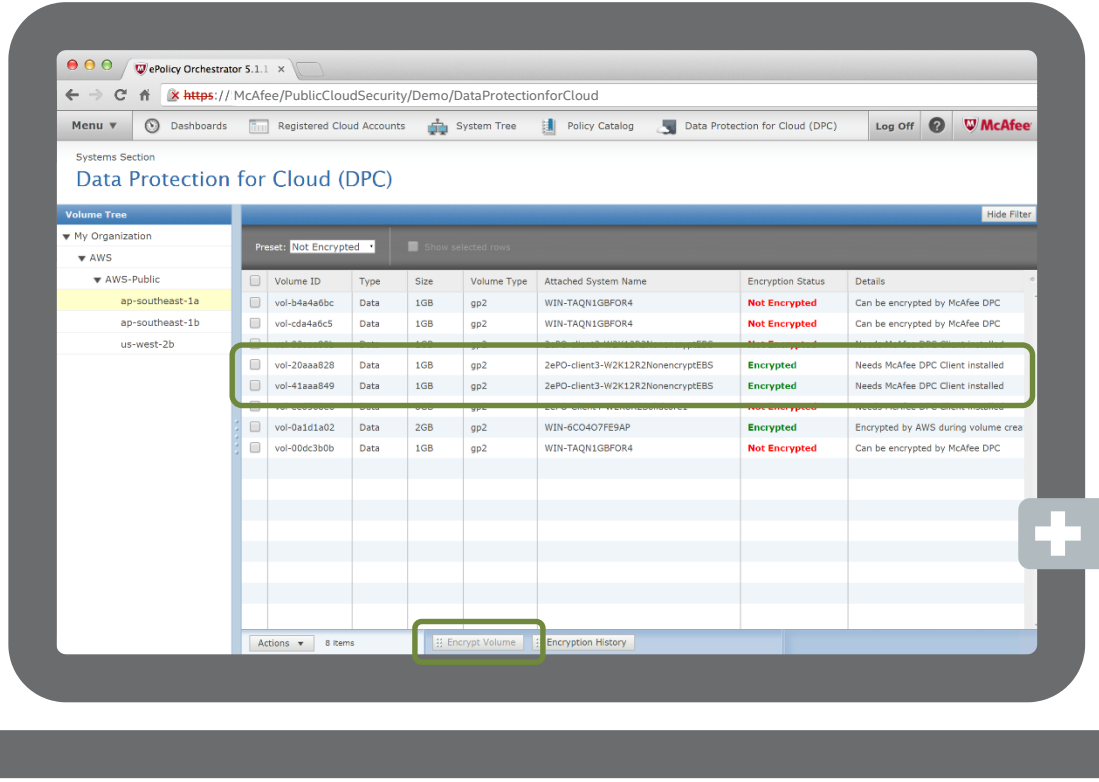
INTEGRITY MONITORING

ENCRYPTION MANAGEMENT

DevOps-friendly deployment

Как защитить данные в «облаке»

- Определение статуса шифрации для томов
- опции по шифрованию созданных томов в 1 клик
- Интергация с Amazon Key Management Service (KMS)



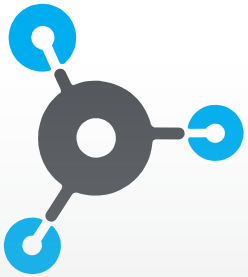
McAfee Public Cloud Server Security Suite

