



Unified Threat Management, Managed Security, and the Cloud Services Model

Kurtis E. Minder CISSP
Global Account Manager - Service Provider Group
Fortinet, Inc.

Introduction

Kurtis E. Minder, Technical Sales Professional

Companies:



Roles:

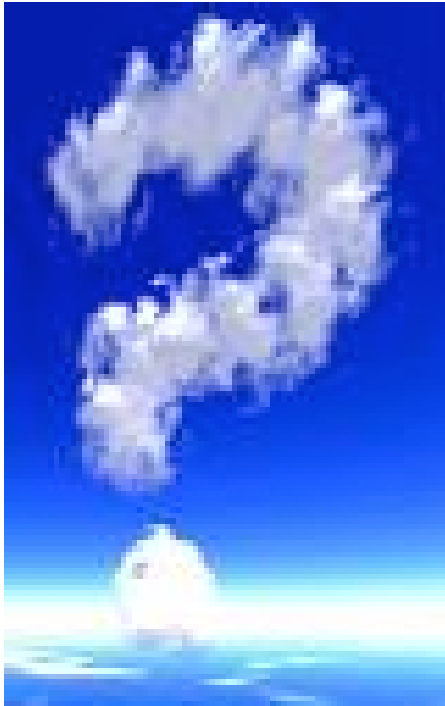
- Security Design Engineer
- Systems Engineer
- Sales Engineer
- Salesperson
- Business Development
- Global Account Manager

Actual work:

- Installation / Configuration
- Design
- Support
- Product development / POC
- Audit
- Penetration testing
- Sales / BD



Agenda



- Security Overview / Appliance Primer
- Unified Threat Management
- Managed Security Services
- Cloud Security
- Questions



Security Overview / Appliance Primer



Firewalls

The Firewall was adopted to protect corporate networks from would-be Internet attackers.

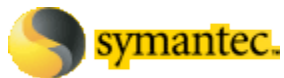
- Firewalls, deployed in-line, typically use a set of network layer rules to determine what traffic can enter/leave the network.
- Improvements to Firewall technology have been largely limited to performance. As bandwidth increased, Firewalls had to process faster. (Some FW companies have increased app visibility)
- New technologies are increasing FW capability to inspect traffic faster and more intelligently



Anti-Virus

Anti-Virus provides software / desktop level risk management for workstations in the enterprise.

- Uses malicious code signature database to determine whether workstation was being attacked/compromised.
- Enterprise solutions evolved to provide central management and enhanced capability for workstation control. (McAfee Enterprise Policy Orchestrator.)
- As larger AV vendors acquire new technologies, feature set improves (DLP, Encryption, Config Management)



VPN

VPN (Virtual Private Networking) was adopted to provide secure remote access to corporate networks.

- Provides remote access via IPSEC or SSL to the corporate network
- Enhanced features can include workstation integrity checks and role based access control
- Also is often used to provide connectivity between networks for business to business transactions.



Intrusion Detection / Prevention

IDS was developed to detect attacks on the network and alert the security administrator

- IPS, typically inline, added the capability to stop the attack automatically or manually
- IDS/IPS originally relied entirely on signatures, but evolved to include clever behavioral, heuristic-based algorithms to detect threats



Content Filtering

Content Filtering/Web Filtering emerged to increase worker productivity and reduce workplace risk.

- Monitors web surfing and other application use leaving the corporate network. Manages which websites each department can use/see.
- Leverages policy to reduce risk of malicious injection of code into the network/users browser.
- Some systems provide value added functions such as web acceleration / caching.




Data Loss Prevention

Data Loss Prevention (DLP) technology was developed as a direct result of lost corporate information from inside the network.

