КИБЕРЗАЩИТА ДЛЯ ЦОД

Безопасность на всех уровнях хранения и обработки данных

Амир Алиев, консультант по ИБ

aaliev@checkpoint.com

Возникновение гибридного датацентра

Защита гибридного датацентра – серьезная проблема

“ С какими из следующих конкретных проблем вы столкнулись, реализуя свою текущую стратегию гибридных технологий?

FORRESTER®

Всплеск продвинутых кибератак на ЦОД

SUNBURST

18 000 центров обработки данных взломаны с помощью инструмента мониторинга SolarWinds

DARKSIDE

$4.4M потерь из-за горизонтального распространения вирусов-вымогателей, шифрующих критически важные системы управления.

CONTI

700GB записей пациентов утекли из центра обработки данных и были уничтожены

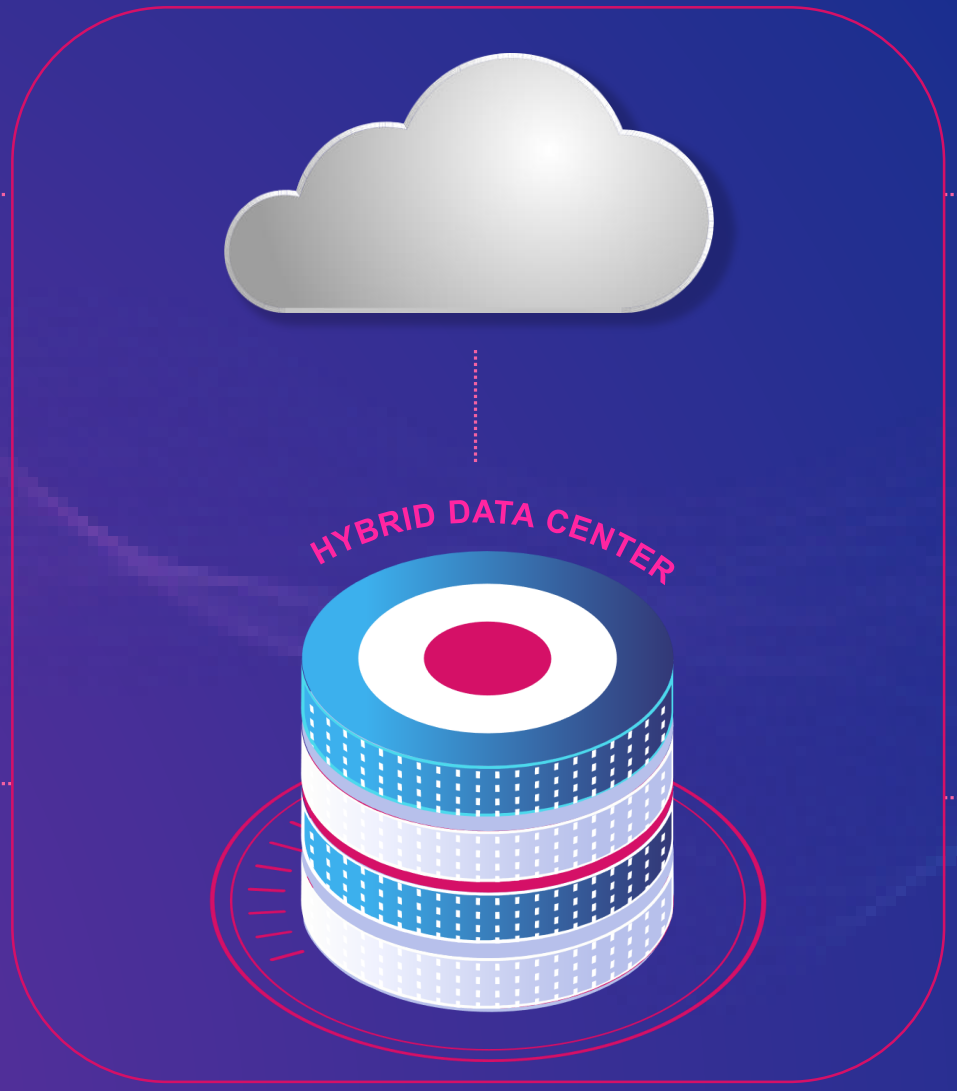
Почему так сложно защитить современный ЦОД?

