КОД ИБ ИТОГИ
МОСКВА 05 ДЕК'19

ОПЫТ МЕЖДУНАРОДНОЙ РАБОТЫ РОССИЙСКОГО ВЕНДОРА

Андрей ГОЛОВ
Код Безопасности

КОД БЕЗОПАСНОСТИ

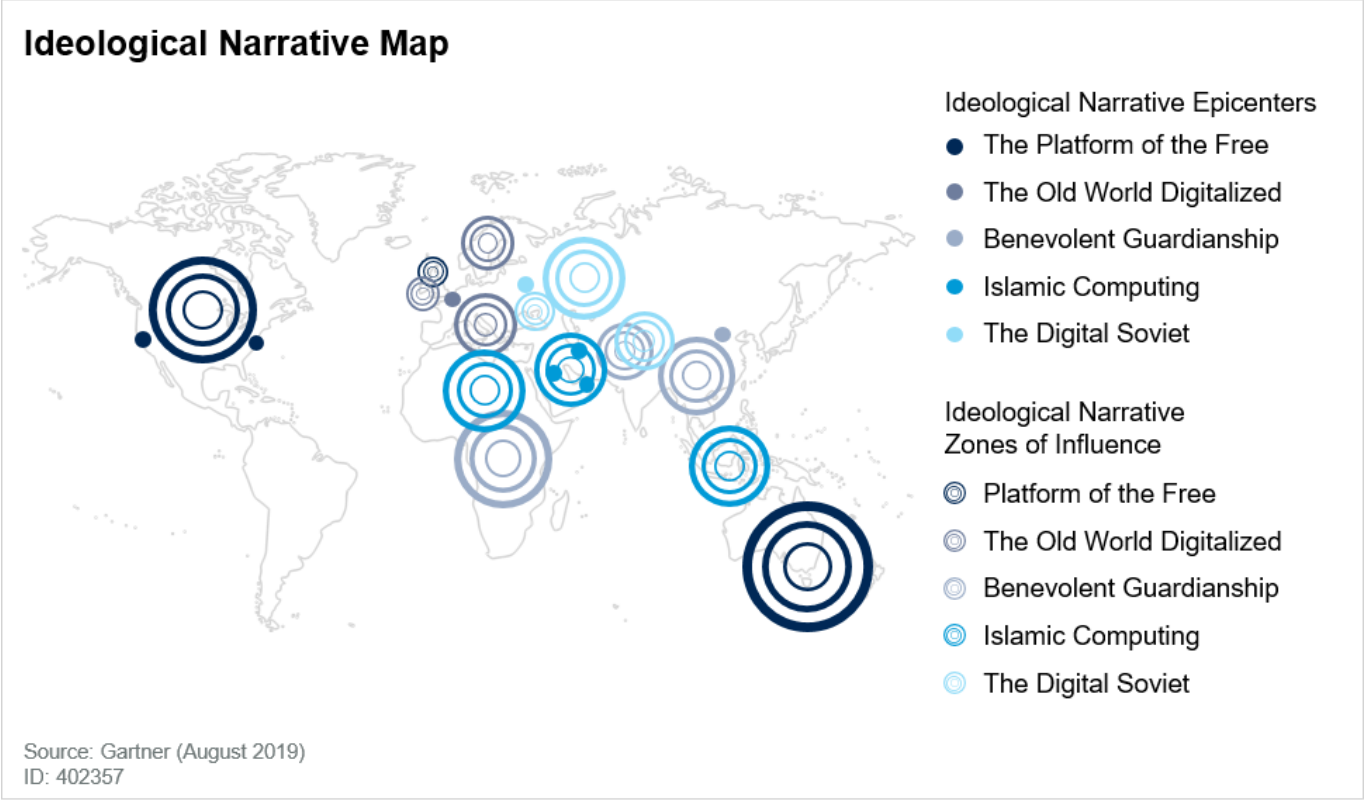
Балканизация Интернета

Интернет разделяется на 5 больших сегментов:

- **Америка**
- **Европа**
- **Ближний Восток**
- **Дальний Восток**
- **СНГ**

При этом технологических поставщиков двое:

- **США**
- **Китай**



КОД БЕЗОПАСНОСТИ

Huawei стал первой жертвой политического соперничества

ПРИМЕР РЕАЛИЗАЦИИ ГЕОПОЛИТИЧЕСКОГО РИСКА

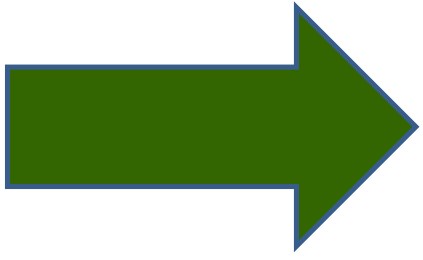
Компания была отрезана от нескольких ключевых технологических цепочек:

- Мобильная платформа Android
- Процессоры Intel, AMD, Qualcomm
- Периферия – Wifi alliance, PCIe, SD association

КОД БЕЗОПАСНОСТИ

Предпосылки создания рынка цифрового суверенитета

- Установка своих правил на своей виртуальной территории
- Технологическая зависимость хотя бы от одного «центра силы»
- Непростые отношения хотя бы с одним «центром силы»
- Решимость использовать технологические рычаги давления



Создание и поддержание цифрового суверенитета

КОД БЕЗОПАСНОСТИ

Компоненты цифрового суверенитета

1

ДОВЕРИЕ АППАРАТНЫМ КОМПОНЕНТАМ

Аппаратный контроль целостности и доверенная загрузка с помощью модулей Root of Trust (АПМДЗ)

2

ЗАЩИТА ЧАСТНОГО ОБЛАКА

Контроль активности администраторов частного облака, контроль безопасности настроек и сегментация виртуальной сети

3

ДОВЕРИЕ ОПЕРАЦИОННОЙ СИСТЕМЕ

Контроль доступа к данным, контроль целостности файлов, процессов и драйверов, а также защита от локального администратора

4

ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Защита от сетевых угроз, сегментация сети и безопасный обмен данными

КОД БЕЗОПАСНОСТИ

Трудности перевода

Продукт	Наша терминология	Терминология Gartner
Secret Net Studio	**СЗИ от НСД**	• Cloud Workload Protection Platform • Information centric Endpoint Protection
	Персональный межсетевой экран	• Zero Trust Network Access

КОД БЕЗОПАСНОСТИ

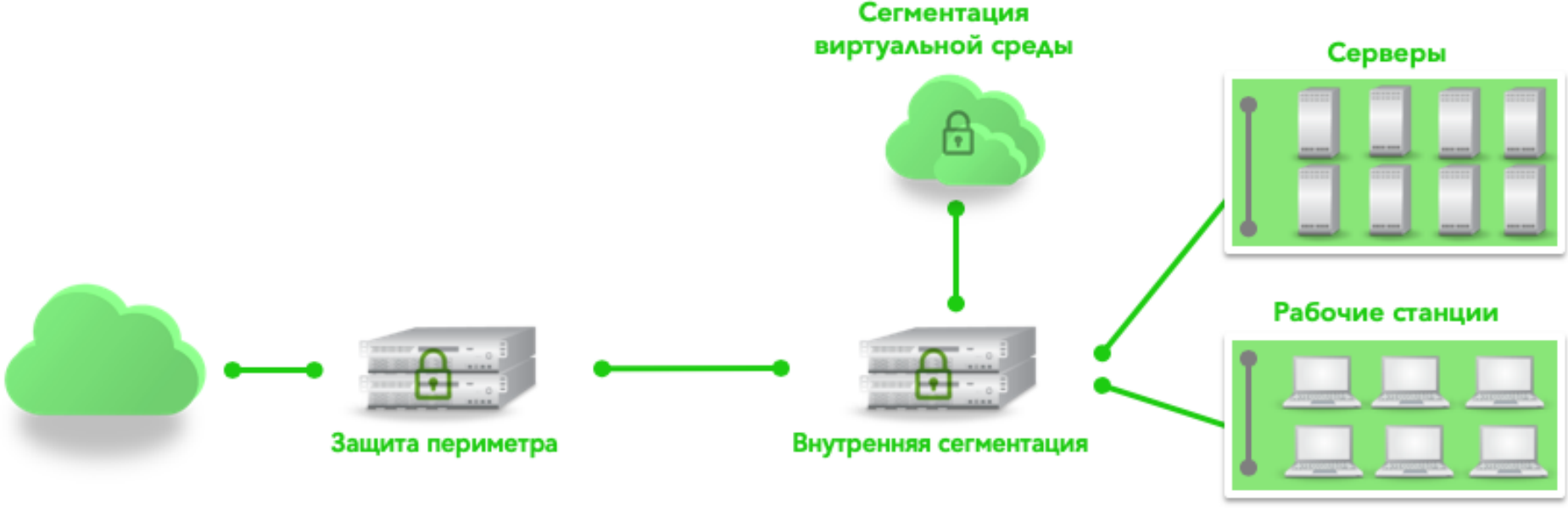
Secret Net Studio: комплексная защита данных