Visibility

Immediate insights into cloud-based and on-premise servers

Protection

Same world-class technologies as physical server solutions



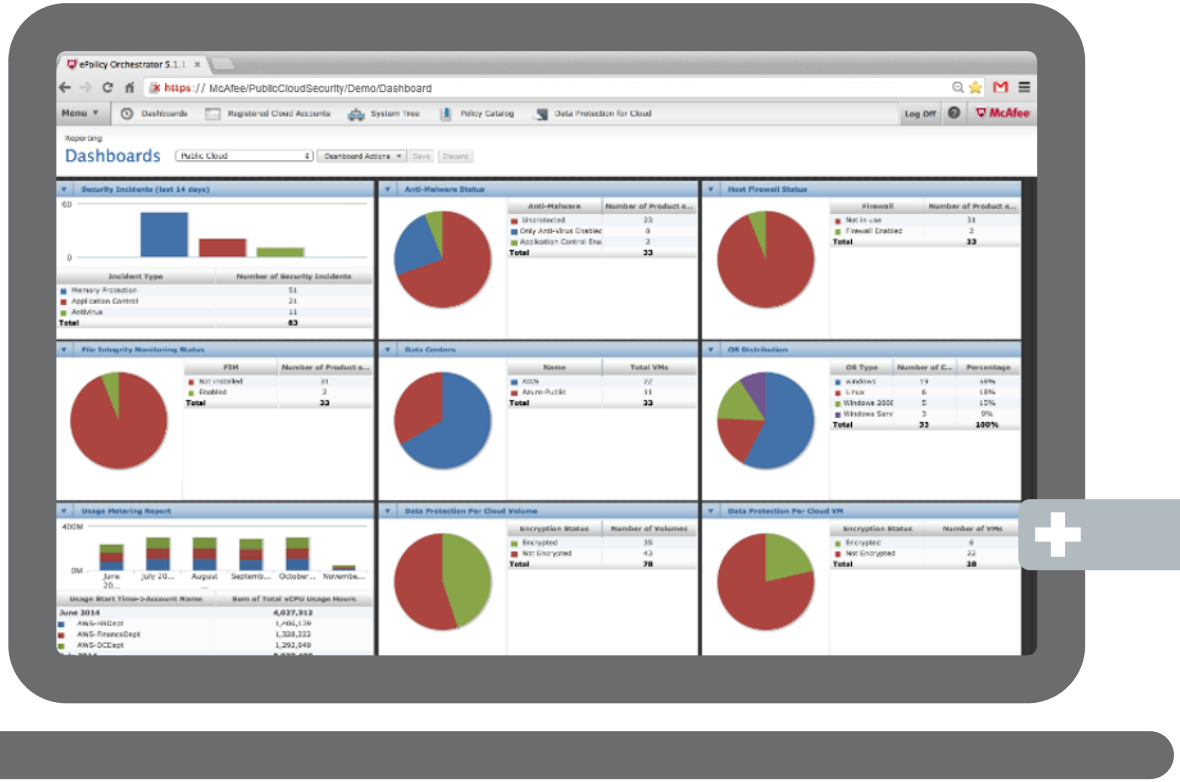
Управление

Единая точка управления. Хороший инструмент SOC

McAfee ePolicy Orchestrator

ePolicy Orchestrator

- Управление безопасностью серверов в облаке и физических с одной консоли
- Автоматическая реакция на инциденты
- Автоматизация бизнес процессов
- AWS иерархия систем логически группируется по регионам



