

# HP Tippingpoint

Network Defense System – protection power beyond IPS

Jari Salokannel  
Security Solutions Architect

©2011 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice

**ENTERPRISE SECURITY**



# Leading Security Research—HP DV Labs

Security effectiveness is only as good as the security intelligence

## ZERO DAY INITIATIVE

1,600+ independent researchers

## THREAT LINQ

2,000+ customers participating

## Partners

SANS, CERT, NIST, OSVDB, etc.  
Over a dozen software & reputation vendors



## HP DV Labs R&D

Leading security research  
and filter development with  
30+ dedicated researchers

### DVLabs services:

- Digital Vaccine
- Web App DV
- Reputation DV
- Custom DV
- App DV
- ThreatLinQ
- Lighthouse Program



TippingPoint Network Defense



# HP TippingPoint has Microsoft coverage a month before other vendors

Number of days after patch that vendor delivers coverage

PATCH AVAILABLE

**-26**

**Days**

**146/163**  
Covered

**0**

**Day**

**117/163**  
Covered

**+1**

**Day**

**59/163**  
Covered

**39/163**  
Covered

**+2**

**Days**

**144/163**  
Covered

**+3**

**Days**

**131/163**  
Covered

 **TippingPoint**

Other IPS Vendors



# TippingPoint Rep DV Service

## Reputation Database

- IPv4 & IPv6 Address
- DNS Name
- Recommended settings
- Rep tags



2 hour updates



## Set Policy Based Upon

- Reputation Score
- Country/Geography
- Device Type - exploit source, malware host, Botnet CnC, spam source



Block Outbound Traffic to Prevent

- Botnet Trojan downloads
- Malware, spyware, & worm downloads
- Access to botnet CnC sites
- Access to phishing sites

Block Inbound Traffic to Prevent

- Spam and phishing emails
- DDoS attacks from botnet hosts
- Web App attacks from botnet hosts



# Facebook

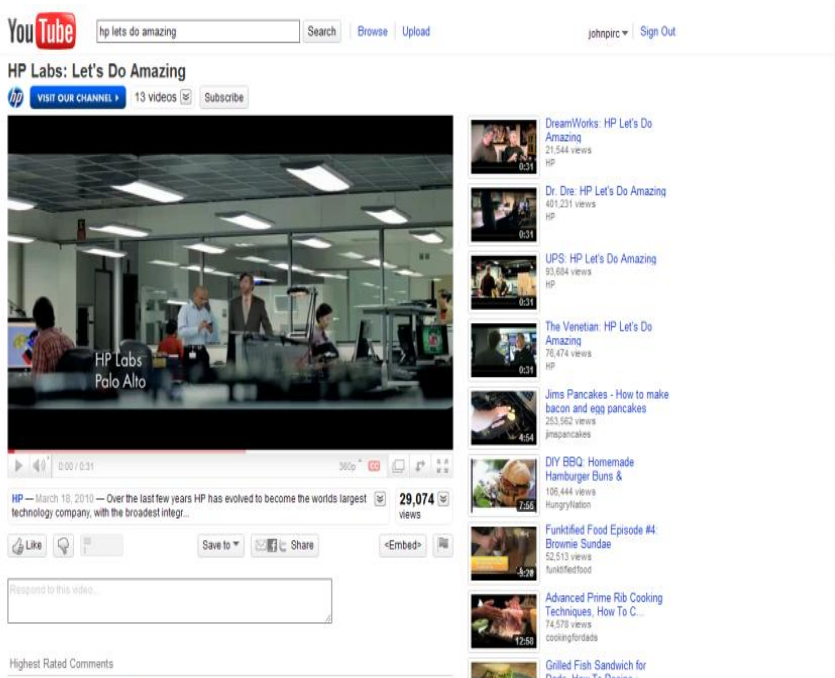


- Examples of what we can do today:
  - Facebook Access allowed with Facebook Chat denied



# Youtube

- Examples of what we can do today:
  - You Tube Access allowed with music downloads and streaming video denied