ЦЕНТРАЛИЗОВАННЫЙ КОНТРОЛЬ:

Невозможность контролировать распределенные локальные и мультиоблачные системы

РАСТЯНУТЫЙ ПЕРИМЕТР:

Разрешить пользователям безопасно подключаться к ЦОД и облаку из любого места



ГИБКОСТЬ:

Сетевая безопасность для ЦОД снижает скорость и гибкость DevOps

МАСШТАБИРУЕМОСТЬ:

Трафик между ЦОД и облаком ежегодно увеличивается вдвое

Check Point
SOFTWARE TECHNOLOGIES

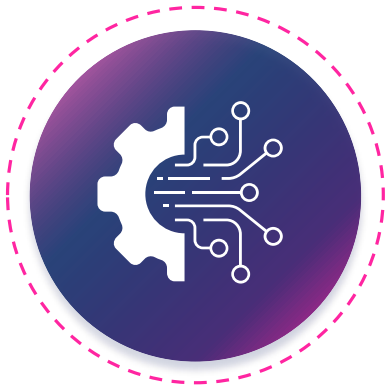
Защитите гибридный датацентр
Производительность и масштабируемость без усложнений

Улучшенный AI и ML Предотвращение угроз

Предотвращайте продвинутые атаки, горизонтальное распространение и атаки на бизнес-процессы

Автоматизация операций в ЦОД

Оптимизируйте процесс управления безопасностью с помощью API

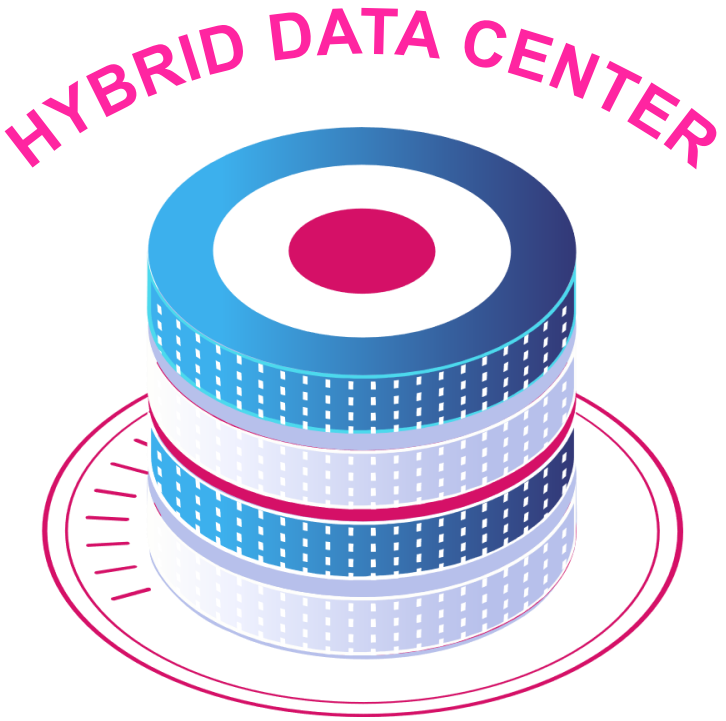


Консолидированное управление безопасностью

Эффективное и унифицированное управление безопасностью и соблюдение стандартов

Предотвратить атаки нулевого дня до того, как они проникнут в ЦОД

- Zero-Day Prevention
- Workload & Container Security
- Application Security for Web & API



Уникальная система предотвращения угроз с ML и AI, разработанная для гибридных датацентров

