Integrated Cyber Defense платформа как основа цифровой трансформации

Стратегия развития безопасности Symantec

Станислав Бубнов

Технический консультант
Stanislav_Bubnov@Symantec.com
Emerging markets

Нынешний ландшафт угроз

Symantec.

Web Threats

More than 1 Billion
Web requests analyzed each day
Up 5% from 2016

1 in 13
Web requests lead to malware
Up 3% from 2016

Email

Percentage Spam Rate

2015	2016	2017
53%	53%	55%

IoT

600%
Increase in Attacks

2016	2017
6K	50K

Vulnerabilities

Overall increase in reported vulnerabilities **13%**

29% Increase in industrial control system (ICS) related vulnerabilities

Malware

92% Increase in new downloader variants

80% Increase in new malware on Macs

8,500% Increase in coinminer detections

Ransomware

5.4B WannaCry attacks blocked

46% Increase in new ransomware variants

Mobile

Number of new variants

2016	2017
17K	27K

Increase in mobile malware variants **54%**

24,000 Average number of malicious mobile apps blocked each day

Финансовый кризис
Проблемы распределения финансов

ЭКСПЛУАТАЦИОННЫЕ РАСХОДЫ НА БЕЗОПАСНОСТЬ

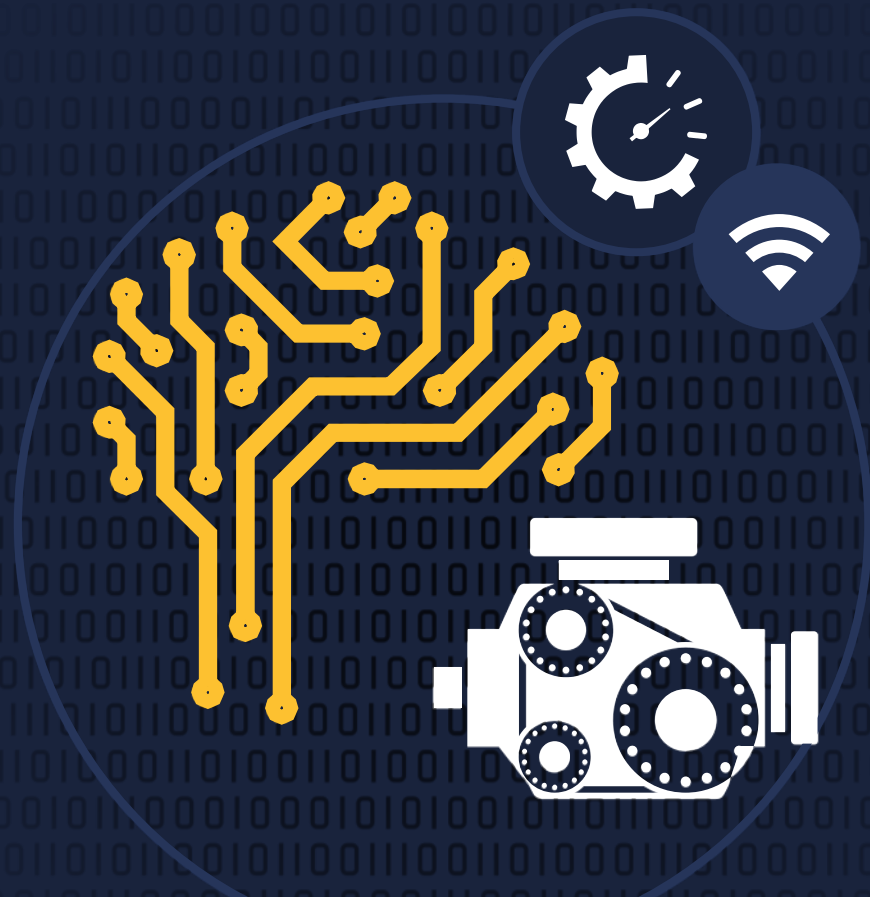
- Привязанность к существующим технологиям
- Ежегодные улучшения безопасности
- Новый регламент
- Увеличение стоимости труда
- Рост стоимости подписки
- Управление двумя средами (традиционная и облачная)

The Internet Gets Darker

Требует присутствия во всех ключевых точка терминации трафика

Актуальность изменяющихся технологий

Организациям придется довериться автоматическим средствам обеспечения безопасности



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Обнаружение угроз – не панацея

Индустрия перефокусируется на Предотвращение

THE GREAT DESTROYER **Petya was unleashed to cause destruction rather than earn its creators money, experts claim**

> Cyber security researchers say virus that is sweeping the globe is a 'wiper' designed to cause mayhem and is not actually 'ransomware'

MONEYWATCH Markets | Money | Work | Small Business | Retirement

By JONATHAN BERR / MONEYWATCH / May 16, 2017, 5:00 AM

"WannaCry" ransomware attack losses could reach $4 billion

Tweet / Reddit / Flip

ancial and economic losses fro
s in at least 150 countries could
he most damaging incidents in

Analysts think Petya 'ransomware' was built for targeted destruction, not profit

Devin Coldewey @techcrunch / Jun 28, 2017

ZDNet VIDEOS | SMART CITIES | WINDOWS 10 | CLOUD | INNOVATION | SECURITY | TECH PRO | MORE | NEWSLETTERS

MUST READ IOS 11.3: SHOULD YOU INSTALL IT?

Ransomware turns even nastier: Destruction, not profit, becomes the real aim

Leaks and dumps are handing more tools for creating ransomware and other malicious software to cybercriminal

By Danny Palmer | August 9, 2017 -- 10:05 GMT (03:05 PDT) | Topic: Security

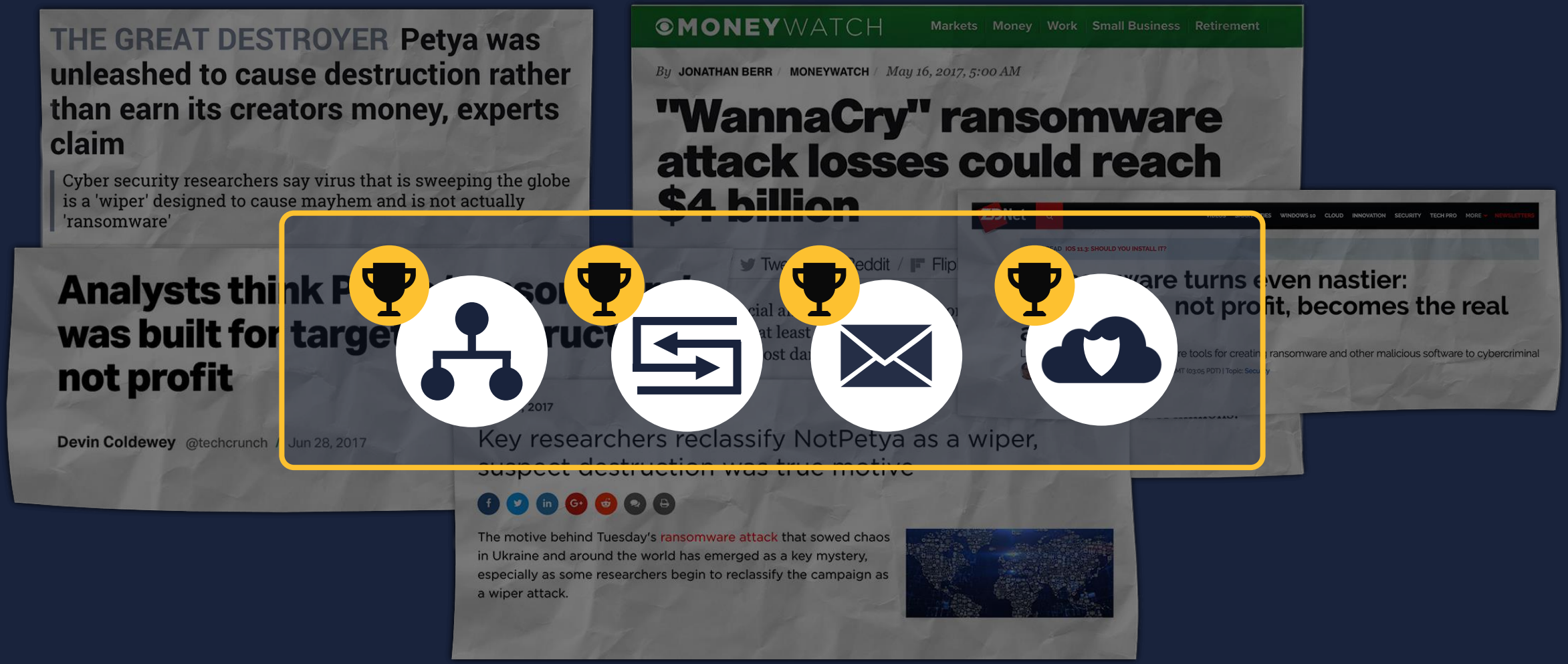
June 29, 2017

Key researchers reclassify NotPetya as a wiper, suspect destruction was true motive

The motive behind Tuesday's ransomware attack that sowed chaos in Ukraine and around the world has emerged as a key mystery, especially as some researchers begin to reclassify the campaign as a wiper attack.

