



# Vectra.AI – лидер рынка NDR

Network Detection and Response

October 2020

Netwell, официальный дистрибьютор. [www.netwell.ru](http://www.netwell.ru)

# Современный SOC невозможен без сети.

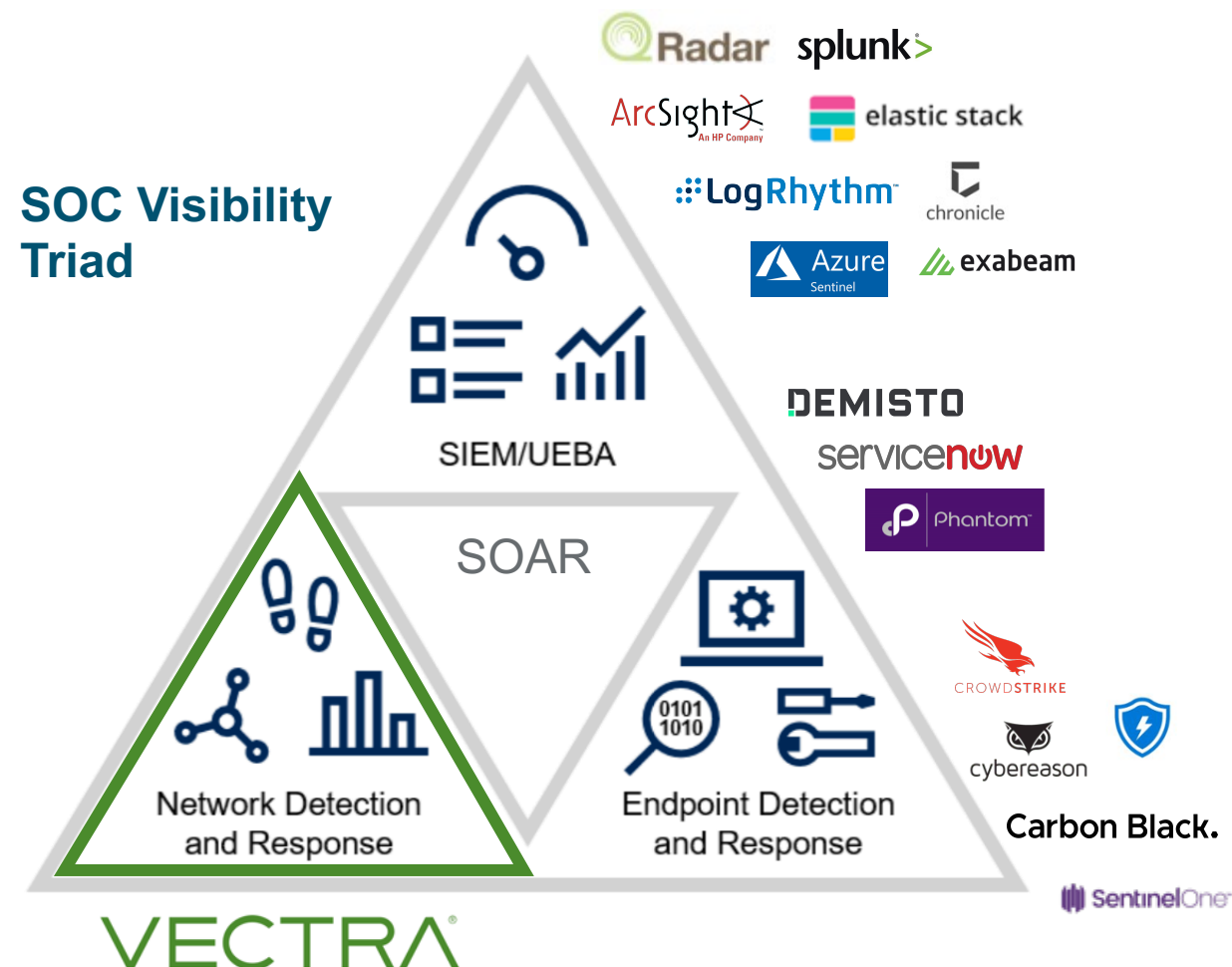
“

Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents.

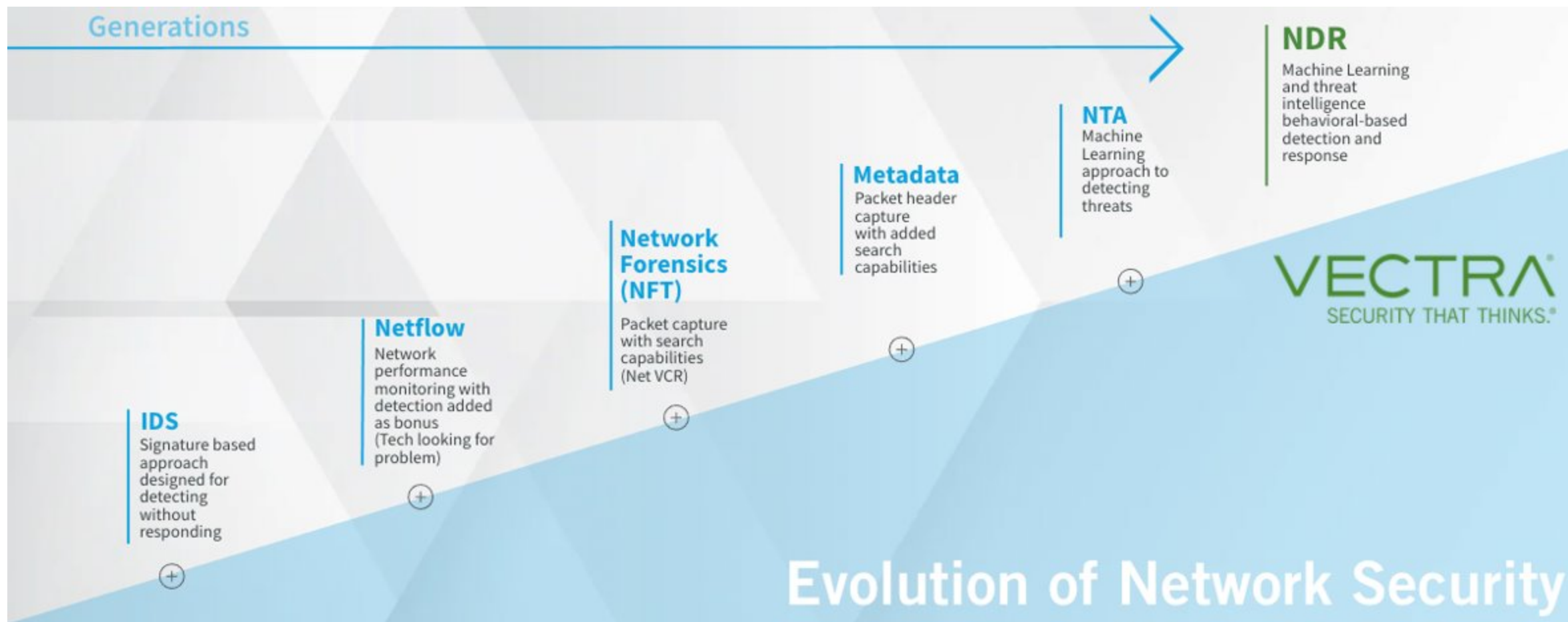
”