Quantum

Высочайшая эффективность безопасности

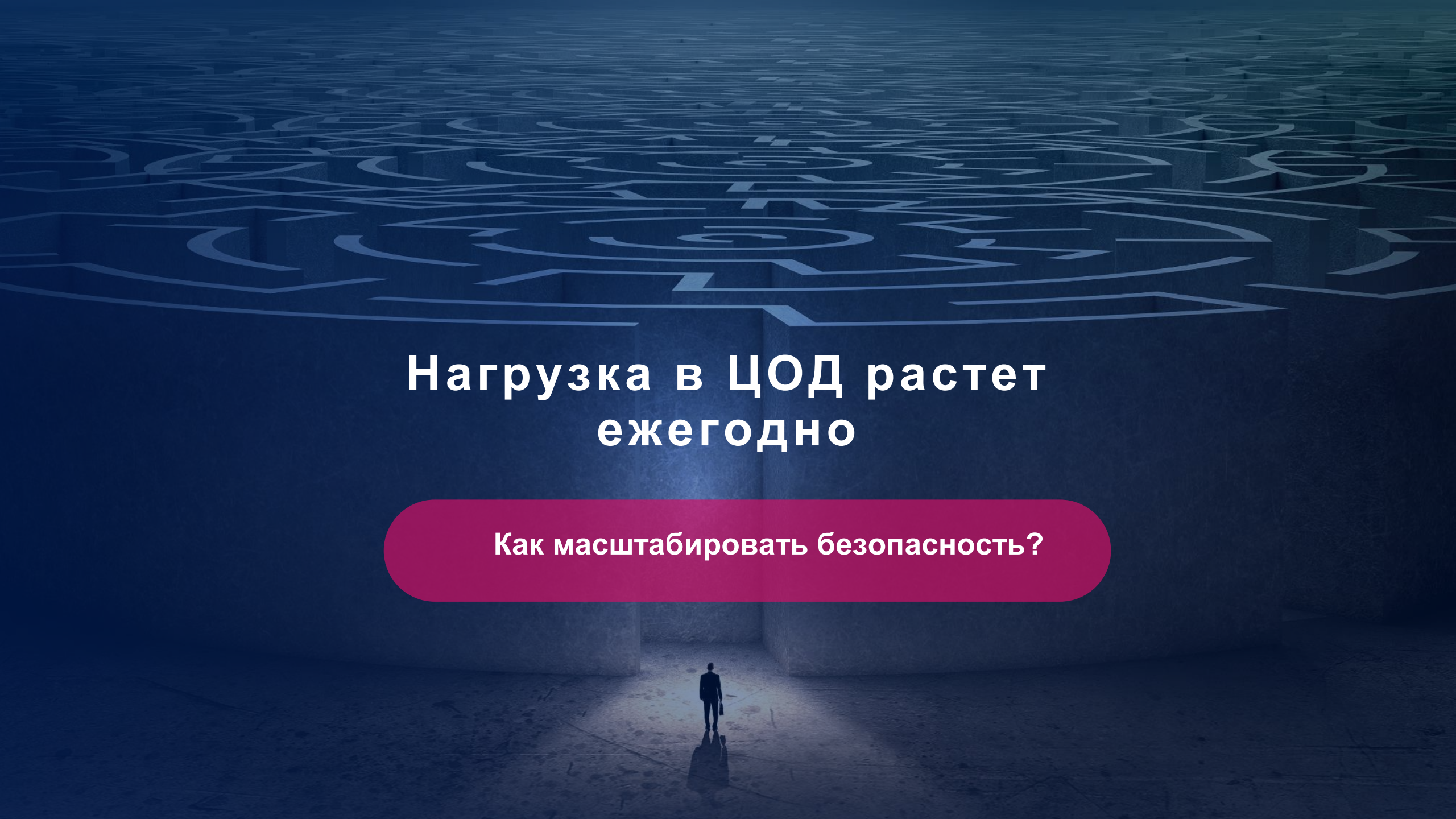
- 100% block rate (NSS)
- 0% false positives (NSS)

Более 60 механизмов предотвращения угроз

- CPU-Level Inspection
- Threat Extraction
- Malware DNA
- NG WAF
- Anti-malware
- Kubernetes runtime security
- Vulnerability scanning