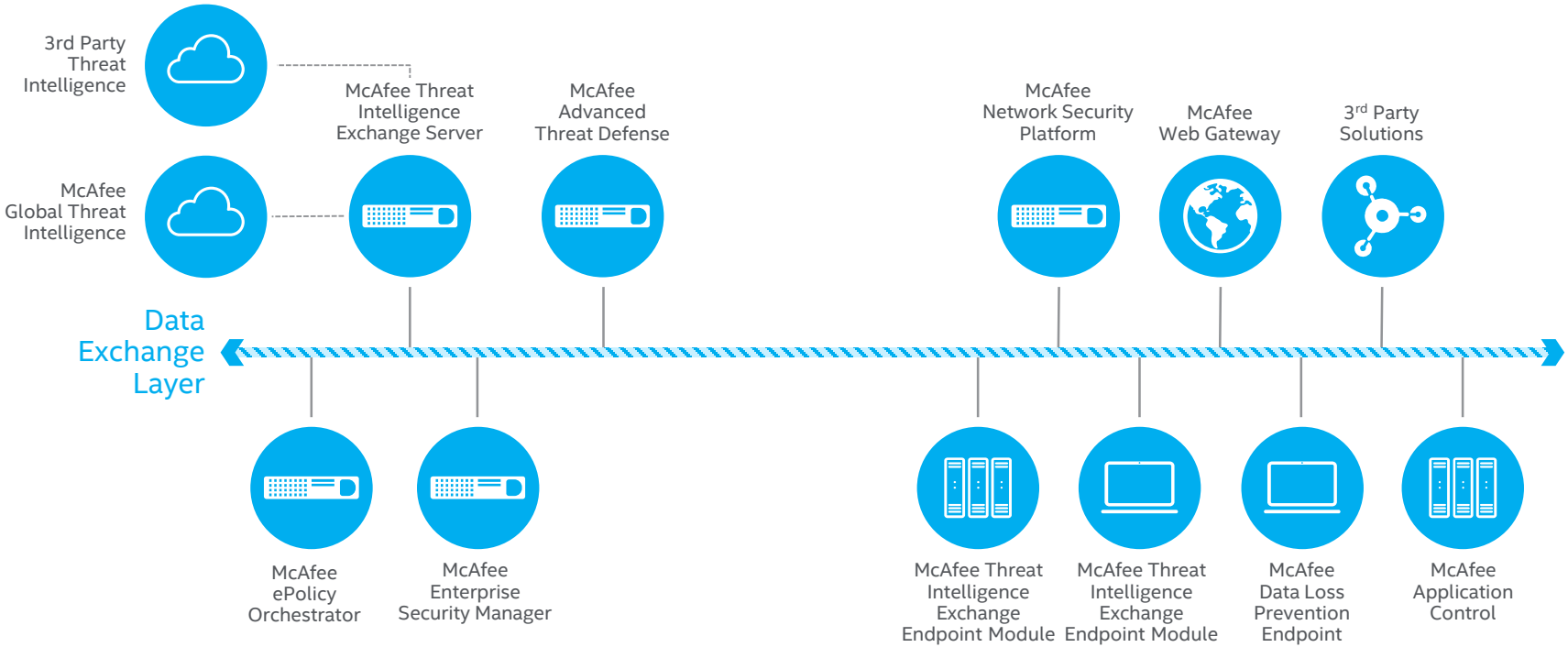
Database Security

McAfee Database Security

Возможность	Результат
Сканирование и учёт уязвимостей	• Автопоиск экземпляров баз данных. Индикация по рискам. Определение критических уязвимостей • Содержит долее 4,700 индивидуальных проверок на наличие уязвимостей. Специально разработана для баз данных. Oracle, MSSQL, MySQL, Db2 и др.
Применение патчей БЕЗ перезагрузки	• Блокировка угроз без установки патчей. Виртуальный патчинг • Защита применяется даже До выхода официального патча • Не требует специальных знаний DBMS для администратора • Non-intrusive software design означает, что никаких изменений или инсталляций в саму базу данных не происходит
Мониторинг баз данных в реальном режиме времени	• Защита баз данных в реальном режиме времени по нескольким векторам • Запись детального аудиторского следа для прохождения SOX, HIPAA/HITECH, PCI-DSS и других аудитов на соответствие • Сенсоры располагаются в памяти. Это позволяет защитить базы данных как на физических серверах, так ив облаке