Source: Applying Network-Centric Approaches for Threat Detection and Response  
March, 2019  
ID Number: G00373460

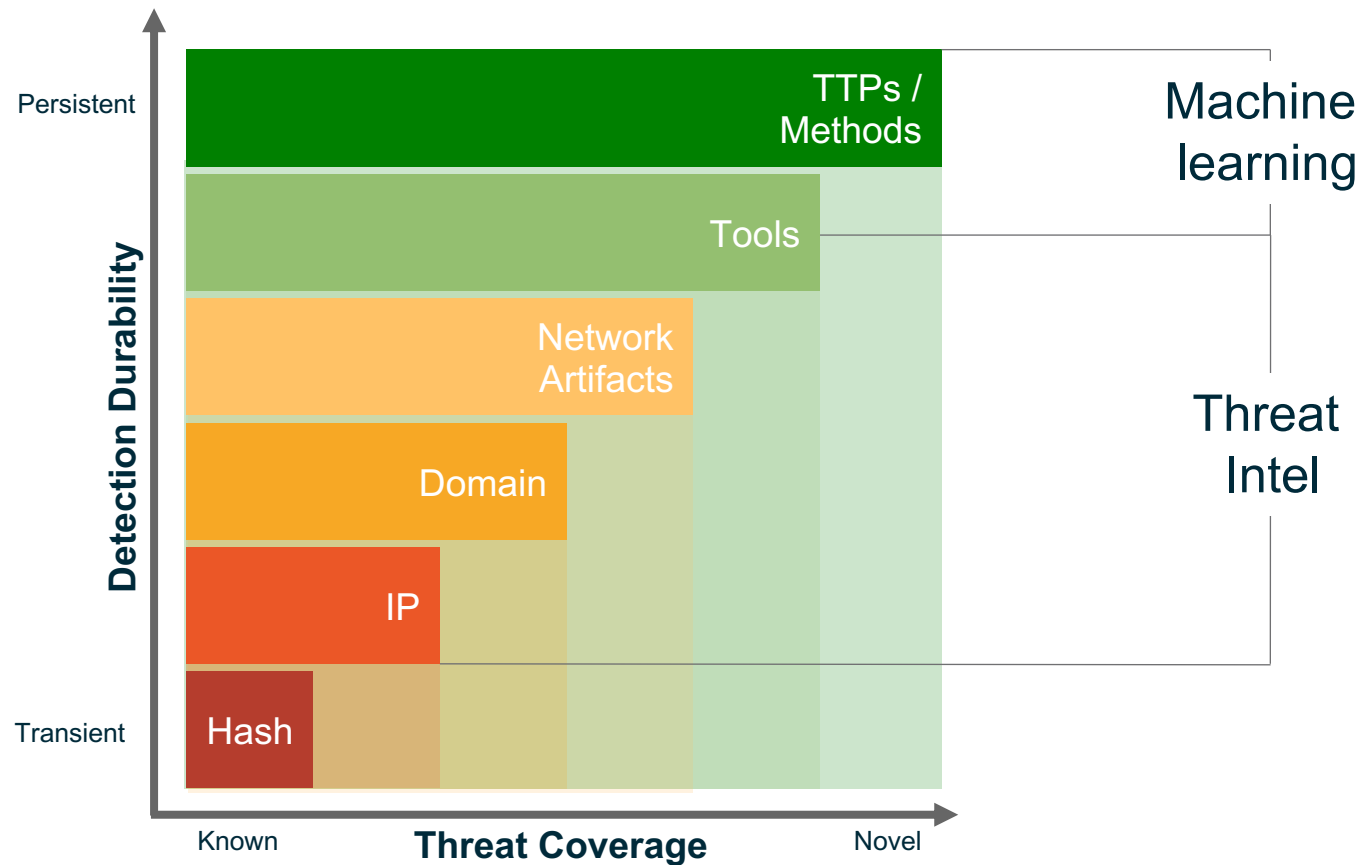
All statements in this report attributable to Gartner represent Vectra's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.