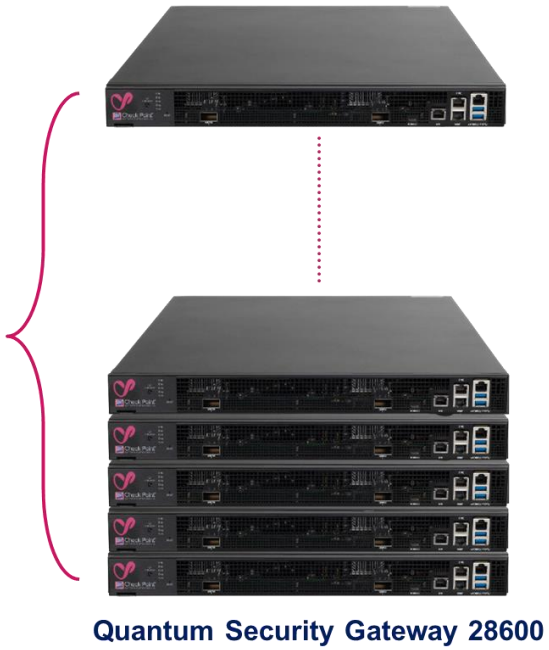
Аналитика угроз в реальном времени

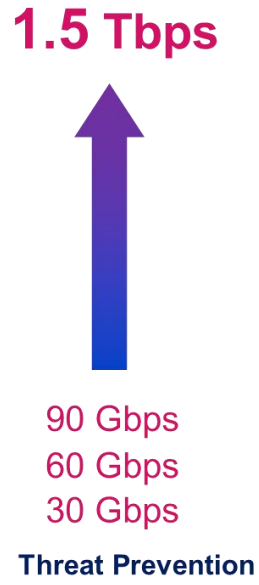
- 3B websites and files
- 150,000 connected networks
- Prevent Zero-day attacks


Нагрузка в ЦОД растет ежегодно
Как масштабировать безопасность?

Гипермасштабируемое решение безопасности №1

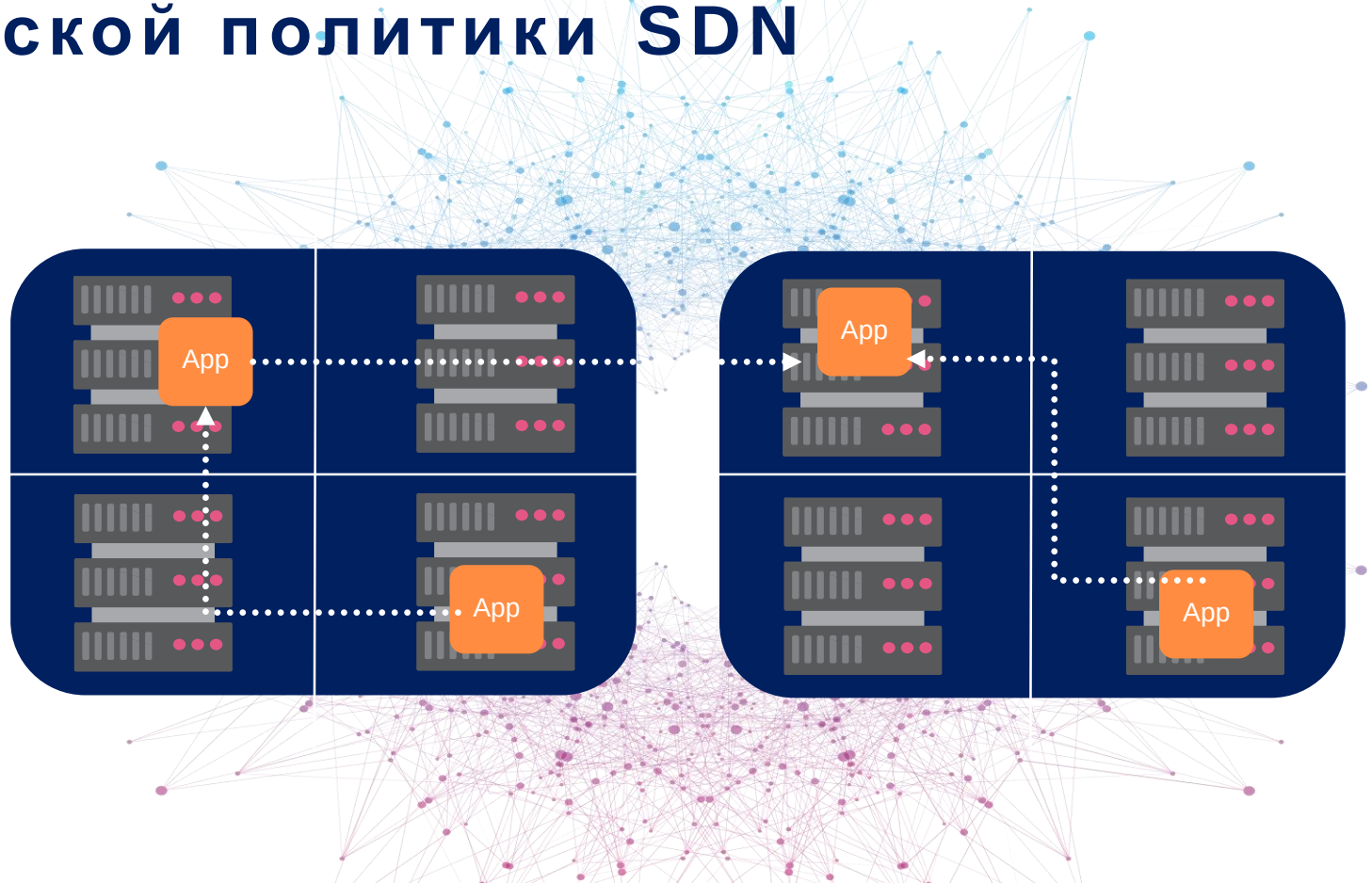
- Масштабирование за минуты
- Масштабирование без простоев
- Экономическая эффективность