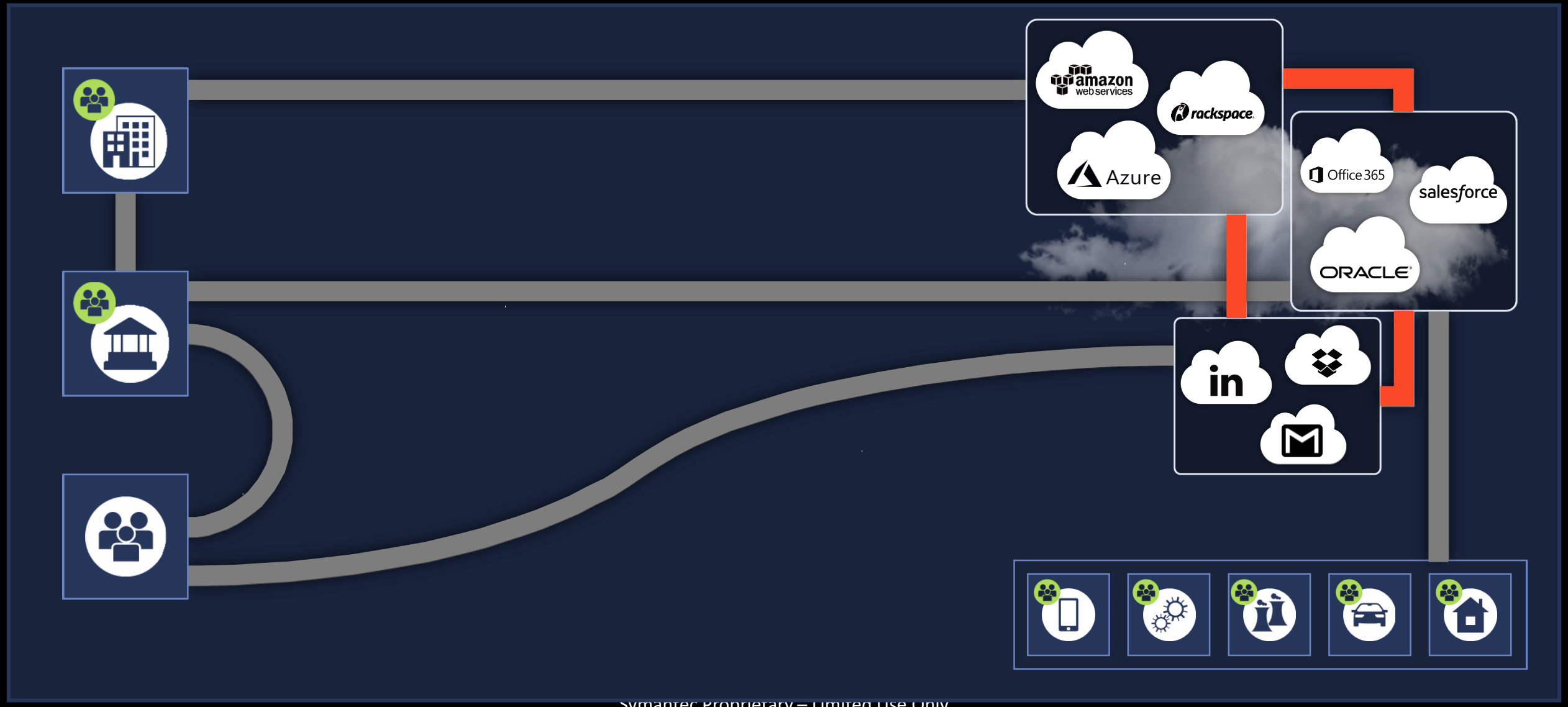
Обнаружение угроз – не панацея

Индустрия перефокусируется на Предотвращение



Дилемма Облачного поколения

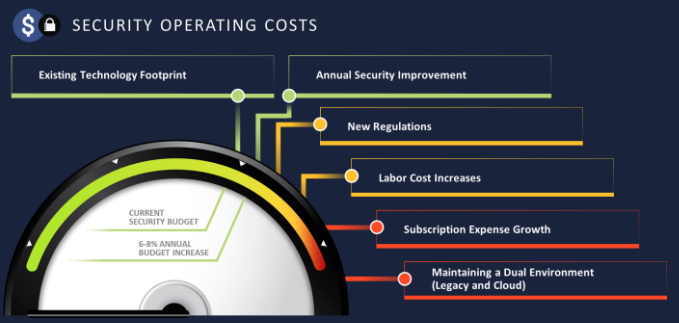
Меняющиеся модель использования информации требует новой Облачной Архитектуры



Дилемма Облачного поколения

Меняющиеся модель использования информации требует новой Облачной Архитектуры

THE COMING FISCAL CRISIS



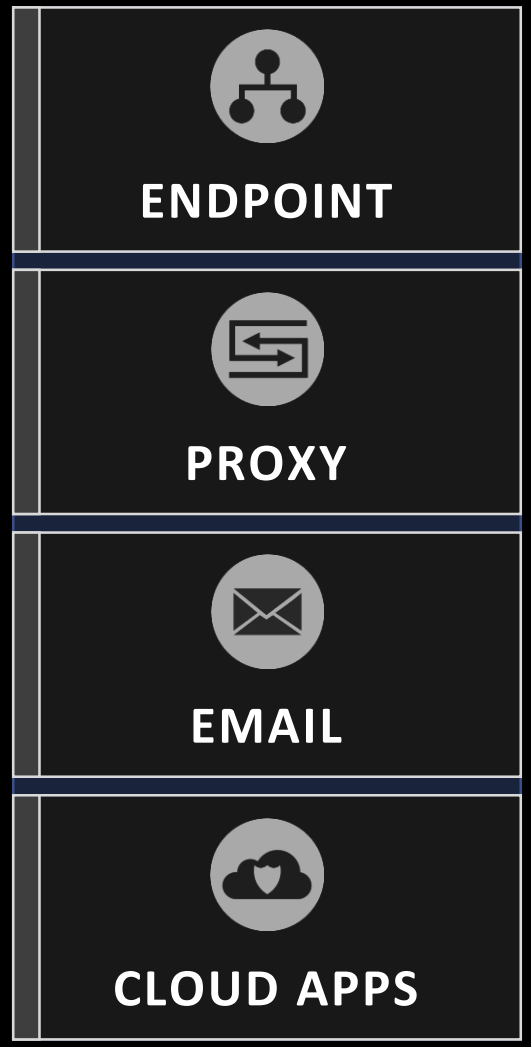
DEEP ARTIFICIAL INTELLIGENCE & AUTOMATION

CLOUD GENERATION ARCHITECTURE & PLATFORMS

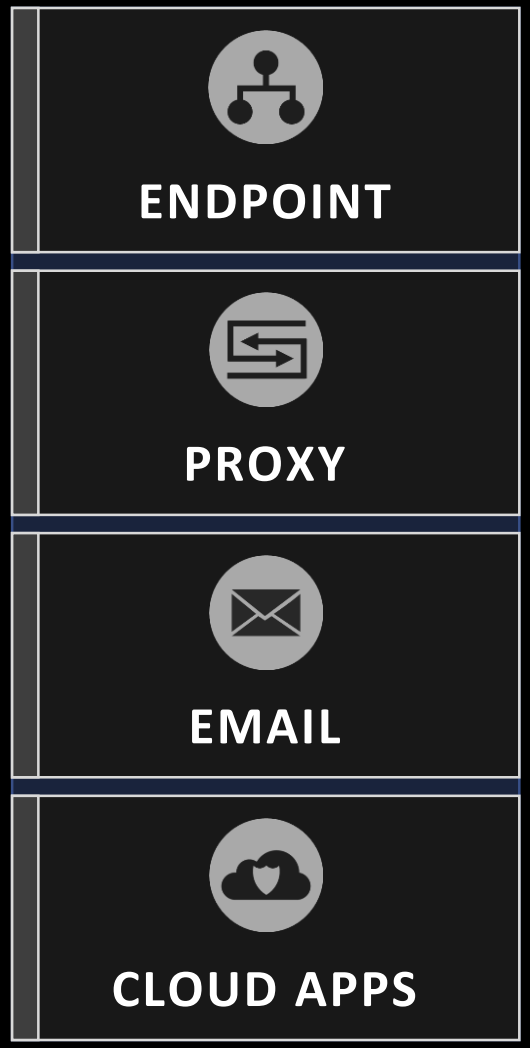
A DARK INTERNET

BEST IN CLASS TERMINATION POINTS & PROTECTION

Основные точки терминации трафика



Обеспечение защиты Cloud Generation



Обеспечение защиты Cloud Generation

ENDPOINT

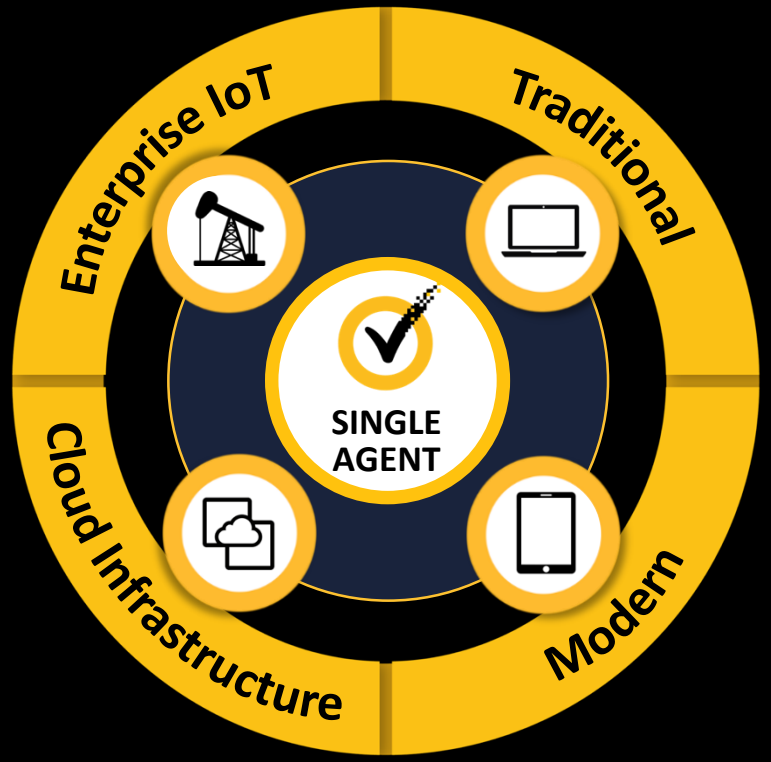
PROXY

EMAIL

CLOUD APPS

Требования к рабочим местам

- Лучшая в своем классе Защита
- Машинное обучение/Искусственный интеллект
- Единый агент/Эффективная архитектура
- Готовность к облачному использованию
- Поддержка любого типа конечного устройства



Слабая защита от вредоносa в период быстро меняющихся угроз

Больше угроз ведут к большему числу агентов

46%
Увеличение числа программ-вымогателей

92%
Увеличение вариантов новых загрузчиков

8,500%
Увеличение обнаружений coin mining программ

7 Среднее число средств управления конечными устройствами и агентами безопасности

Agent	Agent	Agent	Agent	Agent	Agent	Agent
ANTIVIRUS	NETWORK FIREWALL & INTRUSION PREVENTION	REPUTATION ANALYSIS	DEVICE CONTROL & POWER ERASER	ADVANCED MACHINE LEARNING	BEHAVIOR MONITORING	EMULATOR	MEMORY EXPLOIT MITIGATION	DECEPTION	EDR	APPLICATION ISOLATION	APPLICATION CONTROL
Anti-malware				Advance Malware Protection				Deception	Integrated EDR	SEP Hardening	

Технические проблемы

- Как интегрировать
- Проблемы совместимости
- Запутанность, которая ведёт к брешам в безопасности

Операционные проблемы

- Как внедрять и управлять множеством агентов
- Увеличение стоимости и трудозатрат
- Каждый агент нужно обновлять вместе с апдейтами операционной системы
- Рост числа алертов, на которые надо реагировать SOC

Многоуровневая одно-агентная Защита рабочих мест

SEP 14.1 и SEP Hardening на переднем крае технологий

- Использование самого большого в мире гражданского GIN для блокировки общих угроз
- Блокирование сторонних изменений и команд, а также контроль трафика
- Контроль физических параметров устройств (USB, системные файлы)
- Восстановление инфицированных файлов