# Временная шкала Network Security



# Использование ИИ помогает бороться с известными и неизвестными атаками и векторами атак



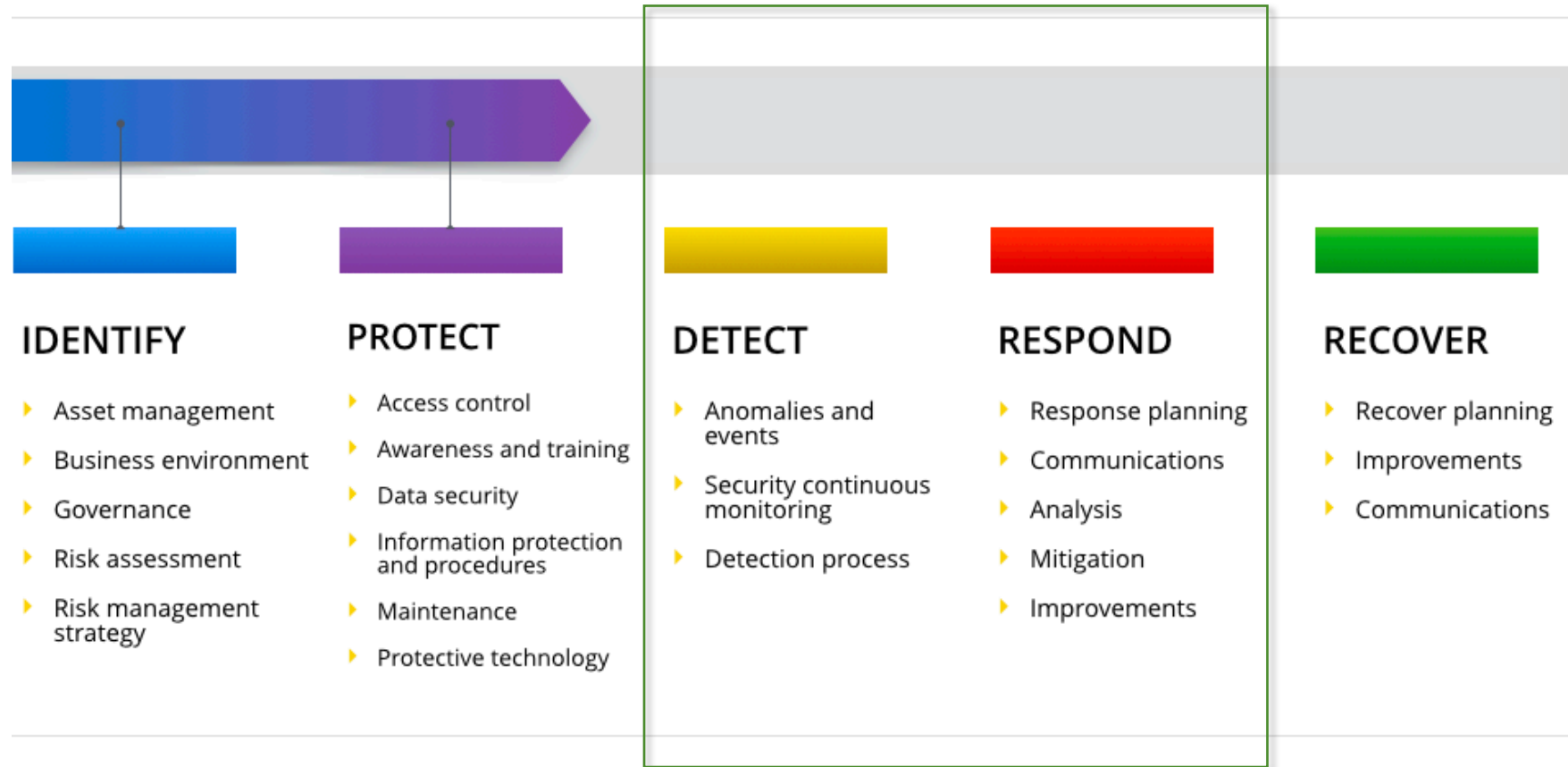
## Durable coverage through Vectra AI

- ▼ Focused on what the threat actor is doing
- ▼ Both novel and known attacks
- ▼ Cover attack vectors: IT, IoT, IaaS & O365

## Labeled coverage of known threats

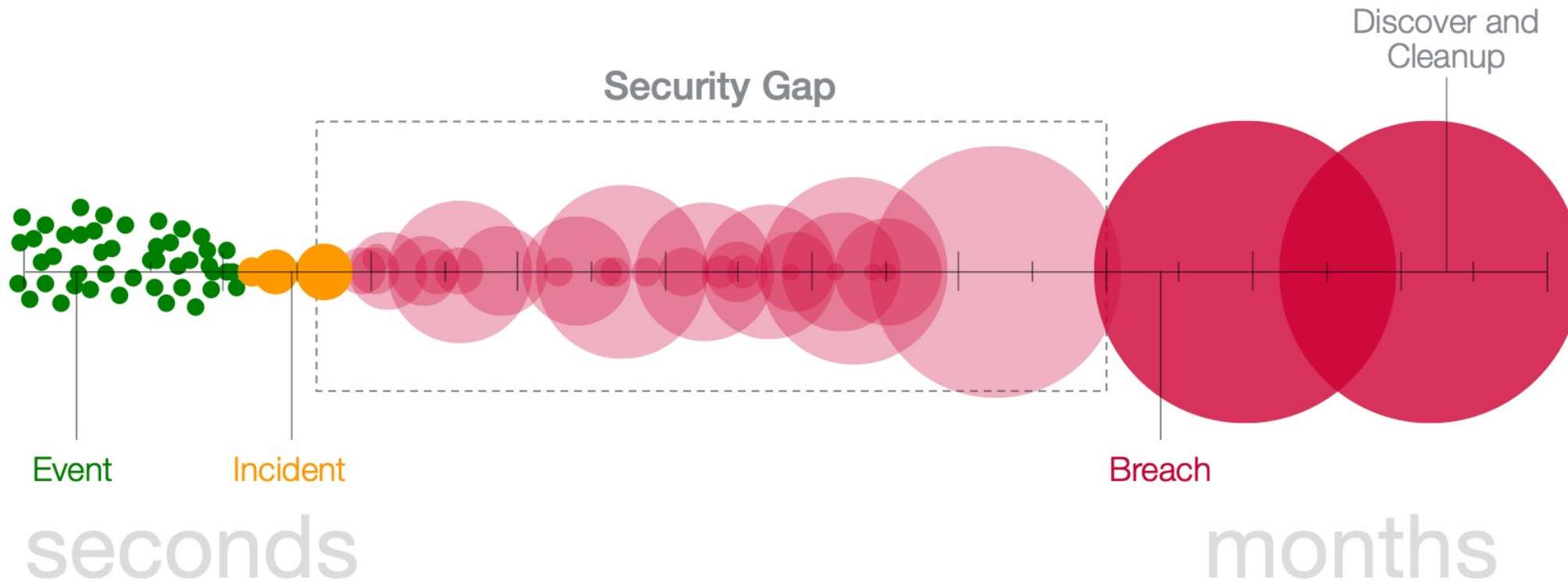
- ▼ Vectra Threat Intelligence is fully managed and curated by Vectra
- ▼ Domains, IP addresses and in-use attacker tools

# Threat Detection & Response



Source: NIST Cyber Security Framework

Vestra останавливает **ИНЦИДЕНТЫ** предотвращая **ВЗЛОМЫ**.  
Детектирование атаки по поведению



# Типовая атака на компанию

What a sophisticated attacker, an APT group and malware do through the Cyber Kill Chain

## Initial access and compromise

- Inside attacker
- Phishing emails and websites
- Exploiting vulnerabilities
- Hardware additions
- Removable media
- Compromised accounts
- SaaS control plane

## Command&control and persistence

## Reconnaissance

Hidden communication with attacker's systems.

Setting up utilities on the compromised systems.

Searching the network for accounts, hosts, service and data.

## Gain more privileges and access

## Move laterally

Elevating privilege levels and moving towards the objective.

Accessing and compromising additional systems and accounts.

## Steal or delete data

## Encrypt and manipulate data

## Hijack resources and build botnets

The breach.

# Объединяем анализ угроз и науку о данных.

Data scientists and security researches build and continually tune self-learning behavioral models that enrich metadata with machine learning-derived security information.

## Security Research

Fundamental attacker behaviors sourced from securing the world's most sensitive assets



## Data Science

Team of **PhD data scientists** who codify behaviors across unsupervised, supervised and deep learning models

## Security Analyst in Software

97% of the MITRE ATT&CK framework

Security **enrichments** (e.g. privilege)

Automate Tier-1 activities: **34X workload reduction**



# Vectra использует науку о данных

## Global Learning



Что: Найти скрытые черты, которые есть у угроз в общем

Зачем: Быстрое детектирование плохого поведения, не требуется локальное обучение

Как: Supervised machine learning

Пример: Random Forest (алгоритм машинного обучения)

## Local Learning



Что: Обучение нормальному поведению и поиск признаков атак

Зачем: Выявить следы атаки, уникальные в сети

Как: Unsupervised machine learning

Пример: K-means clustering (метод кластеризации)