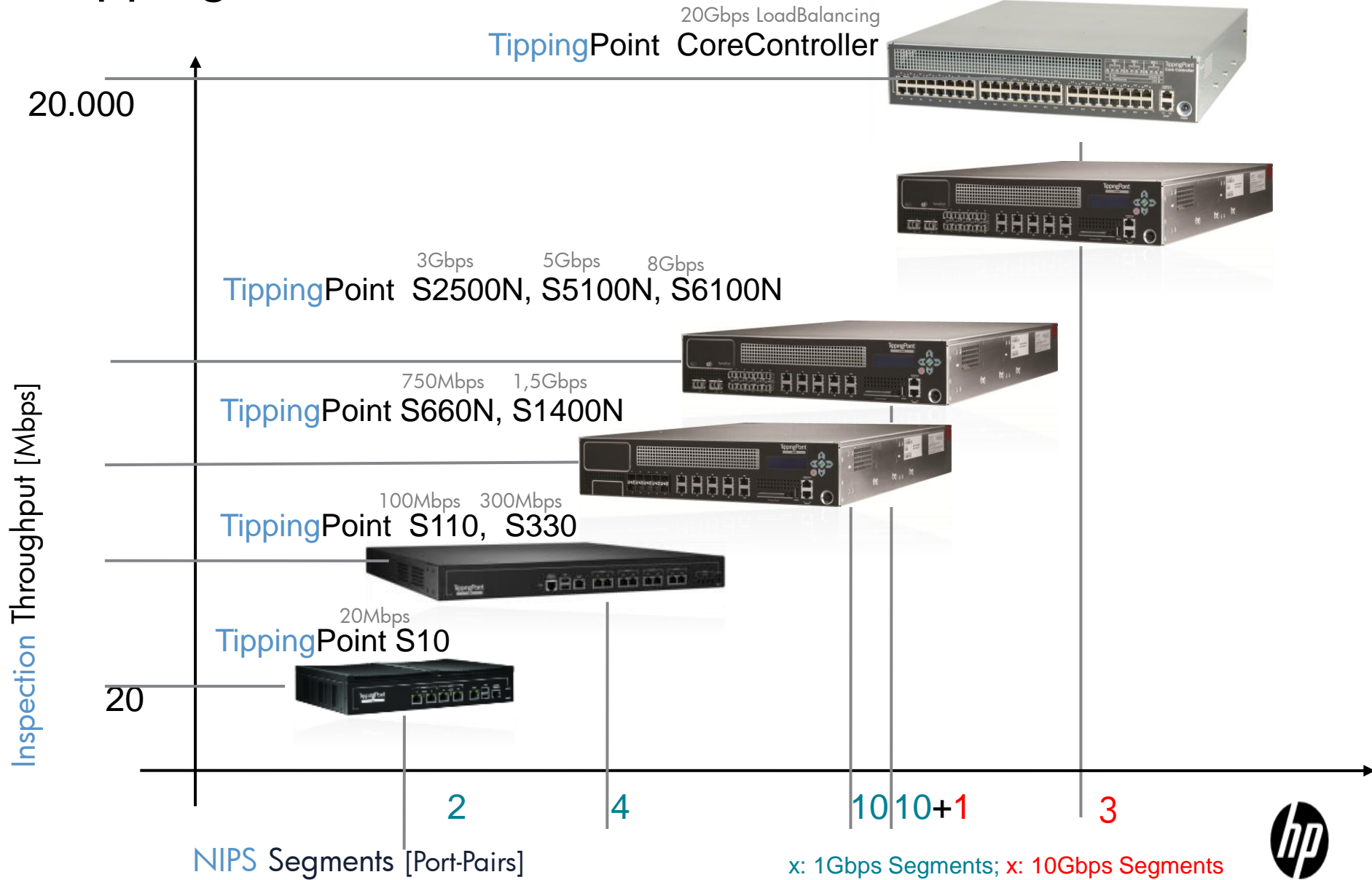
Streaming Video

File Upload

You Tube Access



# TippingPoint NIPS Portfolio

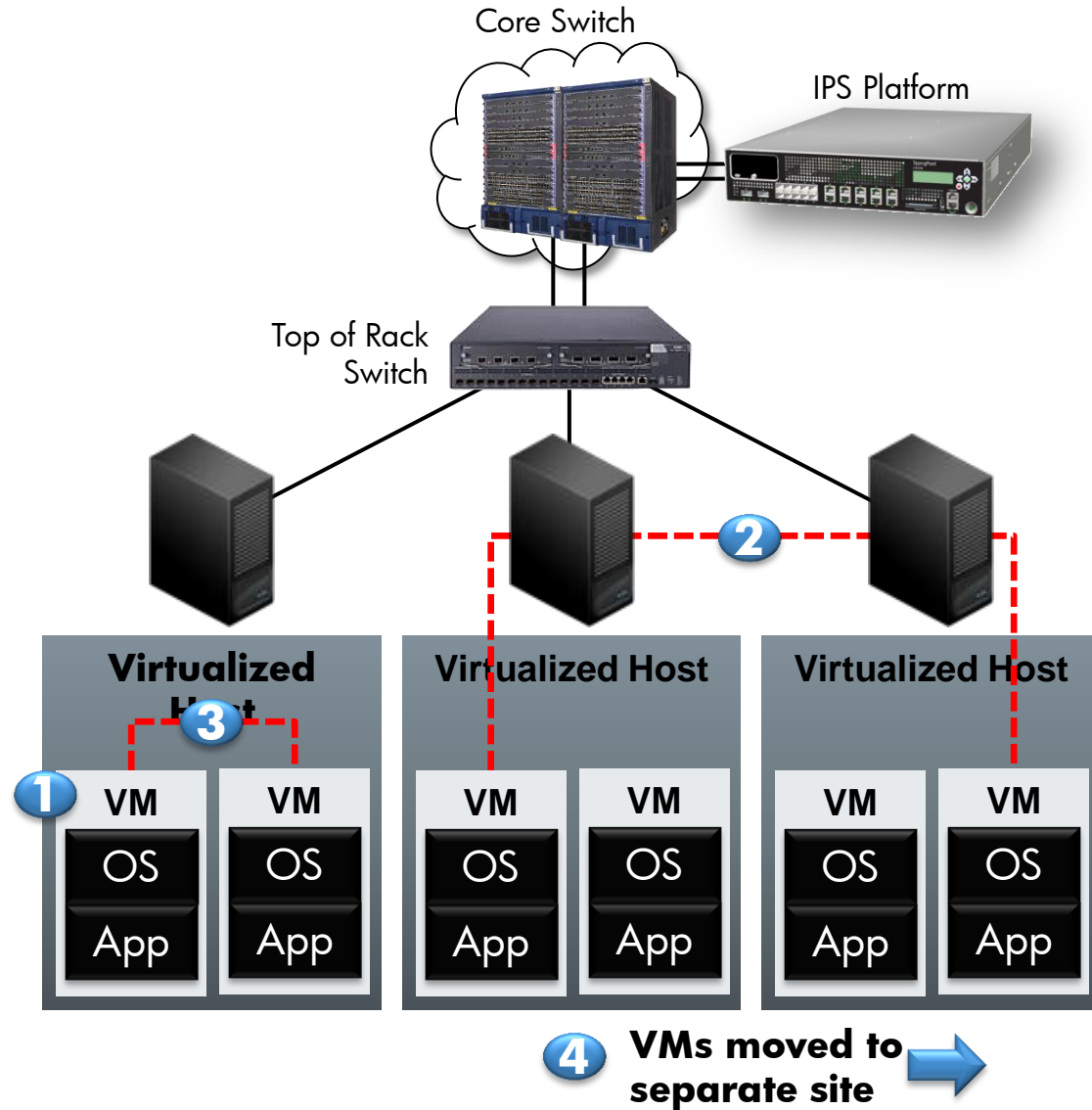


# Virtual Security Framework



# THE VIRTUAL NETWORK VISIBILITY GAP

- 1 Hypervisor Security
- 2 Host to Host Threats
- 3 VM to VM Threats
- 4 VM Mobility



# Secure Virtualization Framework (SVF)

## What's Included

- IPS Platform
- Virtual Controller + Virtual Firewall (vController+vFW)
- SMS / Virtual Management Center (vMC)