Автоматизация межсетевого экрана ЦОД с помощью динамической политики SDN

- Политика, управляется динамическими объектами SDN
- Service chaining

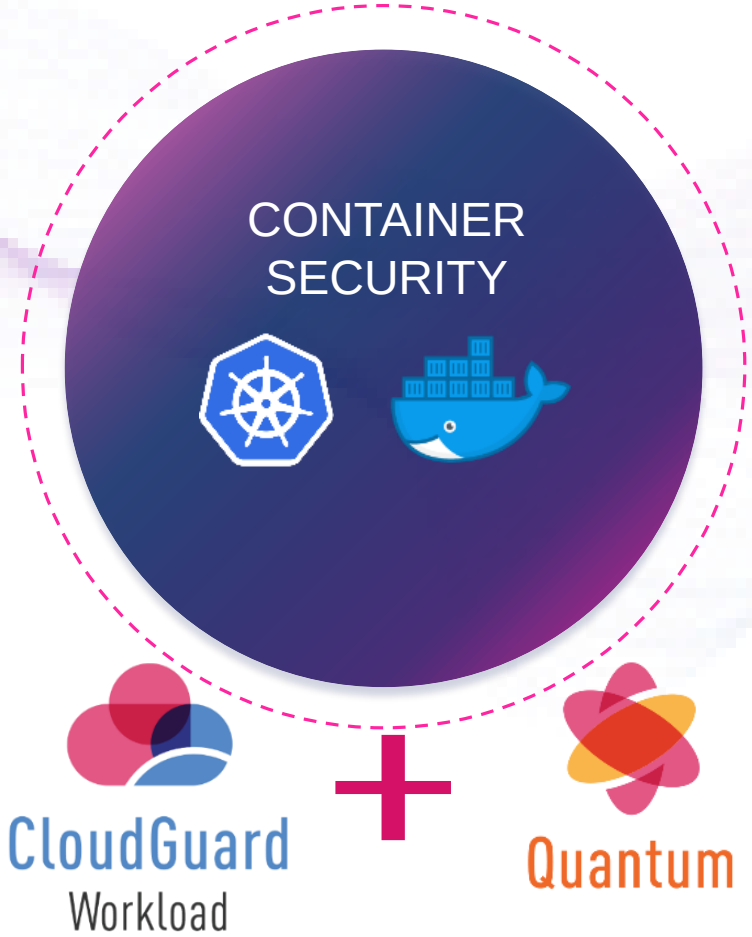


Тесная интеграция продуктов и партнерство

vmware NSX cisco ACI openstack.

Единая безопасность Kubernetes для ЦОД и облака

- Container Posture Management
- Open Source Vulnerability Scanning



- Adaptive Runtime Protection
- Secure Kubernetes Infrastructure

Расширяем безопасность ЦОД с помощью Check Point Next Generation WAF

Cloud Native WAF

Останавливаем OWASP Top 10

API Security

Защищаем API

Bot Prevention

Предотвращаем автоматизированные атаки

Intrusion Prevention

Защищаем инфраструктуру приложений

APPSEC POWERED BY
CONTEXTUAL AI

Автоматизация 90% изменений с помощью адаптивной политики менее чем за секунду

Идентификация пользователей и устройств

okta · PingIdentity · Azure Active Directory

DPI для приложений

SAP · JIRA · servicenow

13	Policy for access to Data Center servers	Any	Data Center LAN	Any	Any	Any	Data Center Layer
13.1	Datacenter Remote Access	Finance User	ERP Server	RemoteAccess	SAP	Any	Accept
13.2	Datacenter Segmentation	Web Frontend	DB Backend	Any	MS-SQL	Any	Accept

