# Стратегия обеспечения безопасности в современных облачных решениях Майкрософт

Александр Липкин

Microsoft

# ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ MICROSOFT


Windows Azure
SQL Azure
bing
Windows Live® Hotmail
Windows Live® Messenger
Office 365
Microsoft® Exchange Online
Microsoft® SharePoint® Online
Microsoft® Lync Online

# Представление о гибридном облаке

# Архитектура гибридного облака

# Эшелонированная защита


Продуктивность и безопасность

Частное облако

Online

Безопасность On-Premise

Аспекты защиты виртуальных сред и ДЦОД

Безопасное взаимодействие с публичным облаком

Соответствие требованиям и стандартам

Программа безопасности облачного вендора

# Windows Server/System Center 2012-технологическая платформа для виртуализации, облачных сред и VDI

## Платформа серверной виртуализации Hyper-V 2012

Лучшая масштабируемость

Максимальная безопасность

Эксплуатационная эффективность

## Виртуальные десктопы и терминальные службы

“Золотой” образ

Эффективный транспорт - Remote Desktop Protocol 8

Максимальный комфорт для пользователя (графика, видео, периферия)

## Платформа управления System Center 2012

Контроль за частными и публичными облаками

Управление гетерогенными средами виртуализации:

- Hyper-V
- VMware
- Citrix

# Безопасность частного облака: осн. угрозы

- Периметр защиты и проблемы сегментирования сети
- Контроль трафика между виртуальными машинами
- Контроль действий администраторов и обслуживающего персонала
- Клонирование виртуальных машин, Sprawl VM увеличивают атакуемую поверхность
- Атака ВМ, находящихся в offline, изъятие виртуального жесткого диска с СХД

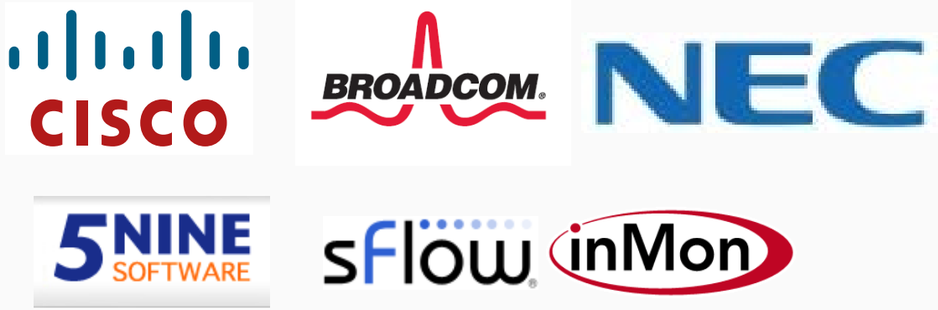
# Как Windows Server 2012 адресует угрозы ИБ:

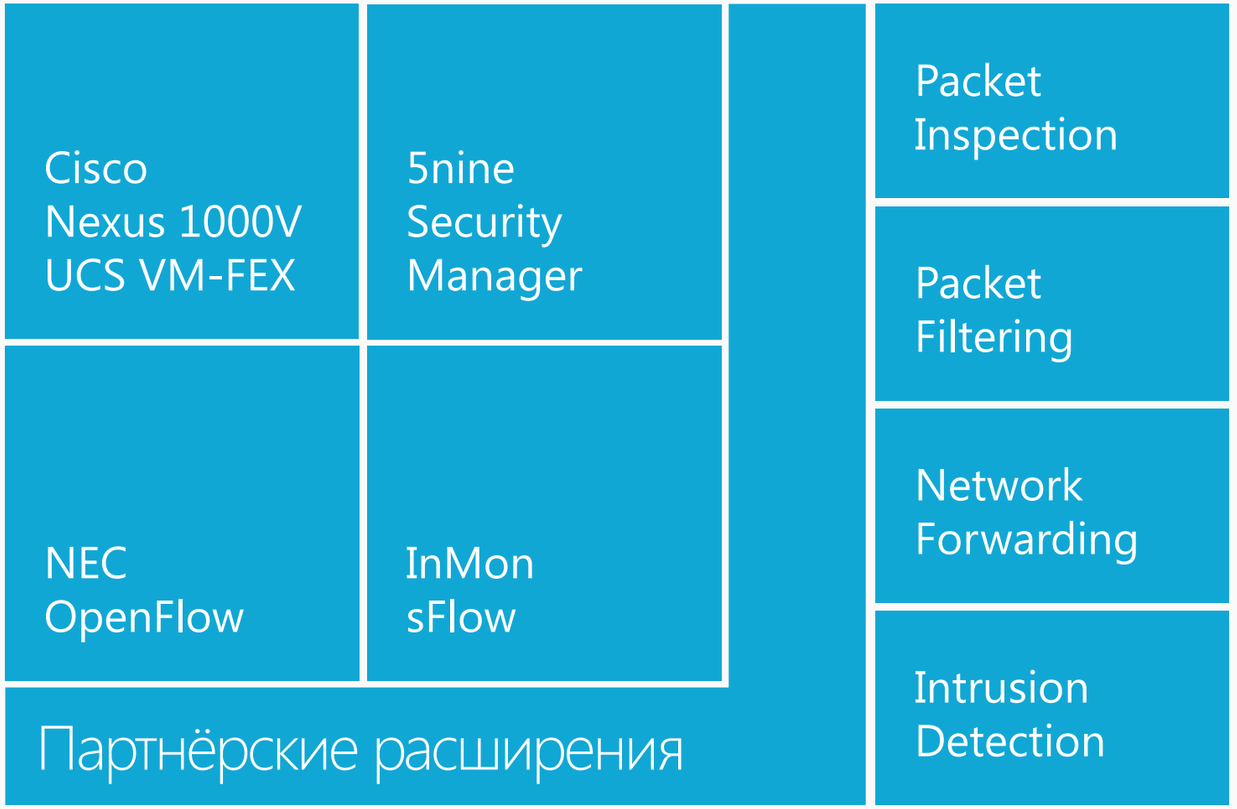
| Периметр защиты и контроль трафика | Клонирование и увеличение числа виртуальных машин | Атака виртуальных машин в offline, кража ВМ |
|---|---|---|
| Управляемый и расширяемый сетевой коммутатор (вкл. Port ACL) | Инвентаризация и контроль ВМ, квотирование ресурсов | Патч менеджмент (в том числе offline), антивирусная защита, шифрование, аудит |