- Защита на основе меток конфиденциальности
- Отсутствие анализа контента для защиты конечной точки
- Опора на аппаратные механизмы защиты (Hardware Based Security)

КОД БЕЗОПАСНОСТИ

Континент 4: Комплексная защита сетевой инфраструктуры

- Концепция UTM
- Централизованное управление
- Высокая производительность
- Поддержка шифрования ГОСТ



КОД БЕЗОПАСНОСТИ

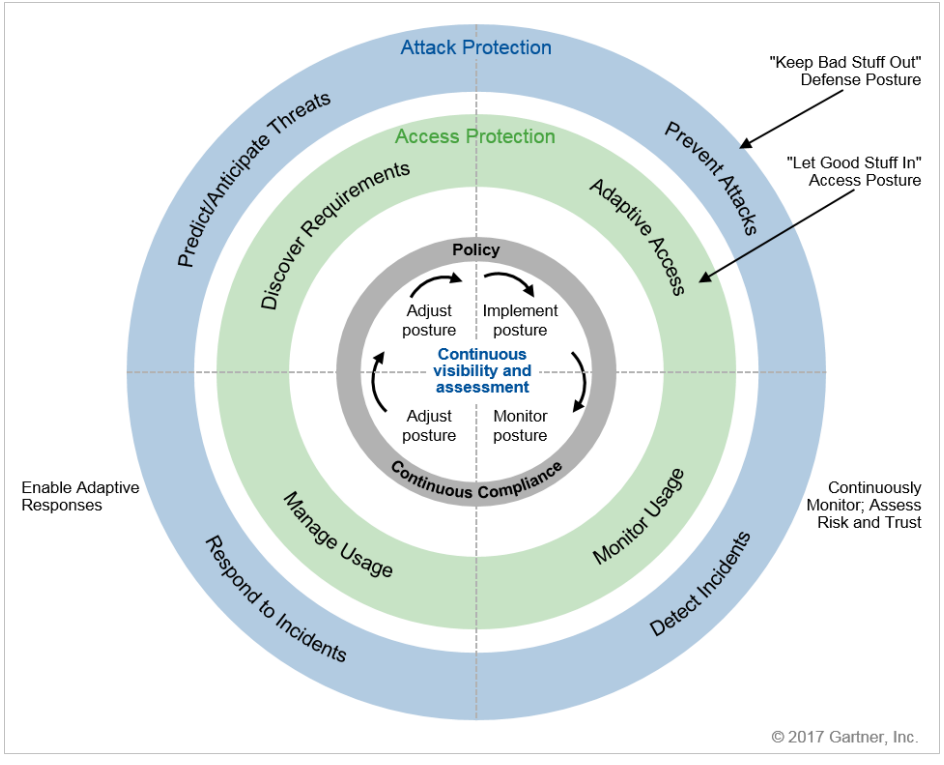
Чего ждать?

Прогноз на 2020

- Усиление геополитической напряженности
- Увеличение числа атак с использованием закладок и атак на цепочки поставок
- Широкое внедрение подхода Zero-Trust
- Внедрение аппаратной безопасности

КОД БЕЗОПАСНОСТИ

Концепция CARTA: Стратегический подход к безопасности



- Комбинация защиты от атак и защиты доступа к данным
- Защита в условиях отсутствия доверия каждому конкретному элементу ИТ-инфраструктуры
- Постоянный процесс предотвращения, мониторинга и реагирования на инциденты

КОД БЕЗОПАСНОСТИ

Перспективные технологии защиты от угроз

Hardware-based security:

- Безопасность на основе аппаратных чипов
- Хранение критичной информации в отдельном чипе
- Реализуется Intel, Google, Amazon и др.
- Снимает необходимость в собственноручной сборке компонентов ИТ-инфраструктуры

КОД БЕЗОПАСНОСТИ

Чего ждать?

Резюме

- В мире сформировалась потребность в цифровом суверенитете
- Мы сформулировали наш опыт защиты недоверенной инфраструктуры в понятные за рубежом продукты
- Мы фиксируем растущий интерес к этой теме

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Андрей Голов
Генеральный директор
a.golov@securitycode.ru