Threat Intelligence Exchange

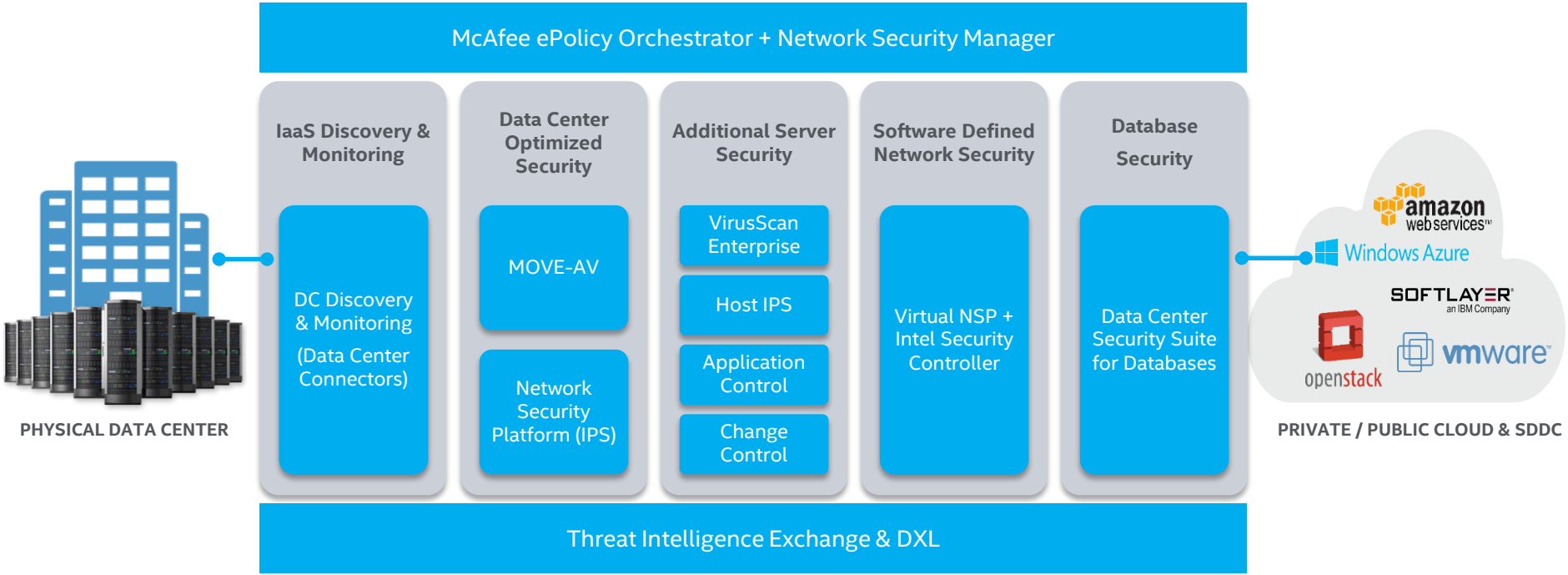
TIE Solution Overview



Подведём итог презентации

Comprehensive Security Portfolio

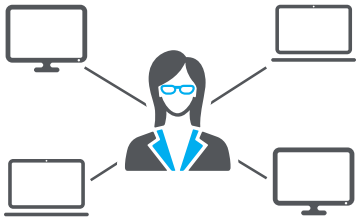
The whole is greater than the sum of its parts to secure hybrid infrastructures



Security for the Hybrid Infrastructure

	TRADITIONAL DATA CENTER (PHYSICAL)	VIRTUALIZED AND PRIVATE CLOUD	PUBLIC CLOUD (IaaS & SaaS)
Server and Storage Security	• VirusScan Enterprise • VirusScan for Storage • Application Control • Change Control • Host IPS	• MOVE AV • VirusScan Enterprise • VirusScan for Storage • Application Control • Change Control • Host IPS	• VirusScan Enterprise • Application Control • Change Control • Host IPS • Data Protection for Cloud • Data Center Connectors
Network Security	• Network Security Platform (IPS)	• Intel Security Controller • Network Security Platform (IPS)	
Edge & Data Protection	• Host Based DLP • Network DLP • Web Protection	• Host Based DLP • Network DLP • Web Protection	• Web Protection

Что это даёт?



Наглядность использования всех ресурсов, физических, виртуальных и в облаке

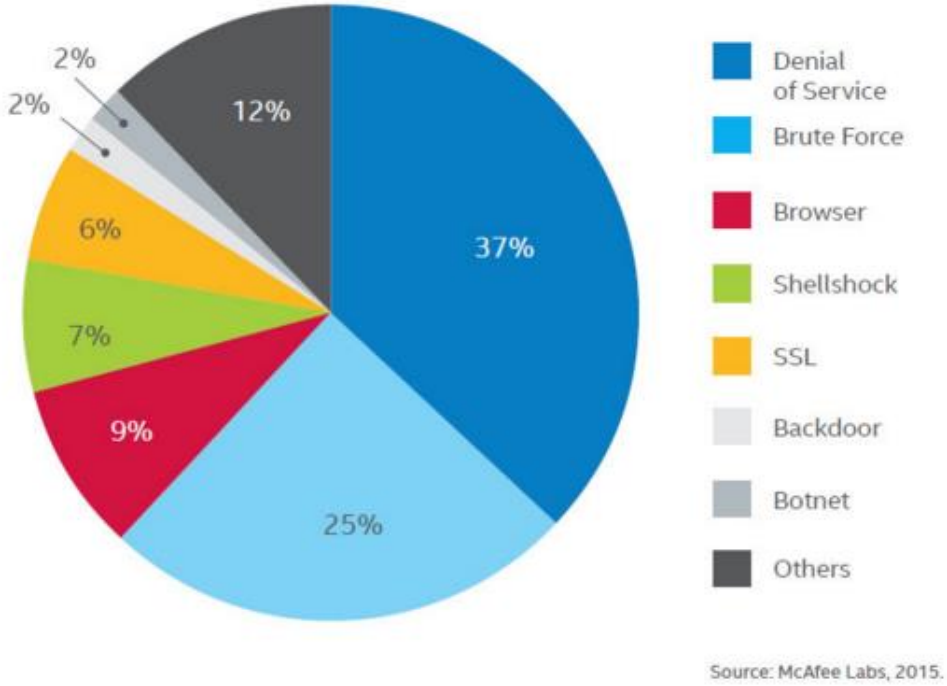
Защита всех ресурсов, физических, виртуальных и в облаке. **Блокировка сложных направленных атак**