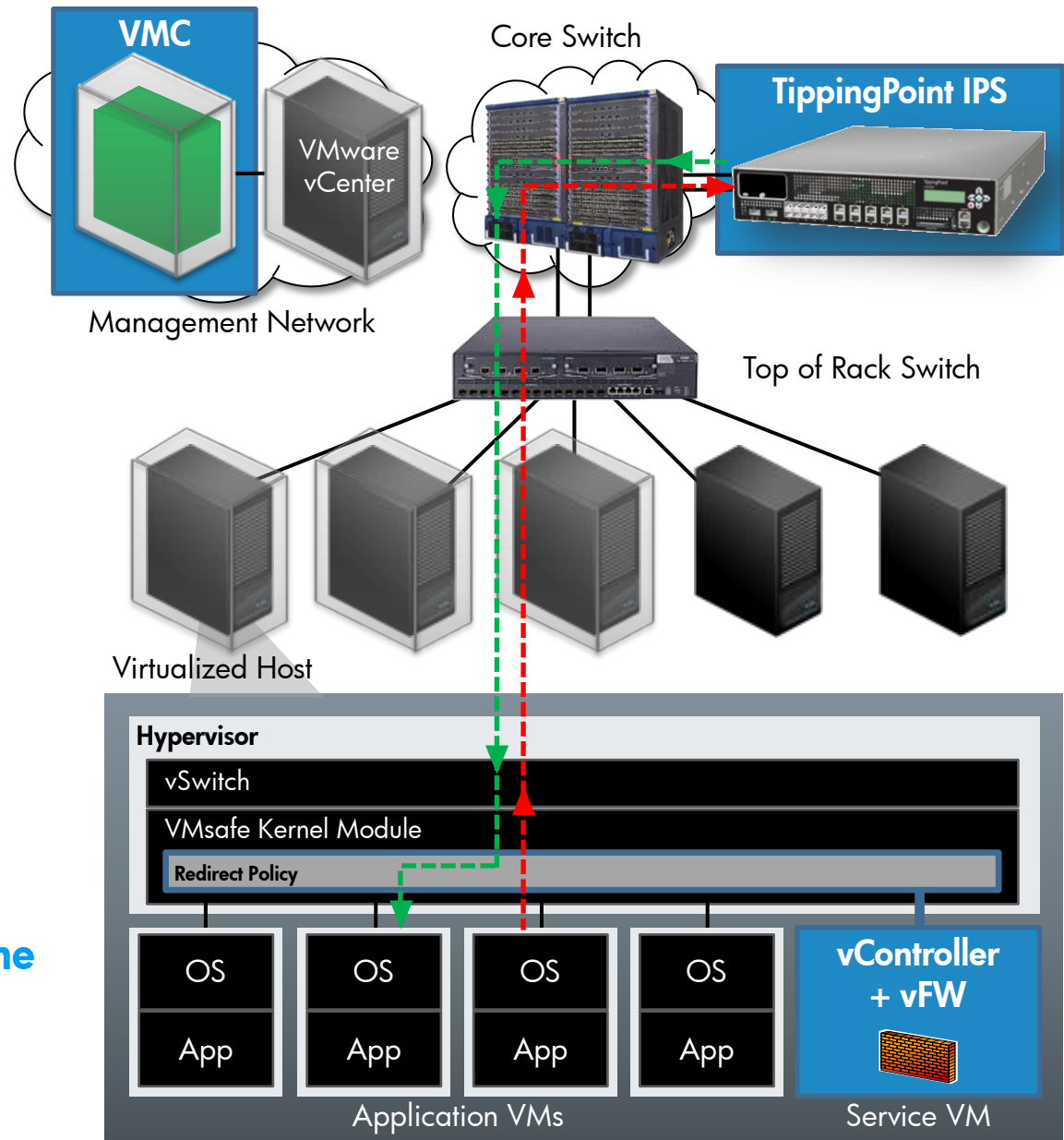
## Securing Virtualization DC security solution