## Integrated Intelligence



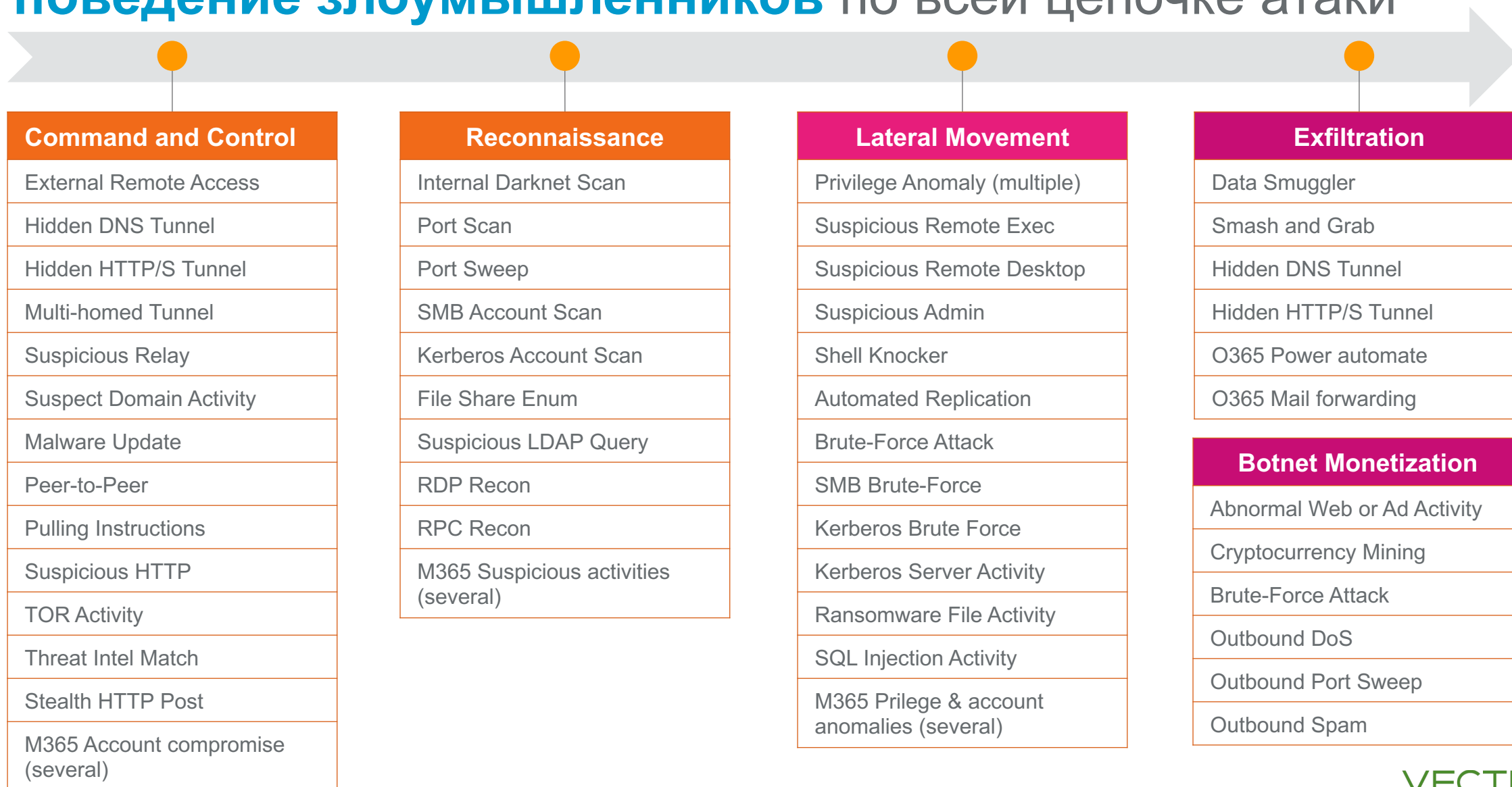
Что: Автоматический скоринг хостов чтобы показать общий уровень зараженности в сети

Why: Быстро отбросить ненужные события, чтобы показать ключевые моменты атаки

How: Отслеживание событий во времени во всех фазах атаки

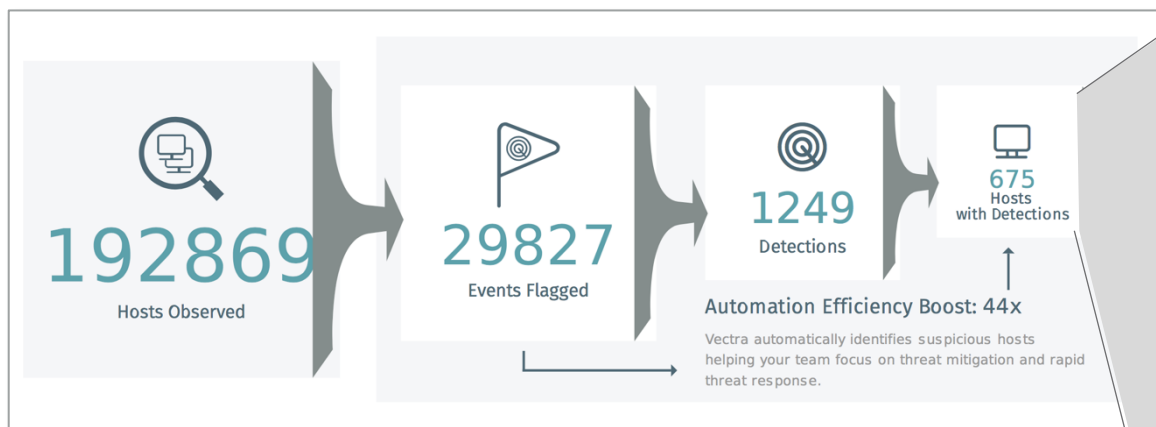
Пример: Bayesian network (графовая вероятностная модель)

# Vectra детектирует поведение злоумышленников по всей цепочке атаки



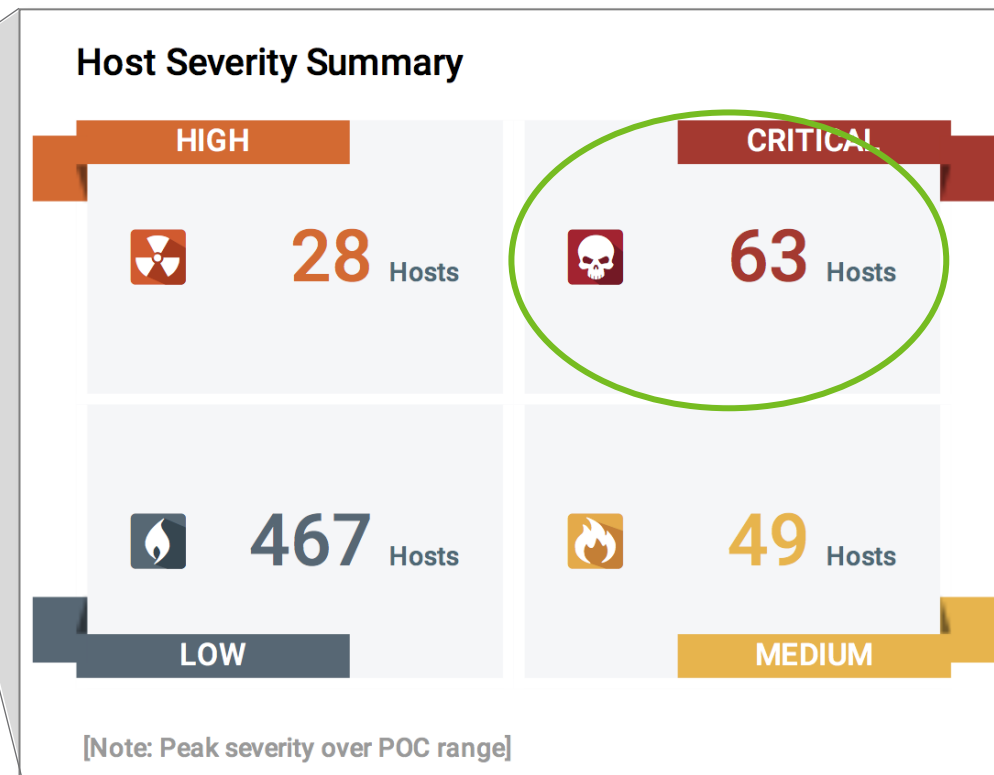
# Низкий шум & высокая точность

*Vectra дает вам это*



**Большинство NDR делают это**

- ▼ 200K hosts monitored  
Sophisticated detection capability  
Accuracy/relevance of detected behaviors



**Бизнес получает = Снижение нагрузки на SOC**

**Cognito отделяет высокоточные сигналы от ежедневного шума**

Source: Actual customer environment in a large multinational enterprise

# Наиболее точное и эффективное решение для детектирование известных и неизвестных угроз



SIEM/logs не дают полный, глубокий, детализированный вид.  
EDR не везде установлены и могут быть обмануты. Когда что-то случается, это всегда видно в сети.