Централизованное управление и отчётность всех ресурсов, физических, виртуальных и в облаке


PROTECT
DETECT
CORRECT
Intel Security предоставляет надёжное решение для защиты гибридных Дата Центров


intel
Security

Top Network Attacks



Source: McAfee Labs, 2015.

McAfee Q1 2015 Threats Report

What are Key Customer Pain Points?

IT / security operations perspective – a point of influence

Customer Pain	How Server Security Solves the Pain
Discover workloads to apply proper security	Automatic discovery of all physical and virtual machines, including those in the cloud
Apply proper security policies for public cloud deployments	Data center connectors for VMware vSphere, Amazon AWS, OpenStack, and Microsoft Azure to provide visibility of server instances
Deploy comprehensive server security with minimal performance impact	High performance malware protection for Windows and Linux servers and anti-virus optimized for virtualized environments
Complete protection against increasing sophisticated threats	McAfee Server Security suites also proactively secure against known and new zero-day attacks and prevents changes that can impose security risk
Protection from unknown threats	Ability to easily find and manage all application-related files and to protect them without labor-intensive list management or signature updates
Continuous compliance	Continuous file integrity monitoring, compliance policy enforcement and change prevention
Complex management of security silos, compliance tools and processes	McAfee ePO delivers comprehensive management and visibility for servers deployed in physical, virtualized and cloud environments

Server Security Suites

McAfee Server Security Suite Essentials

Foundational protection for physical, virtual and cloud deployments

McAfee Server Security Suite Advanced

Comprehensive protection for physical, virtual and cloud deployments

McAfee Public Cloud Server Suite Security

Optimized for public cloud protection

ePolicy Orchestrator	✓	✓	✓
VirusScan Enterprise (VSE)	✓	✓	✓
VirusScan Enterprise for Linux (VSEL)	✓	✓	✓
Host IPS for Servers & Linux Firewall	✓	✓	✓
MOVE AV for Servers	✓	✓	
MOVE Scheduler	✓	✓	
McAfee Agentless Firewall (for servers on VMware ESX)		✓	
Data Center Connector for VMware vSphere	✓	✓	
Data Center Connectors for AWS, Azure, OpenStack	✓	✓	✓
Application Control for Servers		✓	✓
Change Control for Servers		✓	✓
Cloud Encryption Management (for servers on AWS)			✓
Price (Unit of Measure)	Per OS Instance	Per OS Instance	Usage Based Hourly Pricing (Subscription)

Discovery using AWS Connector for ePO

1.
Enter AWS account details

2.
EC2 instances discovered and imported into ePO

3.
Secure your servers

McAfee Server Security

Защита серверов в дата центре и в облаке

McAfee Server Security Suite Essentials

- Базовая защита физических, виртуальных серверов и серверов в облаке
- Лицензируется на экземпляр ОС

McAfee Server Security Suite Advanced

- Расширенная защита физических, виртуальных серверов и серверов в облаке
- Лицензируется на экземпляр ОС

McAfee Public Cloud Suite Security

- Специально для серверов в публичных облаках
- Подписка на количество часов работы CPU