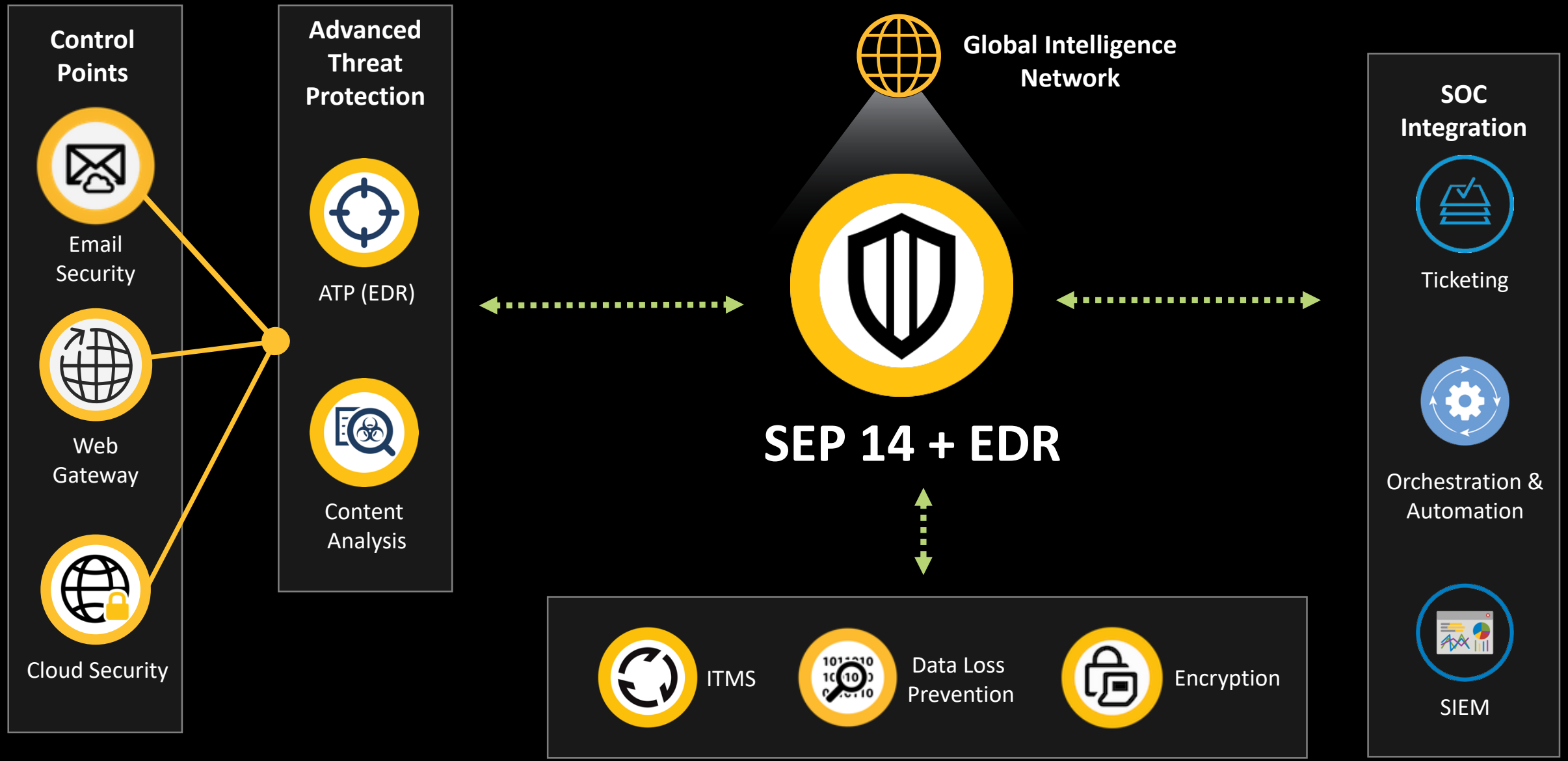
- Наиболее эффективная борьба с программами вымогателями
- Защиты от без файловых угроз
- Виртуальный patching для критических уязвимостей
- Блокирование полиморфных вирусов

- Определение скрытых злоумышленников
- Разоблачение намерений и тактики атакующего для улучшения защиты

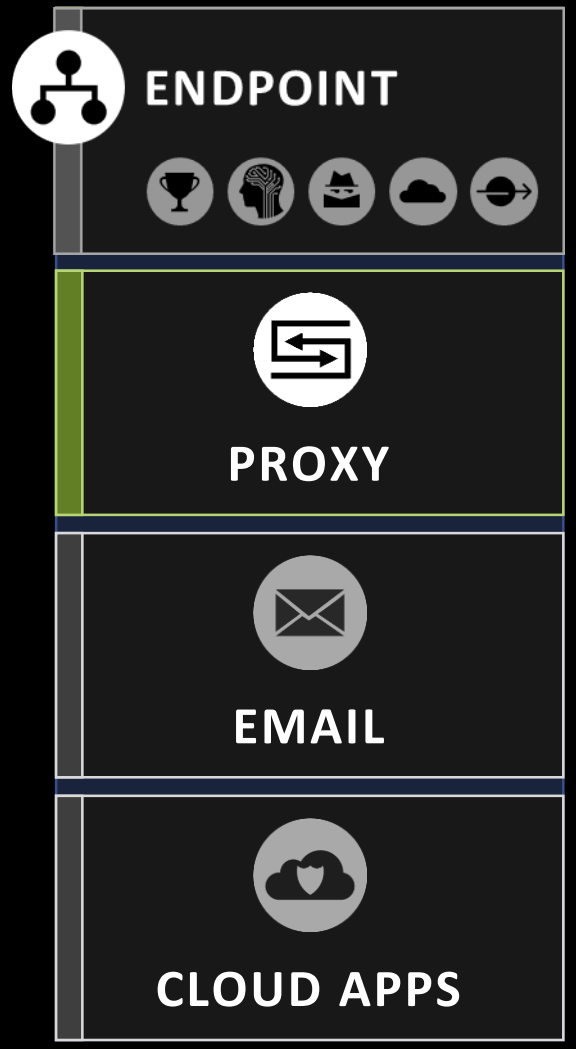
- Определение скрытых угроз
- Мгновенное восстановление рабочих мест
- Автоматические задания IR

- Авто-оценка риска приложений
- Защита корпоративных приложений от эксплойтов
- Изоляция подозрительных приложений от привилегированных операций

Интеграция с Symantec и продуктами партнеров



Обеспечение защиты Cloud Generation



Требования к Прокси

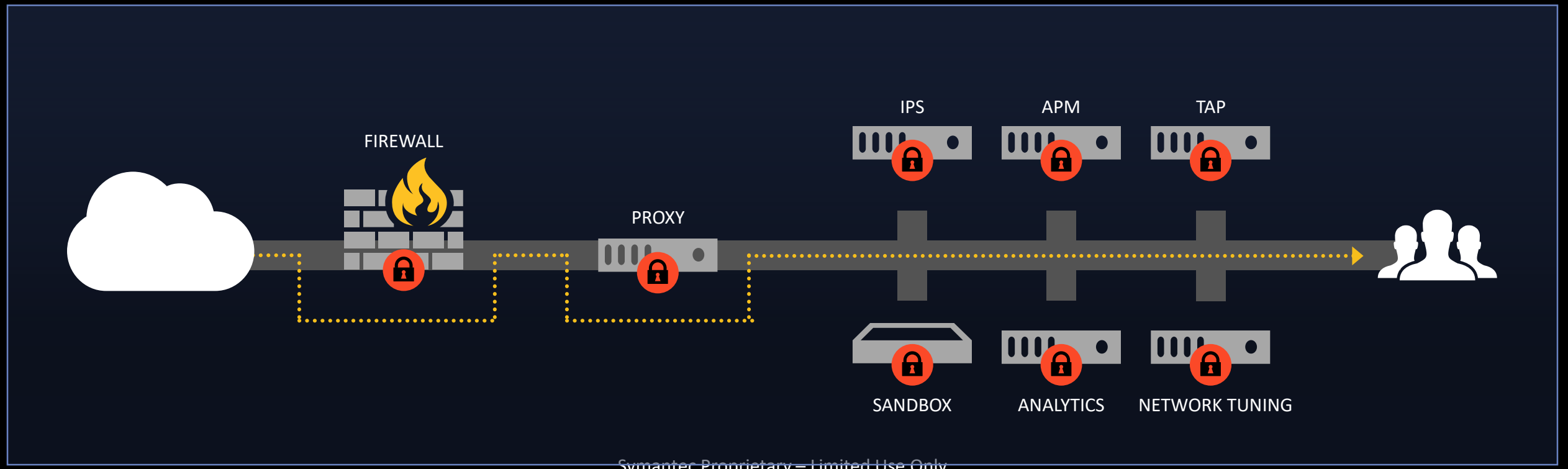
- Лучший в своем классе
- Управление зашифрованным трафиком
- Облако, физический аплайнс или виртуальный форм-фактор
- Интеграция с CASB
- Изоляция сетевого браузера

Зашифрованный трафик скрывает уязвимости

Обход всех средств защиты

Gartner

Половина всех вирусных компаний в 2019 буду использовать тот или иной способ шифрации для доставки вируса, управления активностью или похищения данных



Безопасная дешифрация сетевого трафика

Устранение уязвимости SSL/TLS шифрации

- Безопасная расшифровка SSL & TLS для полной инспекции
- Масштабирование дешифрации с SSL Visibility Appliance
- Настройка политик по категориям для управления приватностью
- Поддержка наиболее широкого перечня шифров

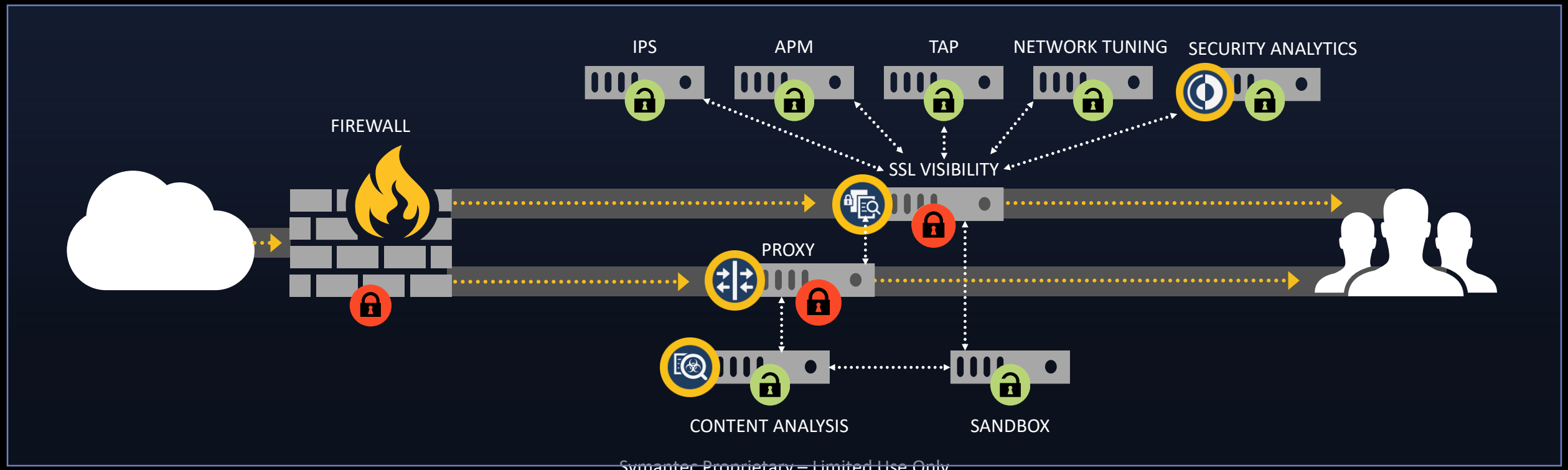
The Security Impact of HTTPS Interception