- Single, purpose-built DC security solution

## Extend IPS solution into the virtual DC

- Leverage previous IPS investments

## Flexibly Inspect Data in Both the Physical & Virtual DC

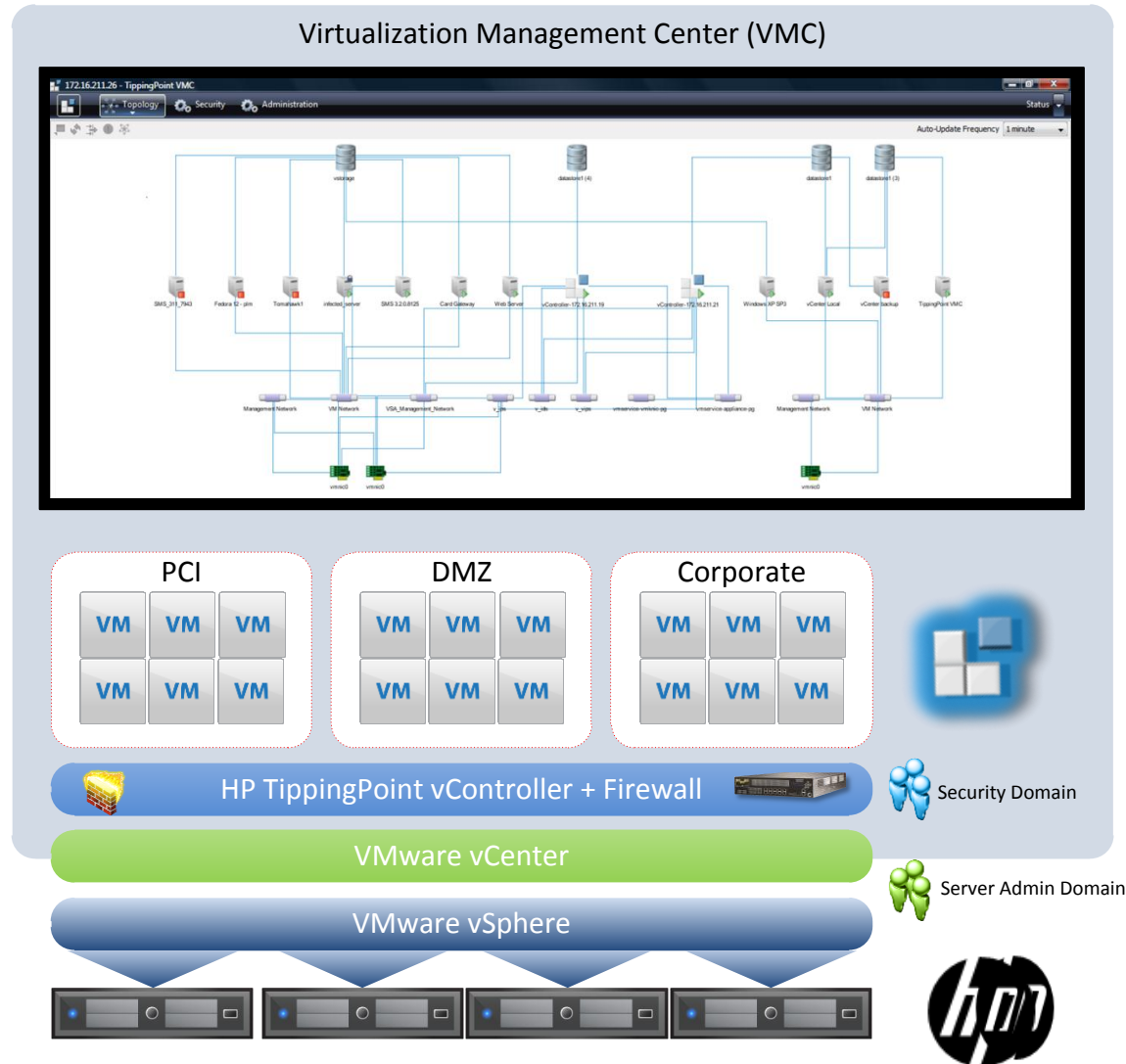


# Virtualization Management Center

visibility and control for VSphere

Maintain Separation of Duties

- vCenter integration provides security teams infrastructure visibility
- Security zones and policies maintained independent of vCenter
- Policies automatically adapt to infrastructure changes
- Enables zone and policy definition based on infrastructure attributes
- Real-time virtual network topology mapping
- Graphical policy visualization



# Summary

- Tippingpoint – More than an IPS
- Probably the best 0-day defense in the world
- Simple and economical to use



*THANK YOU*