→ **Vectra может детектировать такие атаки, которые другие не могут**



Vectra's AI комбинирует как поведение атакующего, так сетевые аномалии при помощи продвинутой аналитики и корреляции

→ **Лучшее детектирование “signal to noise ratio” в реальном времени**



Vectra интегрируется в экосистему SOC

→ **Прямо из коробки с большинством систем, открытый API**



Безагентское внедрение, самообучение, интуитивный пользовательский интерфейс

→ **Продуктивность работы аналитика вырастает в разы**



Минимум ложных срабатываний, приоритезация угроз, автоматизация реагирования на инциденты

→ **34x снижение временных затрат SOC Level-1,  
Переход от анализа инцидентов к триажу всей атаки  
за считанные минуты**

Detect On-prem & Cloud

No decryption of traffic

No signatures

Maps 97% Mitre Att@ck

Can run 100% air-gapped

Comes with curated threat intel

---

Vectra is a pioneer in AI & NDR

Trusted by 500+ organizations

# Безопасность, которая думает.

Сценарии использования и положительное влияние на бизнес

## Снижение риска взлома



Детектирование атаки в процессе; предотвращение взлома



Понимание масштаба атаки

## Увеличение эффективности SOC



Оптимизация ROI



Реагирование на правильные инциденты в правильное время