"A" Symantec / Blue Coat

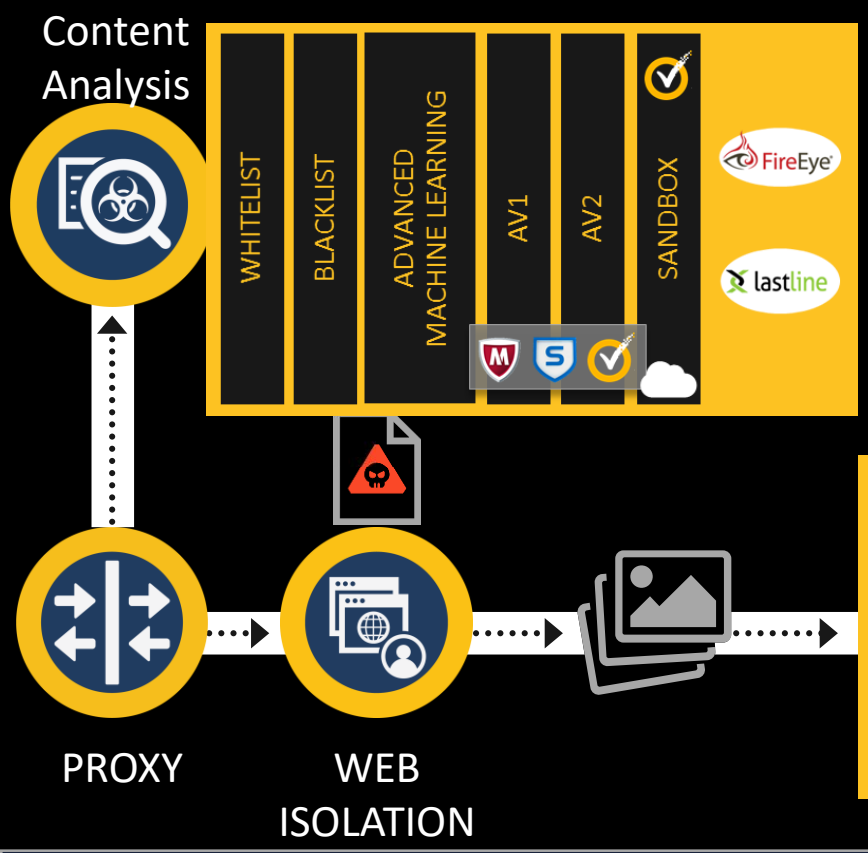
"C & F's" NGFWs, SWG's, ADCs

Testing conducted by:

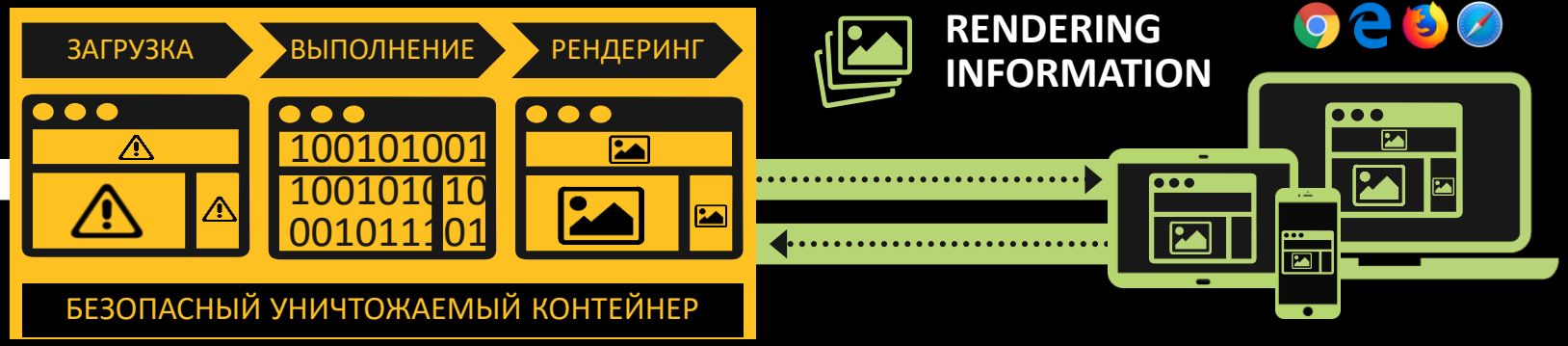
Google moz://a CLOUDFLARE Berkeley UNIVERSITY OF CALIFORNIA UNIVERSITY OF MICHIGAN



Изоляция Web для противодействия угрозам



- Изоляция сайтов без категории/с высоким риском
- Безопасный просмотр веб для VIP пользователей
- Вложенные в Email URLs (phishing)



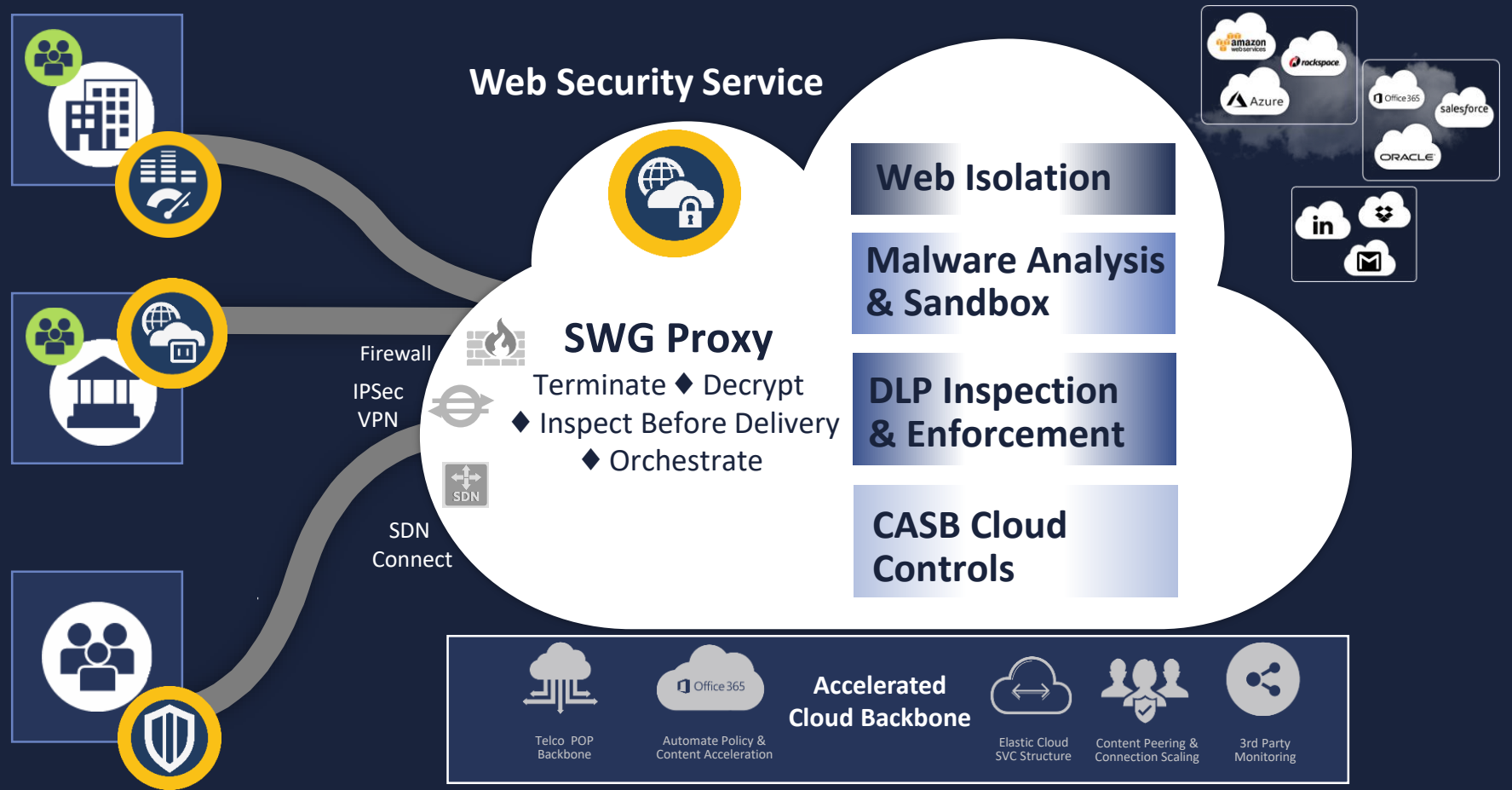
> “Оцените и протестируйте решение удалённого браузинга … как одного из самых значимых способов снизить вероятность успешных web-based атак против ваших пользователей.”

Gartner®

https://www.gartner.com/document/3463618

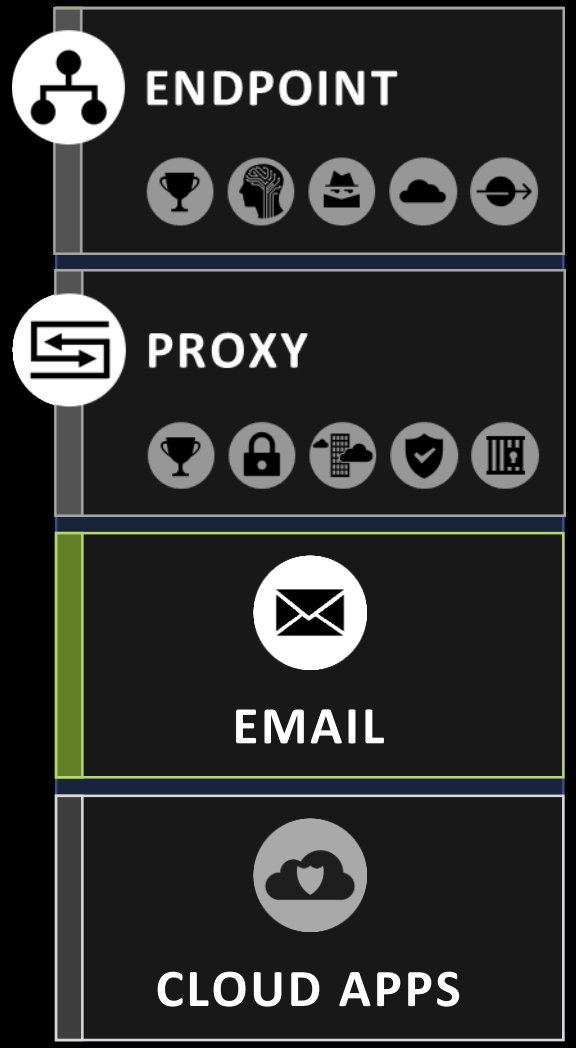
Обеспечение защиты Cloud Generation

Продвинутые средства защиты в облаке



- SWG Proxy At Core
- Threat Prevention and Information Security
- Cloud Controls (CASB)
- Flexible On-ramps, With SEP, SD-Connector
- High-performance Global Backbone
- QoS and Performance Optimization

Обеспечение защиты Cloud Generation



Требования к Email

- Лучшая в классе спам и вирусная защита
- Встроенная контент изоляция
- Защита внутри Компании, снаружи и внутри
- Гибкий форм-фактор
- Машинное обучение/Искусственный интеллект