Статические и динамические теги

cisco ACI · vmware vCenter · vmware NSX-T · aws · Azure

Бесшовная интеграция

SIEM

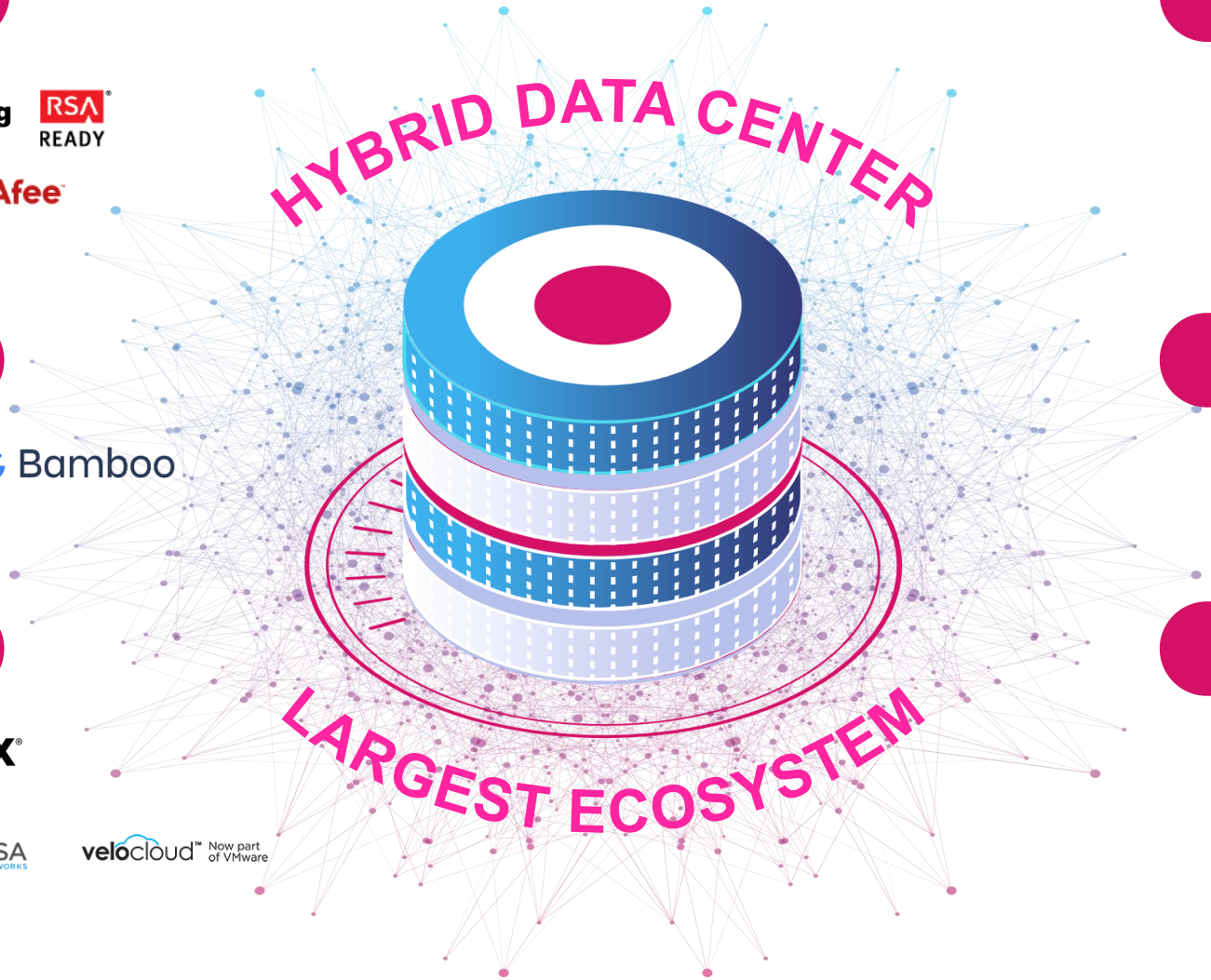
Radar · LogRhythm The Security Intelligence Company · syslog-ng · RSA READY · splunk> · ArcSight · McAfee

CI/CD FRAMEWORKS

GitLab · Jenkins · Bamboo

SD-WAN PARTNERS

aruba a Hewlett Packard Enterprise company · aryaka · CITRIX · CISCO · silver peak · VERSA NETWORKS · velocloud™ Now part of VMware