## Выполнение требований регуляторов



Адаптация к стандартам регуляторов



Простая интеграция с существующими решениями ИБ

## Безопасность в облаке

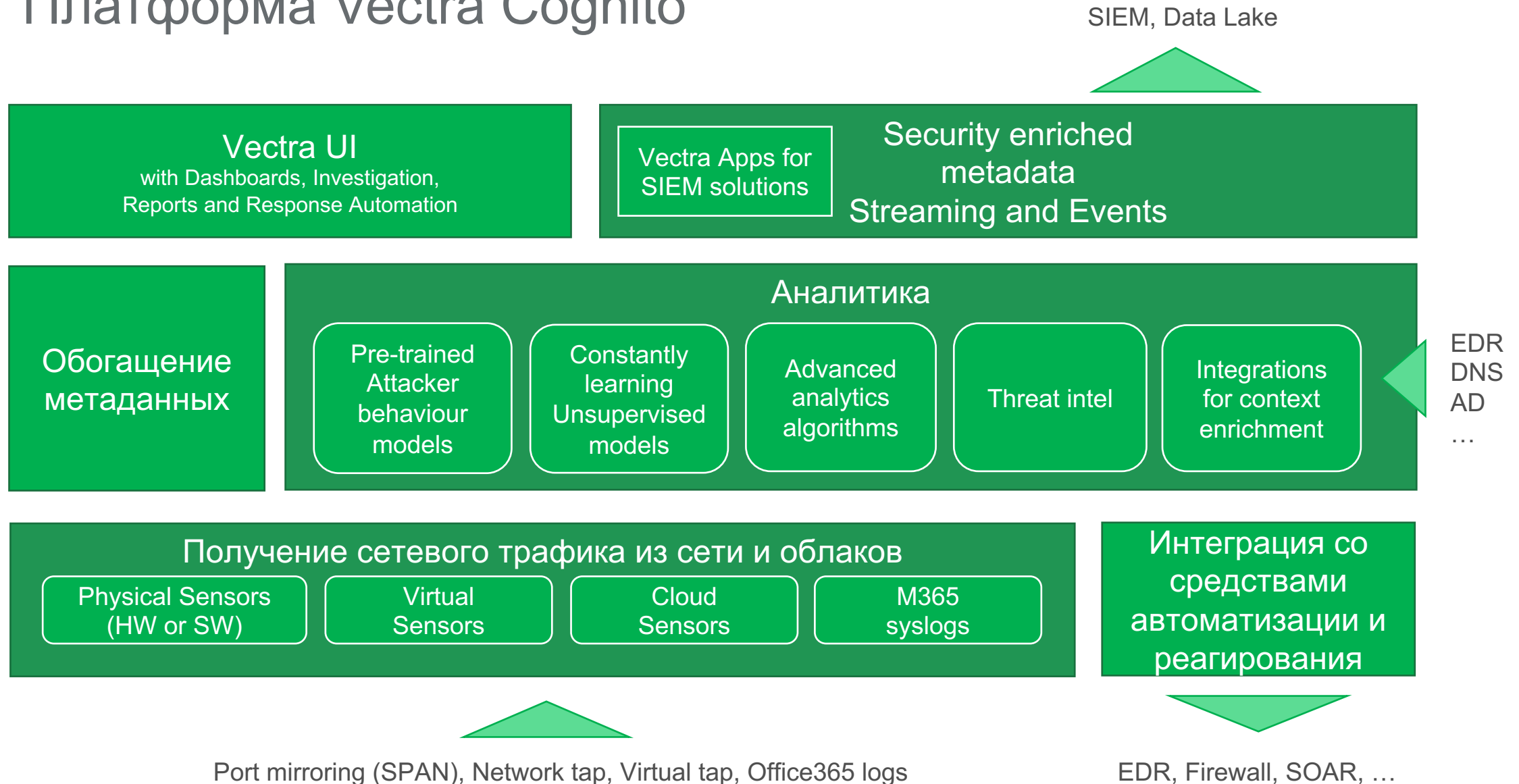


Визуализация приложений SaaS

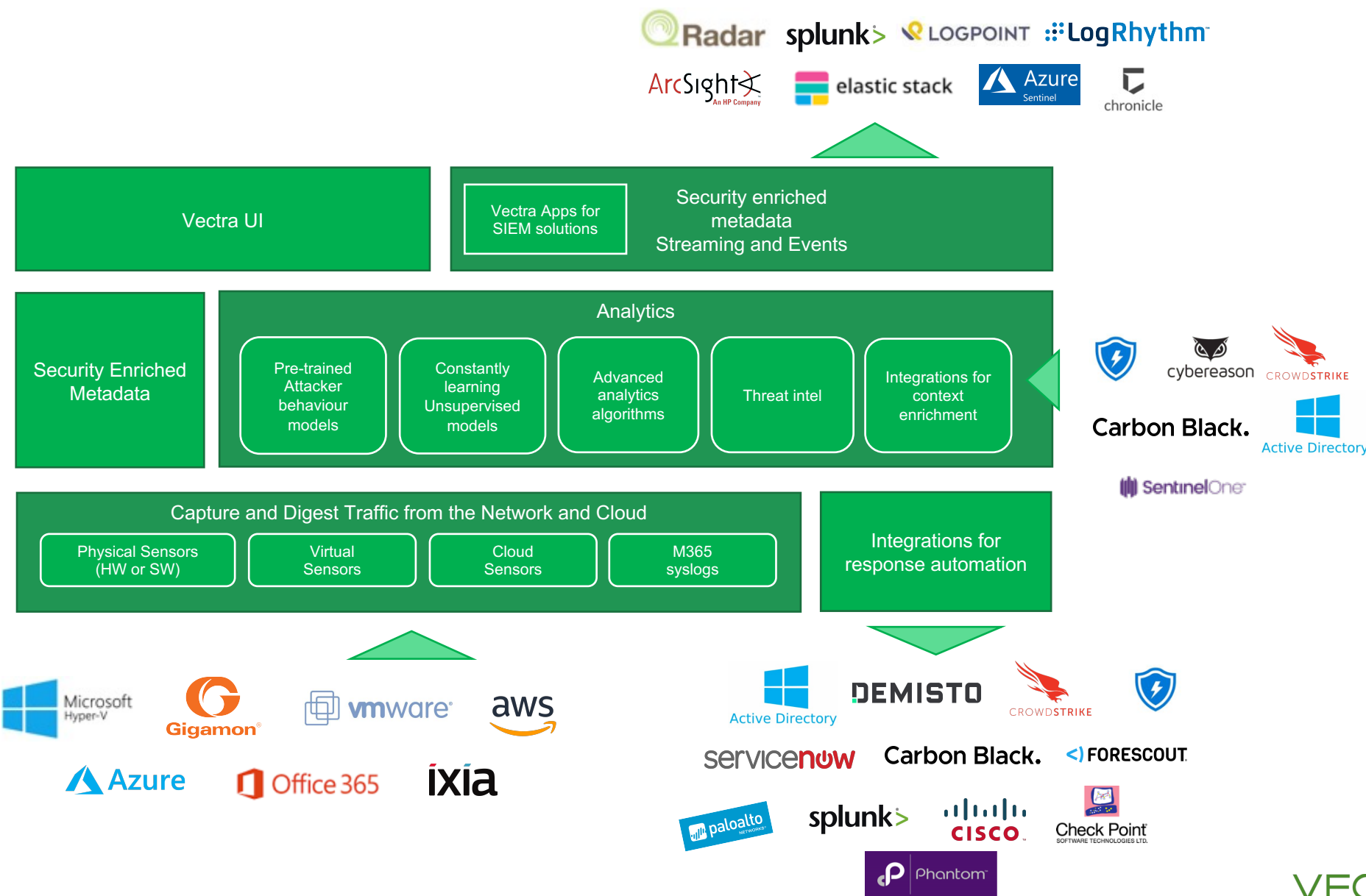


Защита цифровой трансформации

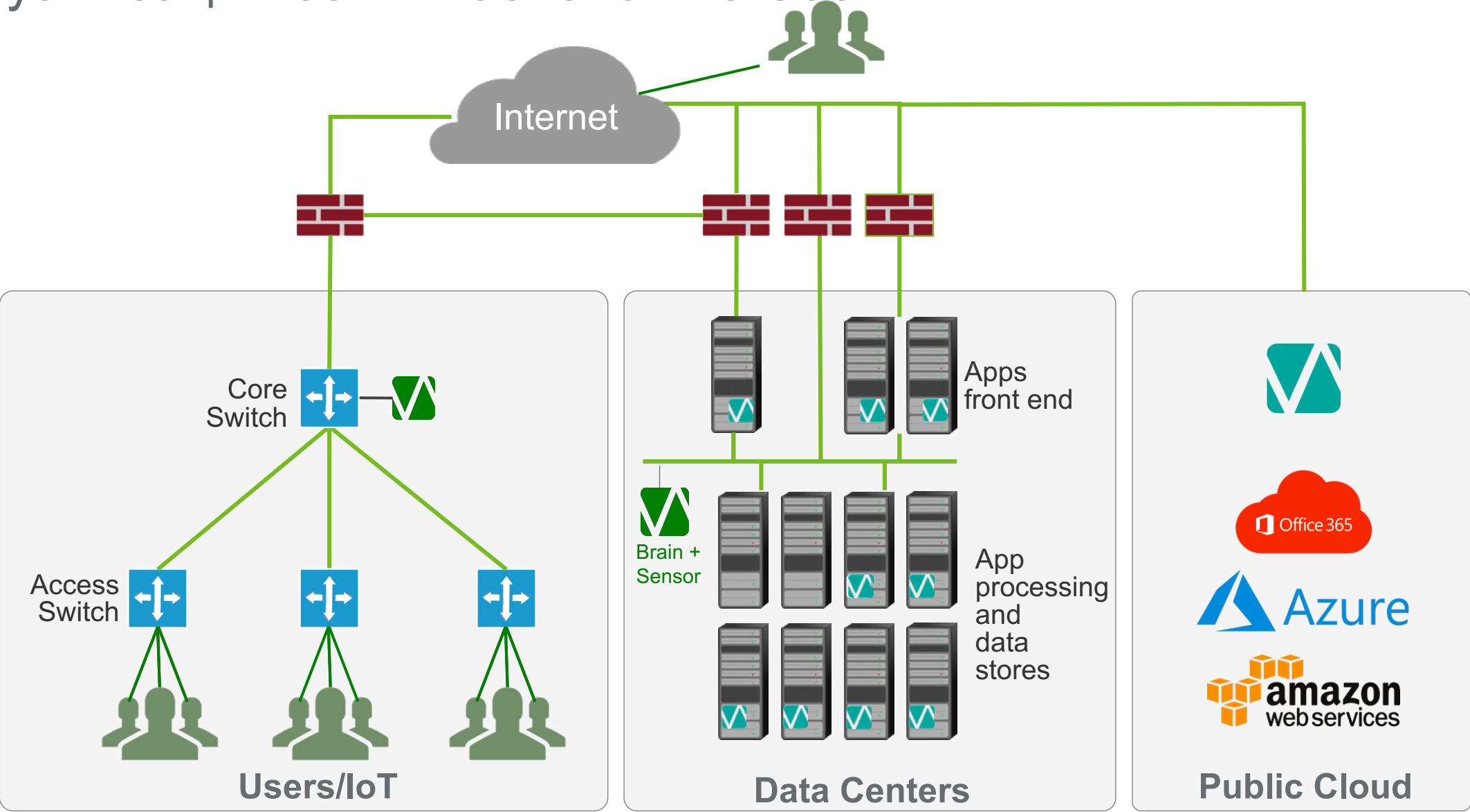
# Платформа Vectra Cognito



# Интеграция Vectra с инфраструктурой ИБ








# Визуализация сети и облаков на 360°





# Основные конкуренты - NDR

Network Traffic Analysis Capability	 <b>VECTRA</b> <small>Security that thinks.</small>	 <b>DARKTRACE</b>	 <b>ExtraHop</b>	 <b>CISCO</b>	 <b>corelight</b>
		<a href="#">Read detailed comparison</a>	<a href="#">Read detailed comparison</a>	<a href="#">Read detailed comparison</a>	<a href="#">Read detailed comparison</a>
Data source	Security-enriched network metadata	Network metadata	Network packet capture and NetFlow	NetFlow	Network metadata
Metadata streaming to data lakes and SIEMs	✓	✗	✗	✗	✓
AI-derived metadata enrichments	✓	✗	✗	✗	✗
Deep learning	✓	✗	✗	✗	✗
Supervised machine learning detections	✓	✗	✗	✓	✗
Unsupervised machine learning detections	✓	✓	✓	✓	✗
Imports IoCs for detection	✓	✗	✓	✓	✓