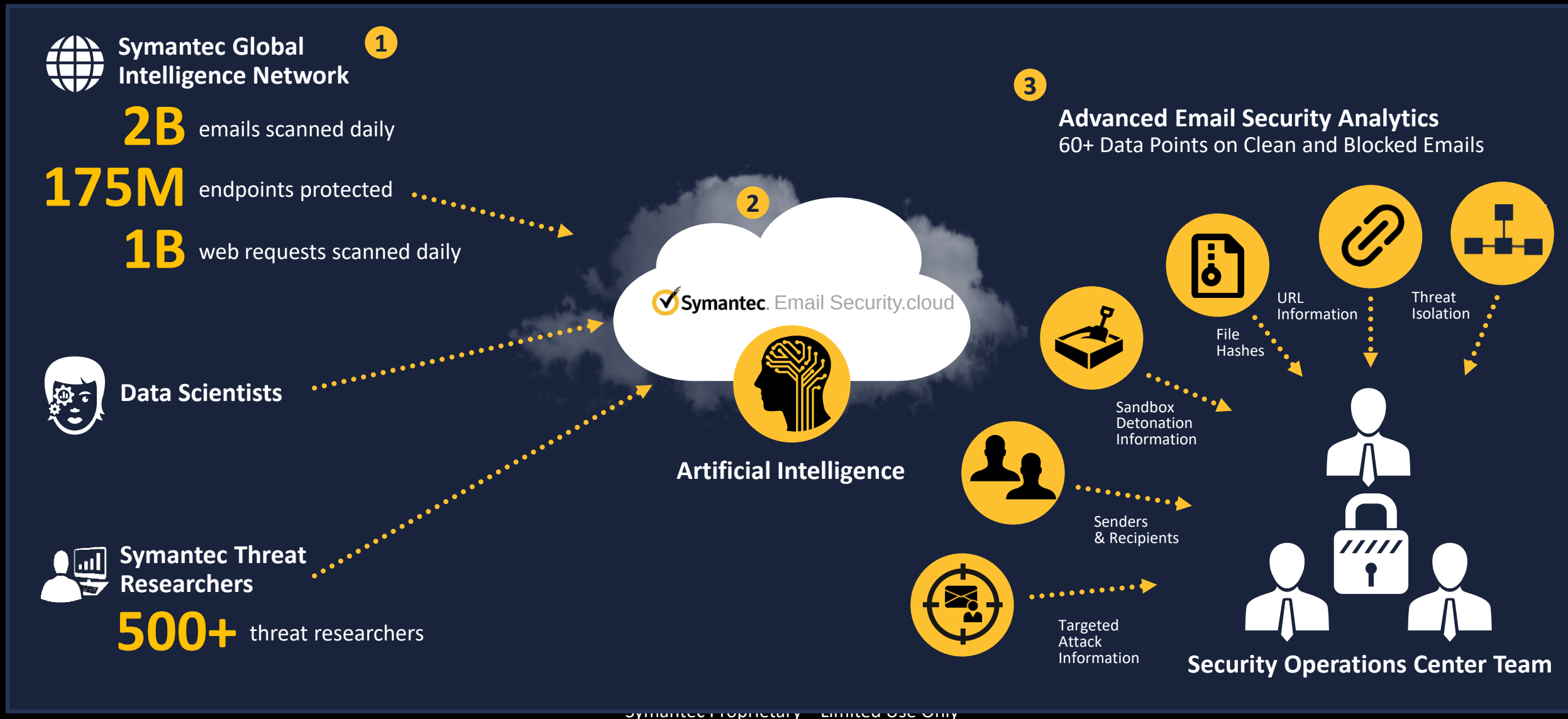
ISTR23: Email

За последний год, 71 процент всех таргетированных атак начинался с адресного фишинга

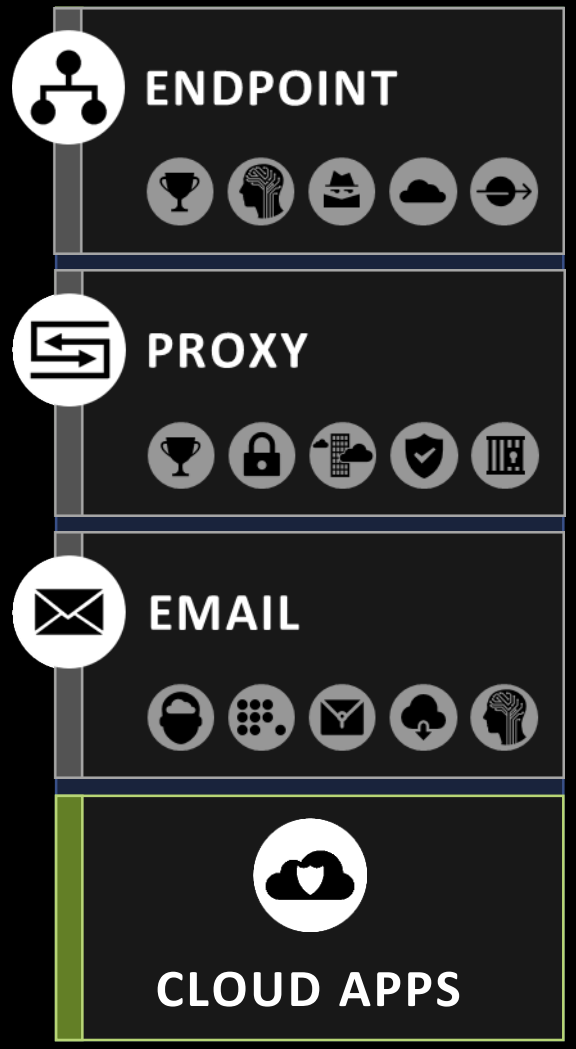
7,710 организаций сталкивались с мошенничеством вида Business Email Compromise каждый месяц

Ботнет Necurs отослал около 15 миллионов вредоносных писем в 2017, 82.5% только за вторую половину года

Продвинутая аналитика Email ускоряет реакцию на целенаправленные атаки



Обеспечение защиты Cloud Generation



Требования к облачному приложению

- Возможность отследить поведение пользователя в облаке
- Контроль доступа к облачным приложениям
- Идентификация пользователей и их действий в облаке
- Защита от вредоносного контента
- Расширение защиты данных в облаке

Проблема

Данные перемещаются в Облако

Office 365

box

salesforce

Gmail

Dropbox

Проблема – данные перемещаются в облако

ISTR23: Cloud

Кибер преступники эксплуатируют **украденные облачные CPU** для энергозатратного **майнинга крипто валюты**

18% всех PII, 13% всех PCI и **56% всех PHI** в облаке находятся в открытом доступе

68% всех организаций имеют сотрудников, которые **слишком рискованно пользуются своими** облачными приложениями

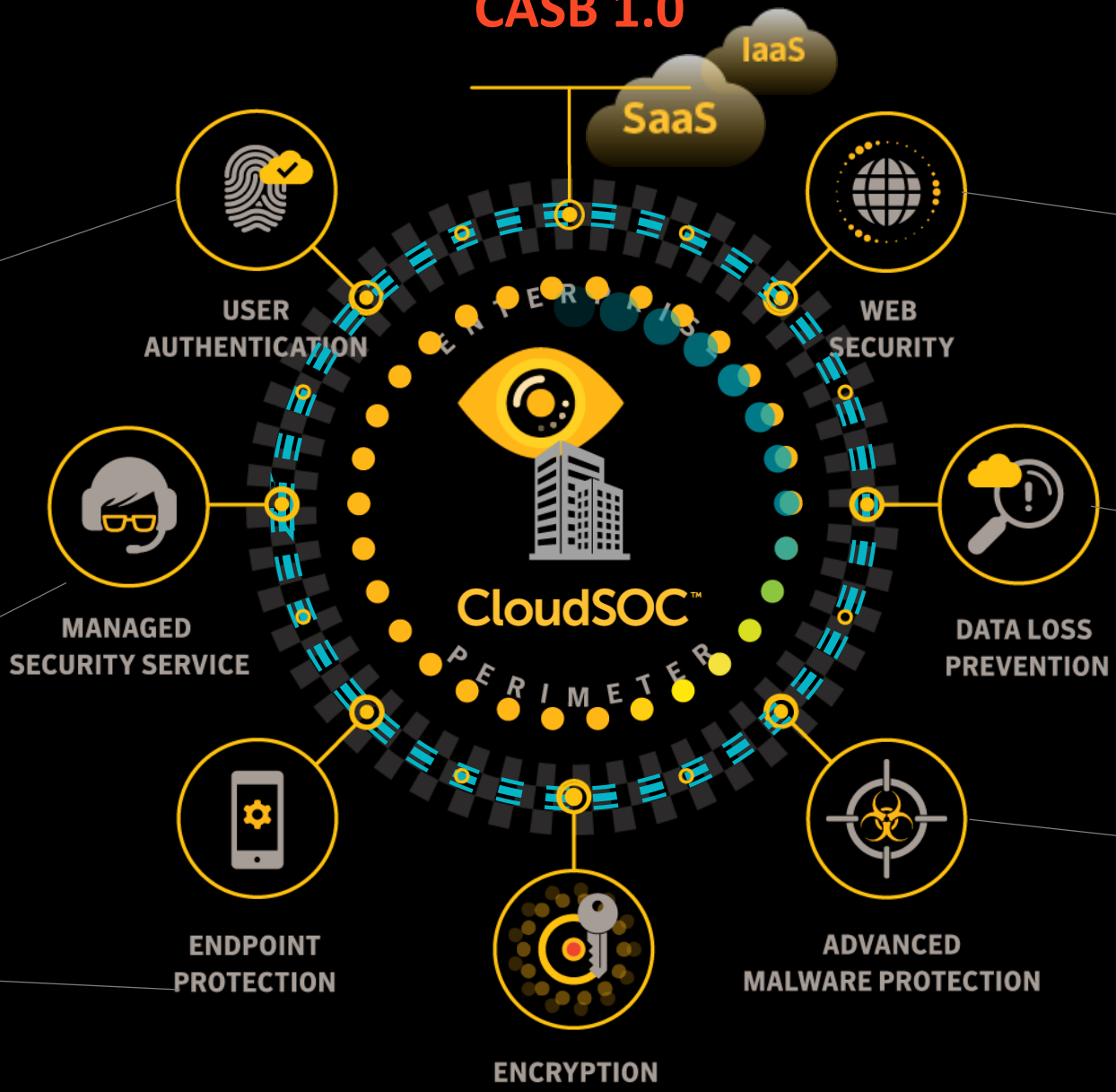
Visibility

Data Security

Threat Protection

CASB2.0

CASB 1.0



CloudSOC задействует VIP для 2-факторной идентификации в случае подозрительных действий

VIP

CloudSOC может расширить возможности IR (реагирование на событие) MSS для Shadow IT и облачных приложений

MSS

CloudSOC может отслеживать пользователей для полного анализа Shadow IT

SEP

CloudSOC усиливает ProxySG контролем над 25,000 приложений

ProxySG/WSS

CloudSOC позволяет задействовать DLP применительно к облачным приложениям

DLP

CloudSOC может задействовать эффективную аналитику вредоноса, чтобы не допустить его в облако

Malware prevention

CloudSOC задействует ICE для отслеживания и отзыва данных после покидания пределов облака