Технологии Windows Server/System Center 2012 для адресации угроз ИБ в контексте виртуализации и частного облака

# Безопасное сетевое взаимодействие

## Hyper-V Extensible Switch – партнерские расширения

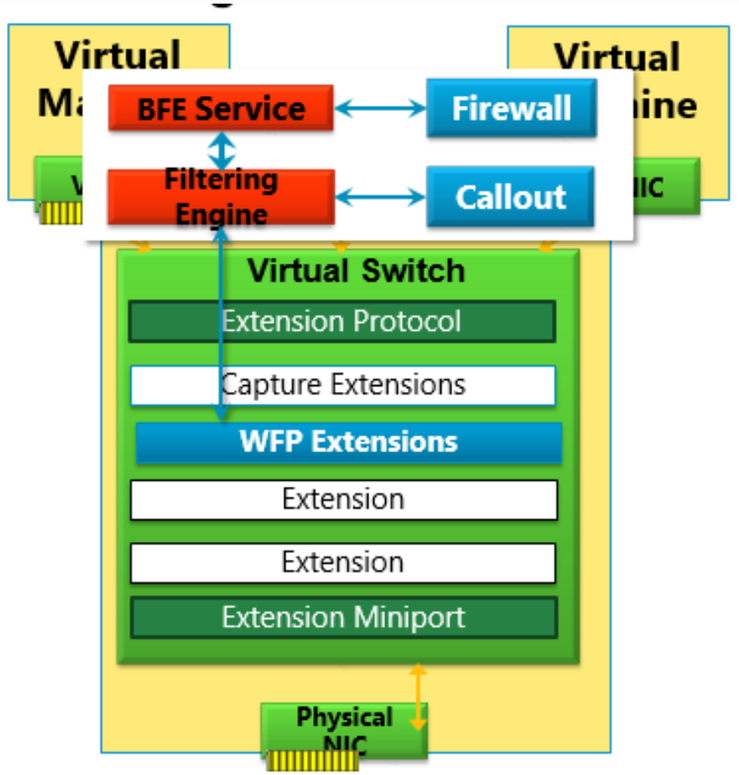


# Защита частного облака

## 5nine Security Manager for Windows Server 2012 Hyper-V

- Мониторинг и фильтрация трафика в рамках всего виртуального ЦОД в реальном режиме времени
- Антивирус и Anti-Malware без агентов в любых гостевых ОС
- Virtual Firewall в режиме Kernel mode
- Обнаружение вторжений (IDS)



# Политики аудита в Windows Server 2012

**Active Directory**

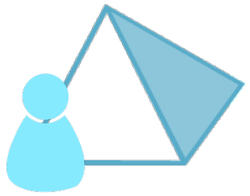
**Файловый сервер**

User claims
Clearance = High | Med | Low
Status = Fulltime | Contract

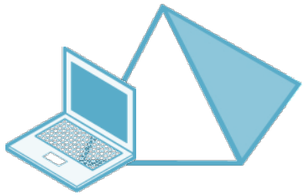
Resource properties
Department = Finance | HR
Impact = High | Med | Low

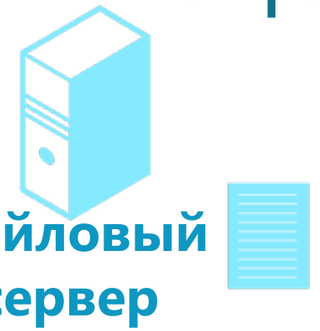
Централизованная политика аудита для бизнес-критичных данных
Audit | Read, Write | if (@Resource.Impact == High) AND (@User.Status != Fulltime)

# Dynamic Access Control – примеры и сценарии



**Active Directory**





**Файловый сервер**

**User claims**
User.Department = Finance
User.Clearance = High

**Device claims**
Device.Department = Finance
Device.Managed = True

**Resource properties**
Resource.Department = Finance
Resource.Impact = High

**Политика доступа**

Для доступа к финансовой информации, которая имеет характеристику “критично для бизнеса”, пользователь должен быть из финансового департамента с высоким уровнем доступа и использовать при этом корпоративный компьютер, закрепленный за финансовым департаментом

Александр Липкин
Майкрософт Россия
alipkin@microsoft.com

# ВОПРОСЫ?