# Куда продаем?

- Замена IDS/IPS
- SOC (Gartner)
- Переход в облака

# Рынок IDS/IPS движется в сторону NDR

**Market Size: Enterprise Network Security Equipment, by Segment, Worldwide, 1Q20 (Millions of Dollars)**

Segment	Vendor Revenue, 1Q20	Vendor Revenue, 4Q19	Vendor Revenue, 1Q19	Revenue Share, 1Q20	Revenue Share, 4Q19
Enterprise Network Security Equipment	2,772.0	3,554.6	2,668.1	100.0%	100.0%
Firewall	2,218.5	2,738.8	2,151.8	80.0%	77.1%
Network Detection and Response <sup>1</sup>	164.9	206.5	120.2	5.9%	5.8%
IDPS <sup>2</sup>	216.6	371.2	230.7	7.8%	10.4%
Network Access Control	172.0	238.0	165.4	6.2%	6.7%

<sup>1</sup> Network detection and response (NDR) was previously referred to as network traffic analysis (NTA) by Gartner.

<sup>2</sup> IDPS = intrusion detection and prevention system

Source: Gartner (June 2020)

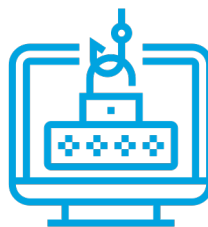
# Проблемы рынка IDS/IDPS

## IDPS ведет к усталости от тревоги



- ▼ IDPS основаны на сигнатурах и статичных правилах для детектирования угроз
- ▼ Без дополнительного контекста (как например поведения хоста) генерят огромное количество ложных срабатываний и низкоуровневых алертов

## IDPS недостатки визуализации



- ▼ IDPS в составе FW не могут детектировать Lateral Movement
- ▼ Сигнатуры могут детектировать только известные атаки; неизвестные атаки или современные атаки основанные на учетных записях остаются невидимы

## IDPS громоздки



- ▼ Правила и сигнатуры IDPS требуют постоянного обновления и настройки.
- ▼ Требования регуляторов требуют статичные установки, что не дает полноценно работать решению, а сигнатуры быстро устаревают.

# Value Proposition

	For:	Product is:	Ideal for:	Better than:	Because:
Key Criteria	<i>Ideal Customer Profile</i>	<i>Product Pitch</i>	<i>Use Cases</i>	<i>Competition</i>	<i>Differentiation and Proof Points</i>
Our Product	<ul style="list-style-type: none"> <li>Any organization that has an IDPS deployed</li> <li>Director/Manager of IT/Security</li> <li>IT Security Analysts</li> </ul>	<p>Vectra Cognito, with its real-time automated threat hunting capabilities, is the ideal replacement for today's IDPS products that cannot block contemporary cyber attacks and cannot detect hidden attacker behaviors inside your network.</p> <p>The Cognito Platform focuses on detecting and mitigating active threats inside the network – from users to IoT devices to data centers and the cloud.</p>	<ul style="list-style-type: none"> <li>Detect advanced, post-compromise behavior</li> <li>Reduce Alert Fatigue</li> <li>Visibility into Unknown threats</li> <li>Network-based Intrusion detection</li> <li>Shifting to a behavioral approach for threat detection</li> </ul>	<ul style="list-style-type: none"> <li>IDPS Vendors</li> <li>NDR Vendors</li> </ul>	<p><b>Attacker behavior instead of Generic Anomaly Detection</b>  <b>Proof point: American University</b>            “We want to spend more time doing what’s beneficial for the university, which is protecting it – not upgrading custom software and sifting through signatures”</p> <p><b>Prioritize Threat Detection and Investigation</b>  <b>Proof point: ED&amp;F Man Holdings</b>  <i>“Cognito was to install and we get immediate visibility into attacker behaviors that hide in traffic”</i></p> <p><b>Proof point: Gartner MG for IDPS</b>  <i>“Vectra addresses the issue of alert fatigue. This solution excels at the ability to roll up numerous numbers of alerts to create a single incident to investigate that describes a chain of related activities, rather than isolated alerts that an analyst has to piece together.”</i></p>

# Ideal Customer Profile

## Target Market (who they are)

<b>Annual Revenue</b>	\$50M - \$500M+
<b># Employees</b>	500 – 50,000+
<b>Industry</b>	Manufacturing, Healthcare, Energy & Utilities, Financial Services, Higher Education, SLED, Government, Technology
<b>Needs</b>	Meet Compliance Regulations, stop attacks that have made it past perimeter defense, reduce workload on security analysts

## Environment (their situation)

<b>Technology Landscape</b>	Existing IDPS Users, has implemented or looking into next generation technologies (CrowdStrike, Splunk, etc.)
-----------------------------	---

### Business Buyer Persona

<b>Title</b>	Director/MGR of IT, IT Security, SOC
<b>Responsibility</b>	Responsible for IT infrastructure/security
<b>Technology Skills</b>	Basic understanding of IT/security tools.
<b>Pain-points</b>	Poor ROI on existing security investments, staff burn-out, incomplete understanding of the attack surface, reactive to threats
<b>Positioning</b>	Position SOC efficiency, improved ROI across security program, increased staff productivity

### Technical Buyer Persona

<b>Title</b>	Security Analyst, SOC Analyst, Network Analyst, IT Analyst
<b>Responsibility</b>	Manages IDPS
<b>Technology Skills</b>	Runs the cybersecurity arm to protect the businesses infrastructure
<b>Pain-points</b>	Too many alerts, too many signatures to maintain, lack of visibility into what's inside of the network
<b>Positioning</b>	Behavioral approach, automation, prioritized threats and high-fidelity alerts

# Qualification Criteria

Criteria	Description
Annual Revenue	50M – 500M+
Contact	Manager, Director, VP, or C-Level Decision-Maker
Buying Stage	Evaluation/Purchase to be completed within 9 months
Need	Adhere and meet compliance, detect and respond to threats that have passed perimeter defenses
Desire	Actionable alerts + guided response, less maintenance and tuning work for security analysts
Technology fit	Any organization that currently has an IDPS deployed
Actions	Prospect Agreed to an introduction call to discuss their pain (Before Scenario/Negative Consequence) and discuss their ideal state (After Scenario)

# Ключевые моменты для разговора о замене IDPS

Чем недоволен заказчик?