ICE

Symantec's Leadership in Gartner Magic Quadrants

Endpoint Protection
1/2018

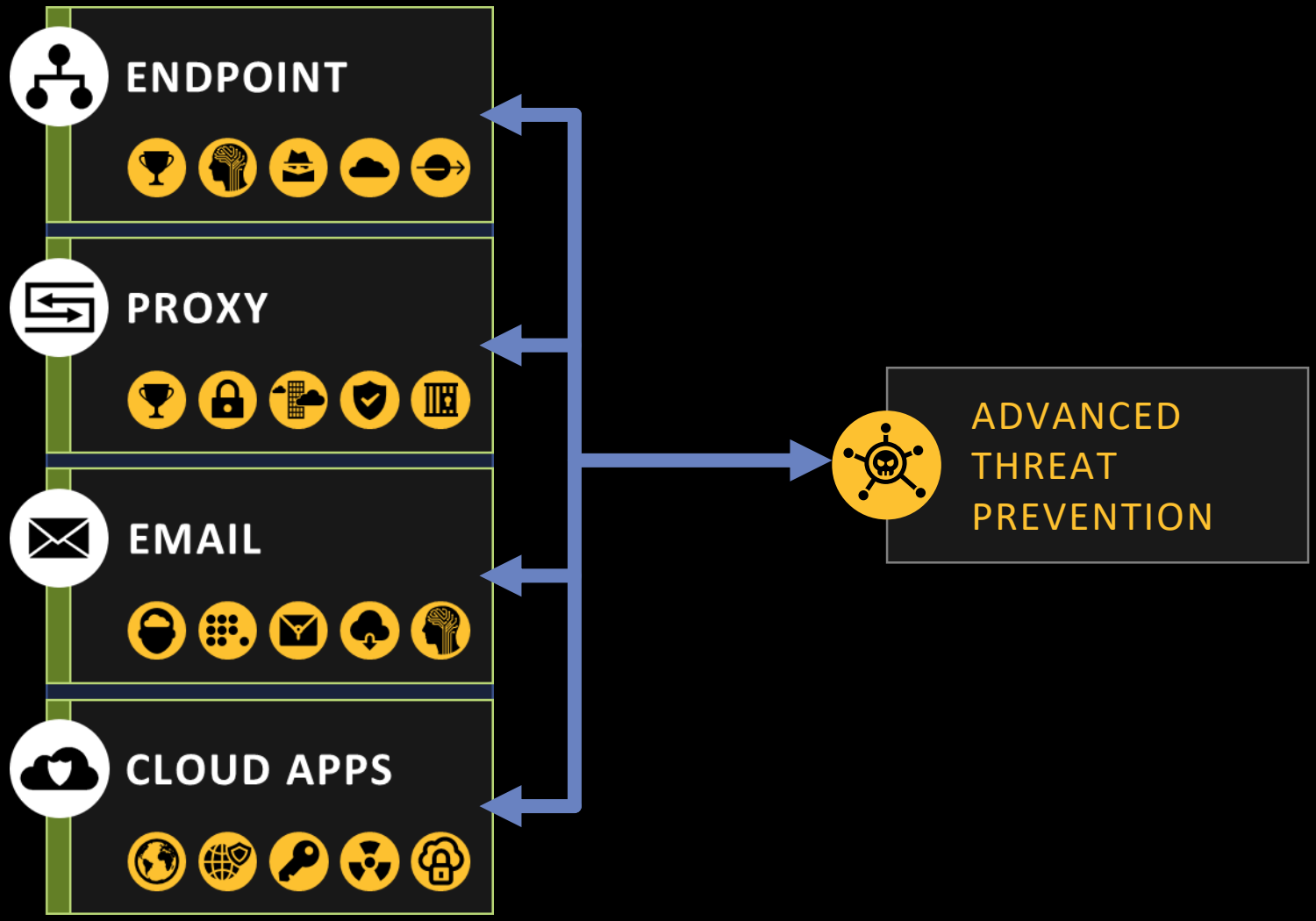
Secure Web Gateways
6/2017

Cloud Access Security Broker (CASB)
11/2017

Enterprise Data Loss Prevention
2/2017

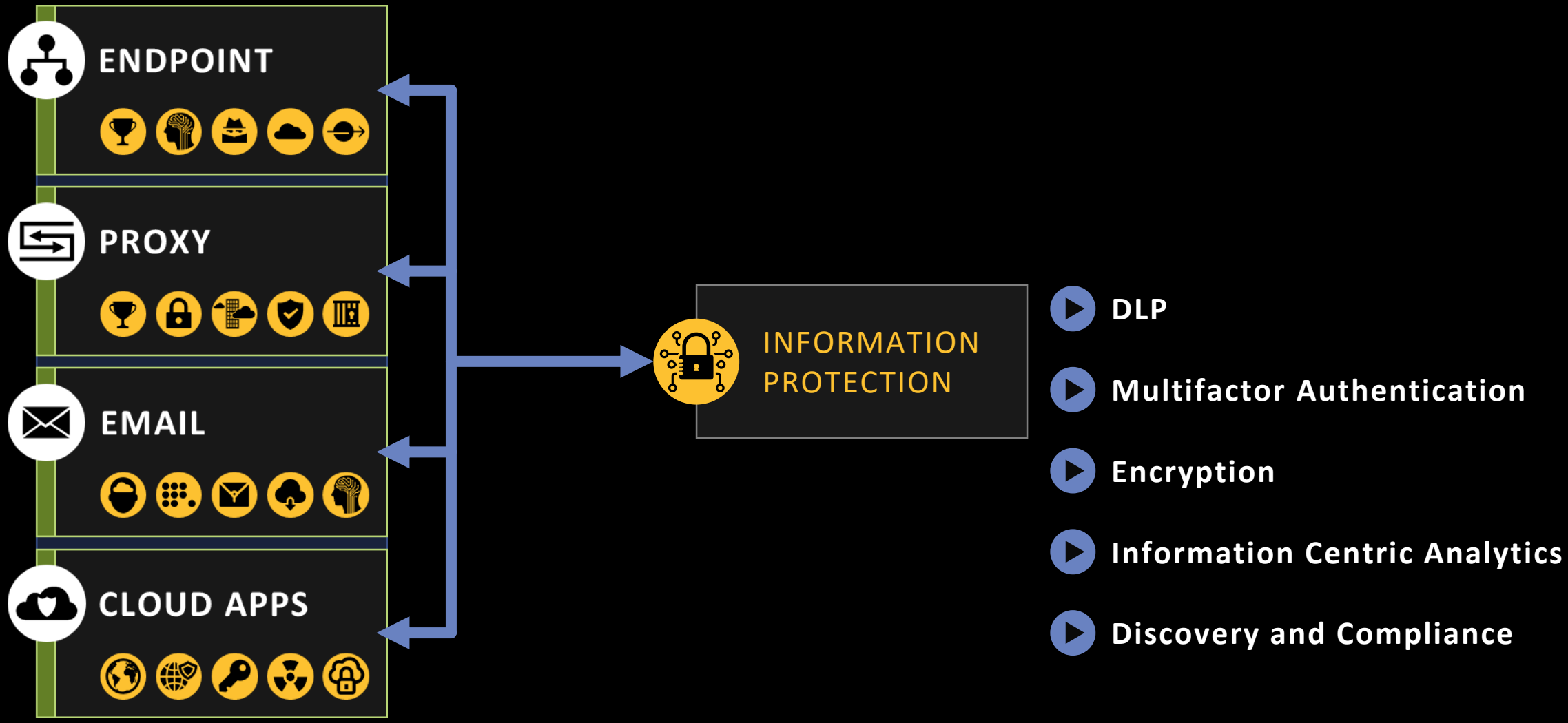
Managed Security Services (MSS)
1/ 2017

Высокотехнологичные сервисы в эпоху Cloud Generation

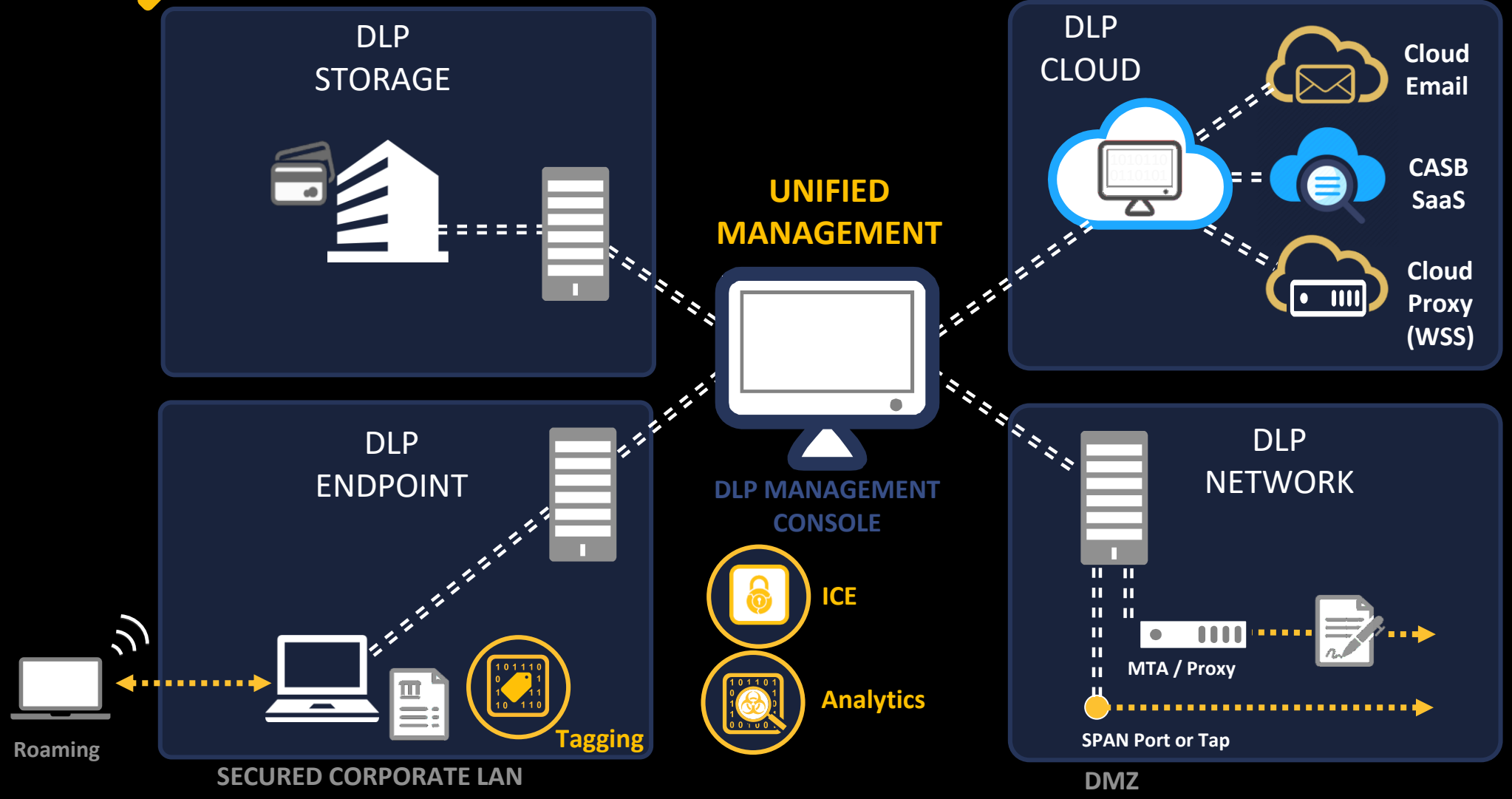


- Content Analysis
- Sandboxing
- Endpoint Detection & Response
- Full Packet Capture & Metadata