ORCHESTRATORS

openstack. · vmware vCenter · ANSIBLE · HashiCorp Terraform

NETWORKING

IPv6, IPv4 MODBUS

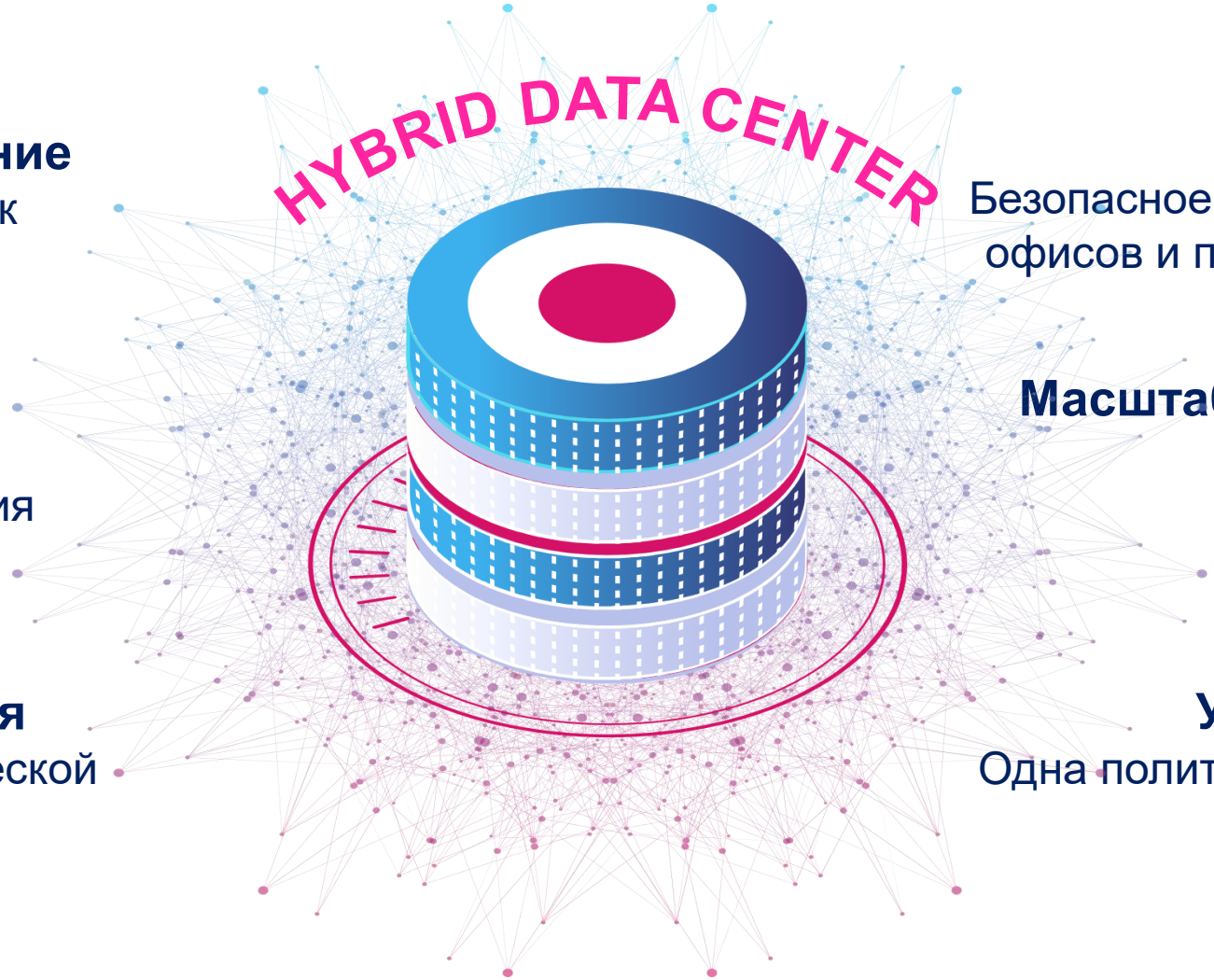
COMPLIANCE

PCI DSS HIPPA GDPR

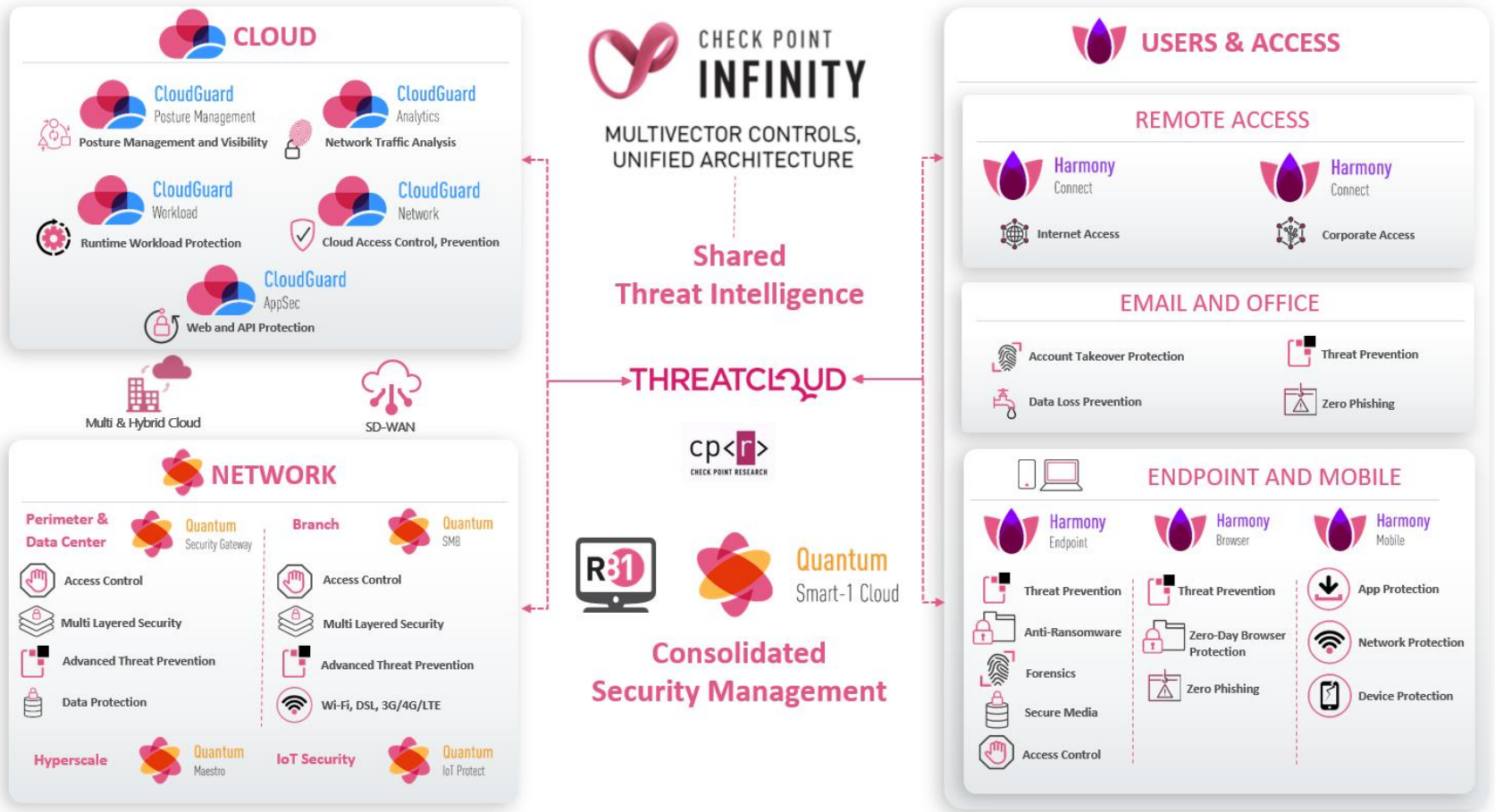
Подводя итоги

6 причин почему Check Point – лучшее решение для гибридных датацентров

- **Предотвращение**
  продвинутых атак
- **Изоляция**
  Zero Trust +
  микросегментация
- **Автоматизация**
  с API и динамической политикой



- **Связность**
  Безопасное подключение офисов и пользователей
- **Масштабируемость**
- **Унификация**
  Одна политика для всего



Контакты:

Амир Алиев
+7 985 645 68 36
aaliev@checkpoint.com

Виктор Крымский
+7 916 489 94 18
vkrymskiy@checkpoint.com

Check Point
SOFTWARE TECHNOLOGIES LTD

СПАСИБО

Амир Алиев, консультант по ИБ

aaliev@checkpoint.com