1

## Усталость от тревоги

(отношение сигнал/шум)  
IDPS генерят очень  
много событий

2

## Известные/ Неизвестные атаки

IDPS основаны  
на сигнатурах

3

## Содержание и поддержка

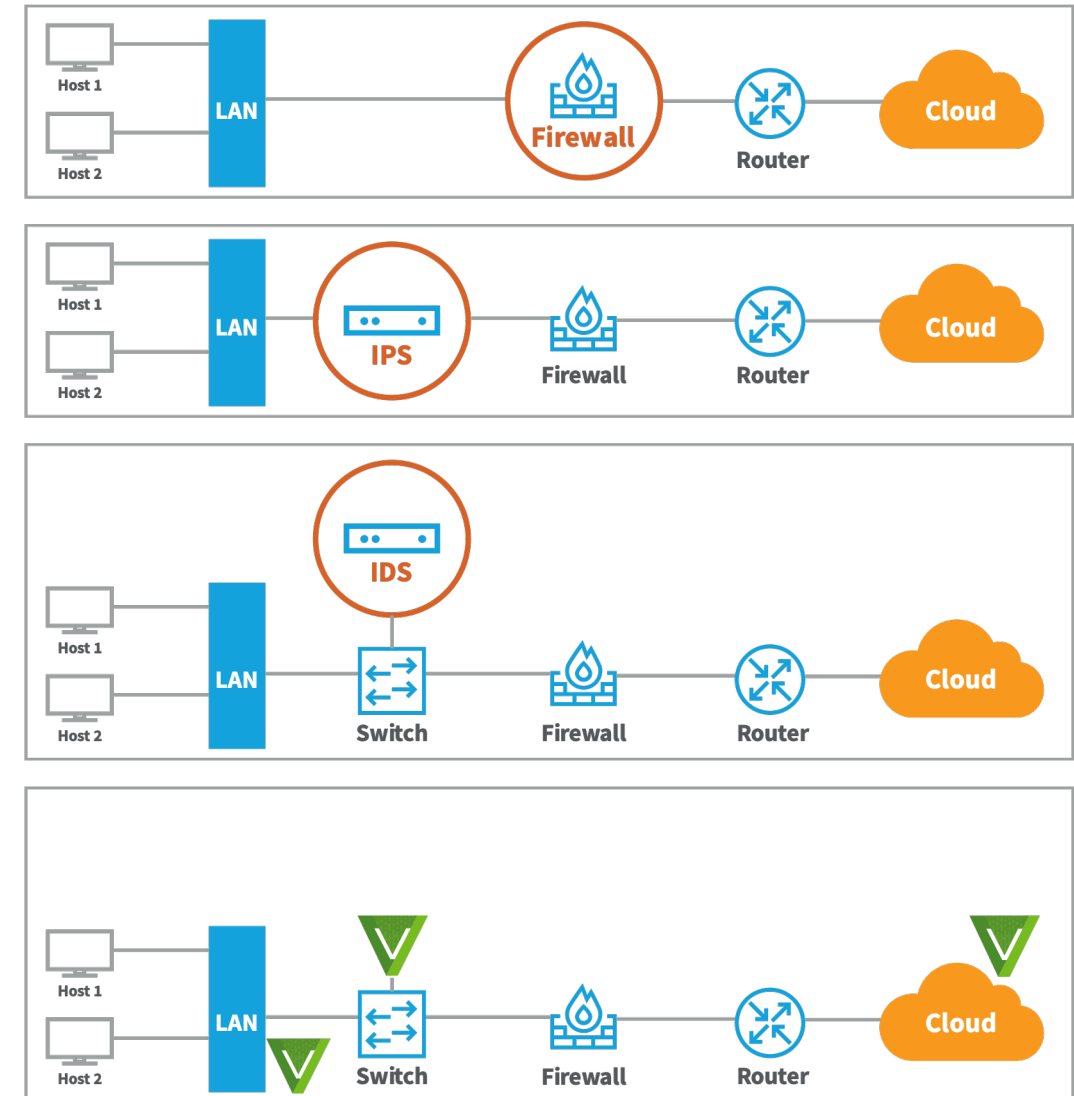
IDPS требуют  
постоянной настройки и  
тюнинга



# IDS vs IPS vs Firewall vs NDR

Parameter	Firewall/IPS	IDPS	NDR
Abbreviation for	Firewall/Intrusion Prevention System	Intrusion Detection and Prevention System	Network Detection and Response
Usage	Filters ingoing and outgoing traffic based on manual rules + Inspect ingoing and outgoing traffic, stops known attacks based on signatures	Monitors traffic, sends alerts on policy violations or known attacks.	Monitors all network traffic, uses AI combined with signatures to stop threats
Principle of working	Filter based on IP and Port + Looks for signatures of attack, prevent that attack.	Looks for traffic patterns or signatures, generate alert.	Leverage AI with signatures to look for known and unknown attacks and stop them
Placement	Inline at network perimeter (Firewall)	Non-inline via Span port, or tap	Non-inline via Span port, or tap
Vendors	Palo Alto Checkpoint Cisco	<ul style="list-style-type: none"> <li>Cisco (Sourcefire)</li> <li>Alert Logic</li> <li>Trend Micro (Tipping Point)</li> <li>McAfee (Intrushield/Network Security Platform)</li> <li>Bro</li> </ul>	Darktrace ExtraHop Corelight / Zeek Awake PAN – Cortex Bricata

## Where's the IDS comparison\*\*\*



# Что дает NDR

Использование NDR для замены IPS/IDS

## Эффективность SOC

- ▼ Аналитик переключается с настроек сигнатур на анализ приоритизированных событий и поиска угроз.
- ▼ Объединенное решение для ЦОД и облаков

Vectra will provide a **90%+ efficiency improvement** from current anomaly-based detection approaches

## Выполнение требований регуляторов

- ▼ AI-based triaging (приоритезация инцидентов)
- ▼ При выполнении требований регуляторов

Compliance with **(PCI DSS) v3.2**  
And **(PA-DSS)**

## Снижение риска

- ▼ Детектирование известных и неизвестных атак.
- ▼ Перевод высоточных алертов в поведение
- ▼ Показ полного поведения в контексте

Automate Tier-1 activities:  
**34X workload reduction**

# This is Vectra.

Hundreds of  
global customers.



Highly  
recommended.

**97%** ON  
GARTER

Created by security professionals  
for security professionals.

Our core team consists of security researchers,  
data scientists, platform engineers, and UI designers.

Dozens of  
five-star ratings.



Vibrant  
cybersecurity  
community.



Recognized innovator and industry leader.

Only visionary in  
2018 MQ for IDPS



Technology innovator  
by EMA research



Visionary innovation  
by Frost and Sullivan



Deloitte 500 fastest  
growing technology



Approved for CDM  
Phase 3 DEFEND



Red Herring Global  
100 Winner



IDC Innovators: AI  
Security Solutions



CyberSecurity  
Breakthrough Awards



Computing  
Security Awards





VECTRA<sup>®</sup>  
SECURITY THAT THINKS.<sup>®</sup>