Высокотехнологичные сервисы в эпоху Cloud Generation



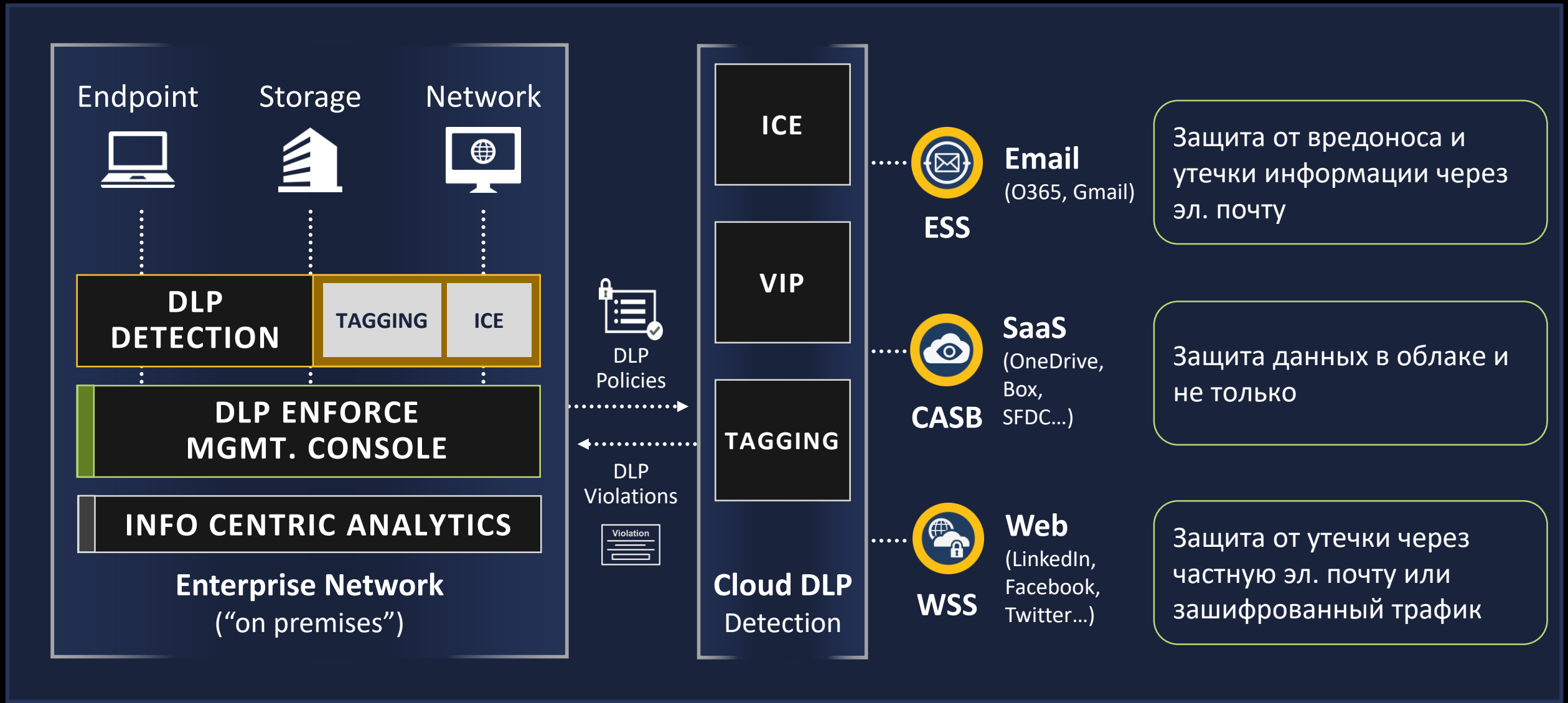
ОПРЕДЕЛЕНИЕ МОНИТОРИНГ ЗАЩИТА



- В облаке
- Все точки контроля
- Единая консоль управления
- Mobile & BYOD

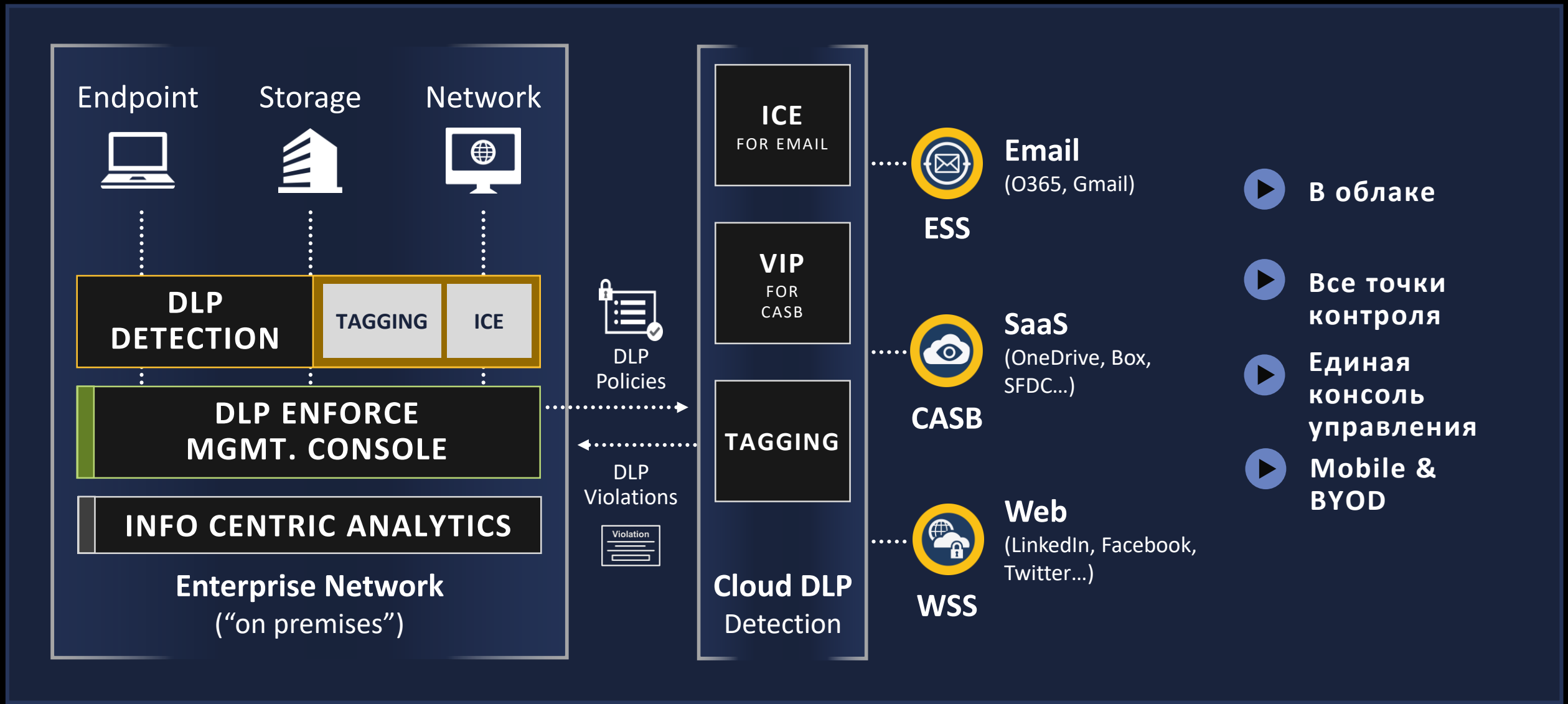
Решение

Аппаратное и облачное решения

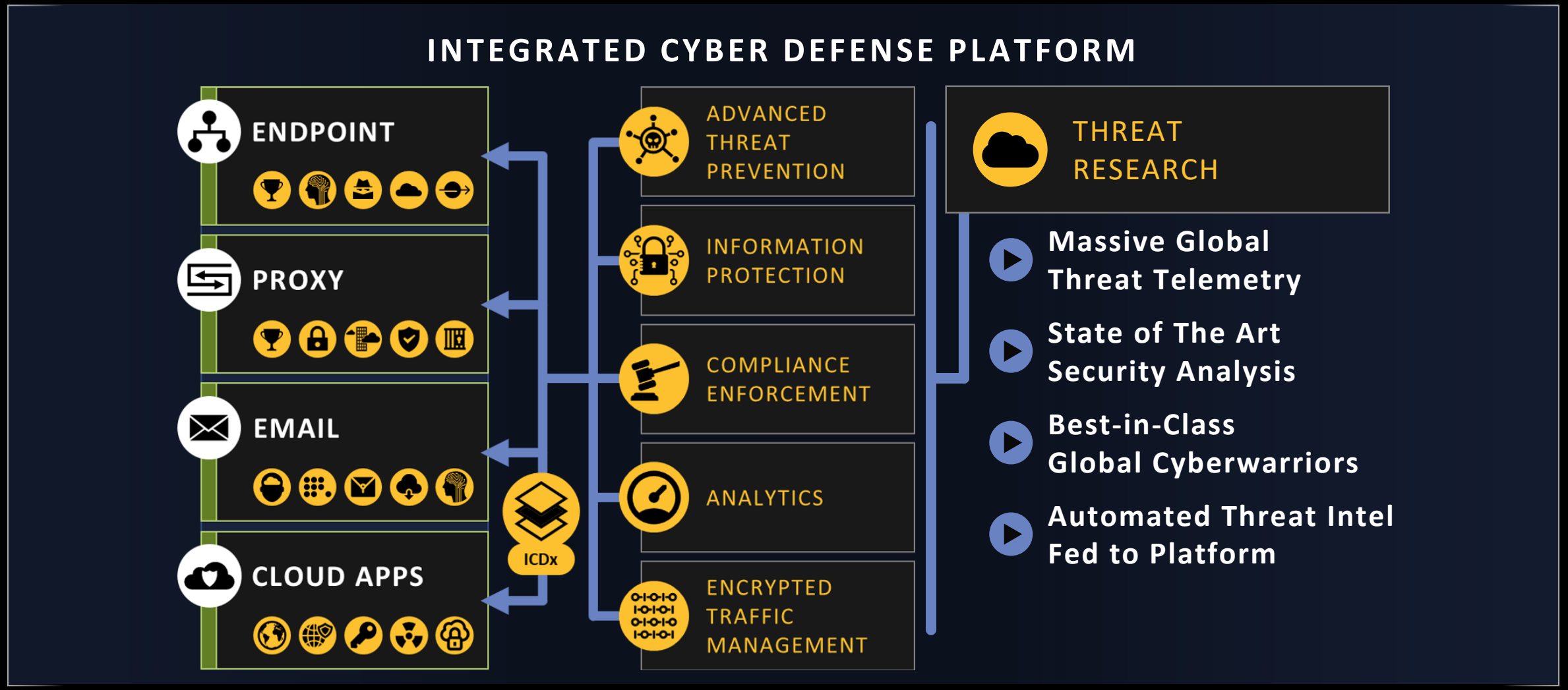


Решение

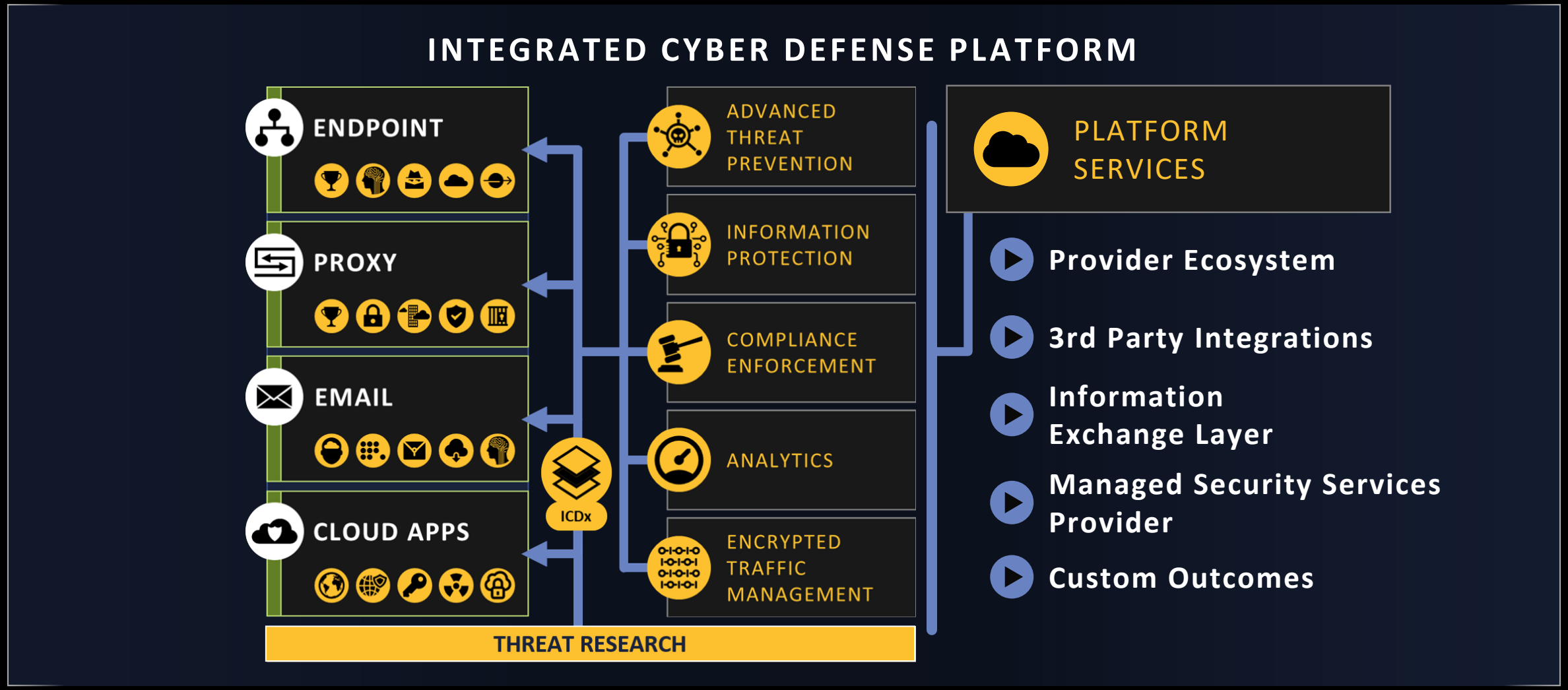
Аппаратное и облачное решения



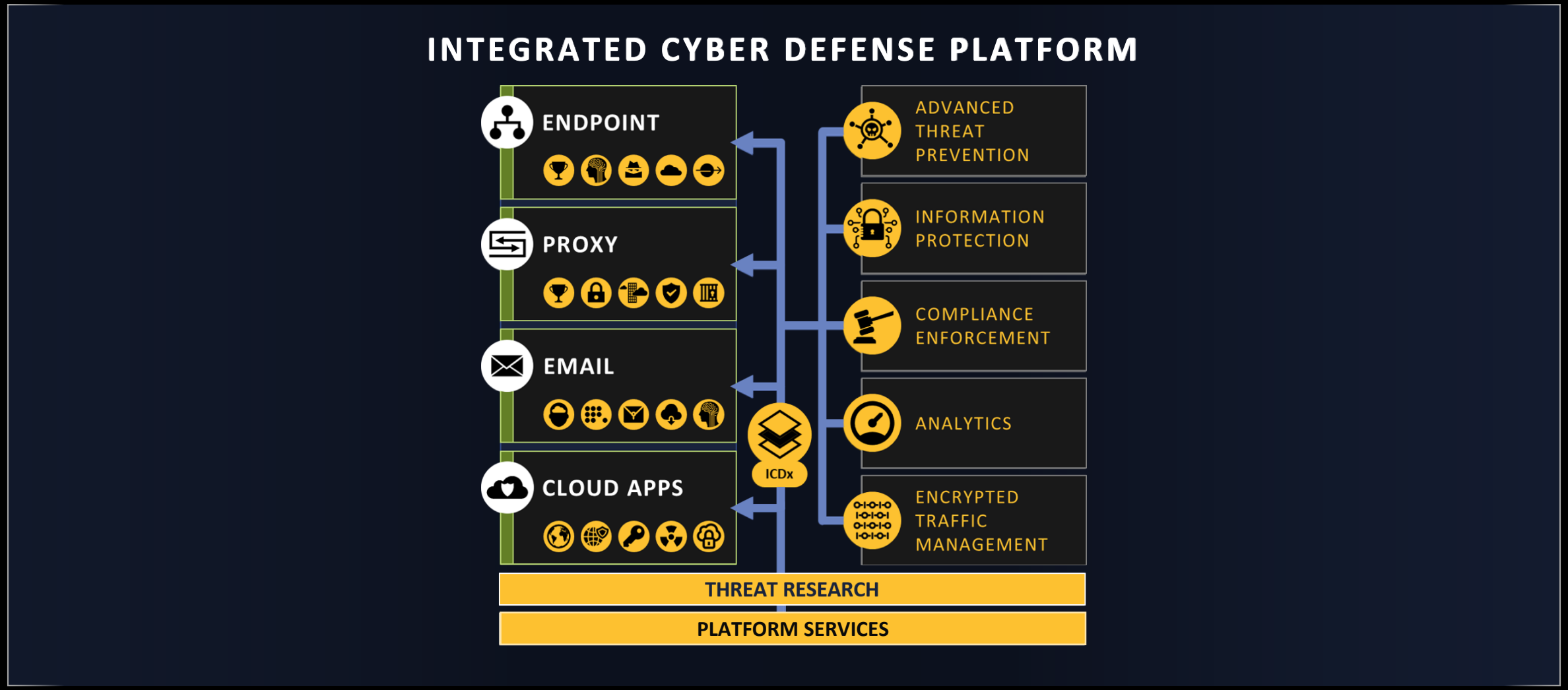
Защита данных в эпоху Cloud Generation



Delivering Protection in The Cloud Generation



Delivering Protection in The Cloud Generation

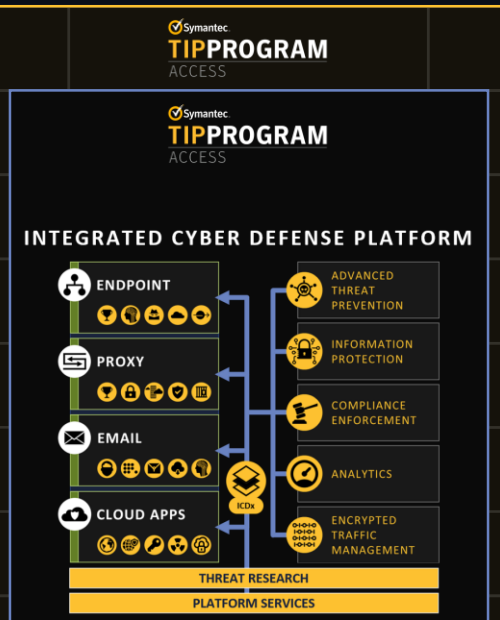


600+ PARTNERS INQUIRIES → **94** TECHNOLOGY PARTNERS → **178** INTEGRATIONS

A10 · AASHTO · Accellion · AGARI · AGAT · ALLURE · AREA 1 · Banco de Bogotá · Attivo Networks · boldonjames · Centrify · Compuverde · Citrix · CLOUDGENIX · ctera · cyber OBSERVER · cpacket Networks · CYBERSPONSE · CYMULATE · DB Networks · DELL EMC · docker · ECHOWORX · exabeam · f5 · Fidelis Cybersecurity · FLEXERA Software · HITACHI · gradian · indeni

Symantec TIPPROGRAM ACCESS

Bay Dynamics · CISCO · CounterTack · DEMISTO · Dropbox · FireEye · ForeScout · FORTINET · gemalto · Google



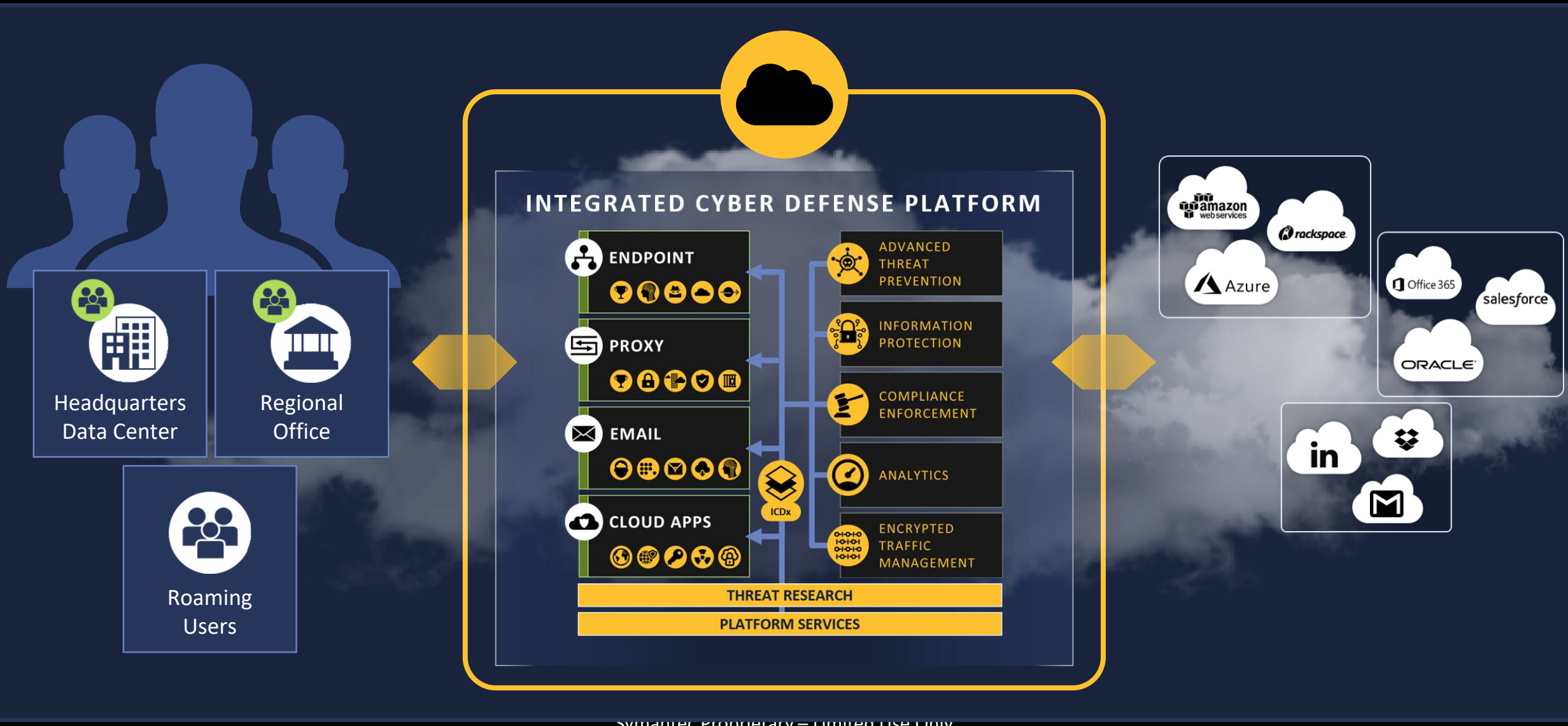
amazon web services · splunk> · servicenow · box · IBM · Microsoft

vmware · VENAFI · REVERSINGLABS · radware · Qualys. · Phantom · ORACLE · lastline · NetApp · MICROFOCUS

Intsights · ipswitch · ixia · LogRhythm · McAfee · MetaNetworks · MobileIron · napatech · NETSCOUT · NCR · NETDIALOG · NUTANIX · opentext · redhat · RSA · Pulse Secure · SAP · salesforce · silverpeak · slack · SOPHOS · SWIMLANE · SYMPHONY · THALES · thycotic · TITUS · tufin · VARONIS · VERSA Networks · yammer

Symantec Integrated Cyber Defense

Delivering a Simplified Security Model for the Cloud Generation




Symantec