- DLP Technology uses a multi-faceted approach to solving the Data Leak problem, including network based sensors, workstation software, and complex policy management
- The technology is largely developed to keep corporate intellectual property and finance data from being distributed.
- Also used to maintain compliance initiatives around SOX, HIPAA; showing due diligence toward securing patient / customer data

FORTINET


VERICEPT

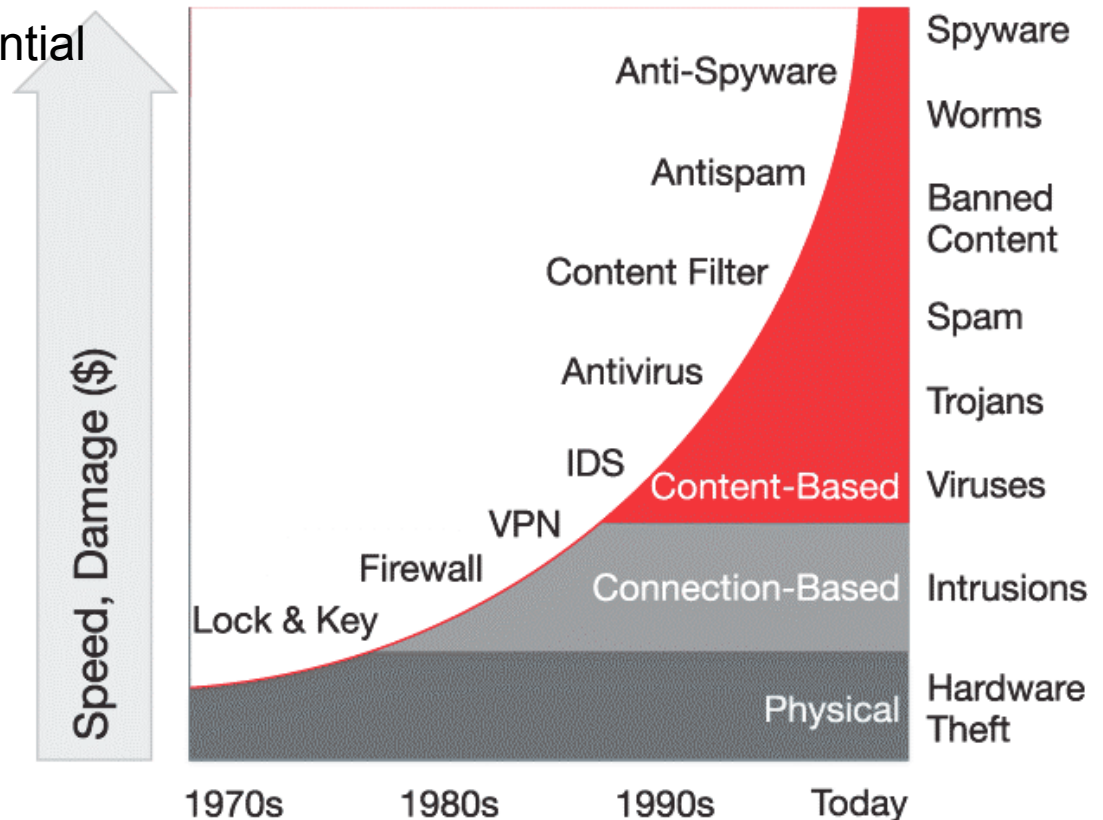
 **symantec.**

 **VONTU**

McAfee®

Threat Evolution

- Malicious code exposing confidential data has increased significantly
 - Multi and Blended attacks are now a common practice.
 - Email is the most common delivery mechanism.
- The motive and intent is changing
 - Moving from notoriety to financial gain.
 - Theft of financial and personal information.
- Traditional security isn't enough



The Traditional Approach to Network Security

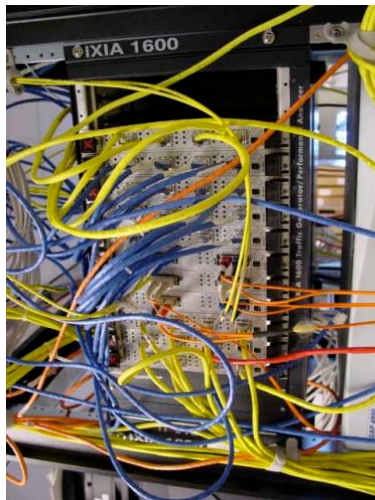
First you buy routers, firewalls, VPNs, server load balancers...



Then you buy network intrusion prevention, anti-virus, anti-malware, anti-spyware, anti-spam, anti-etc...



Then you buy proxies, web filtering, instant messaging security, data loss prevention, tomorrow's security product, and on and on.



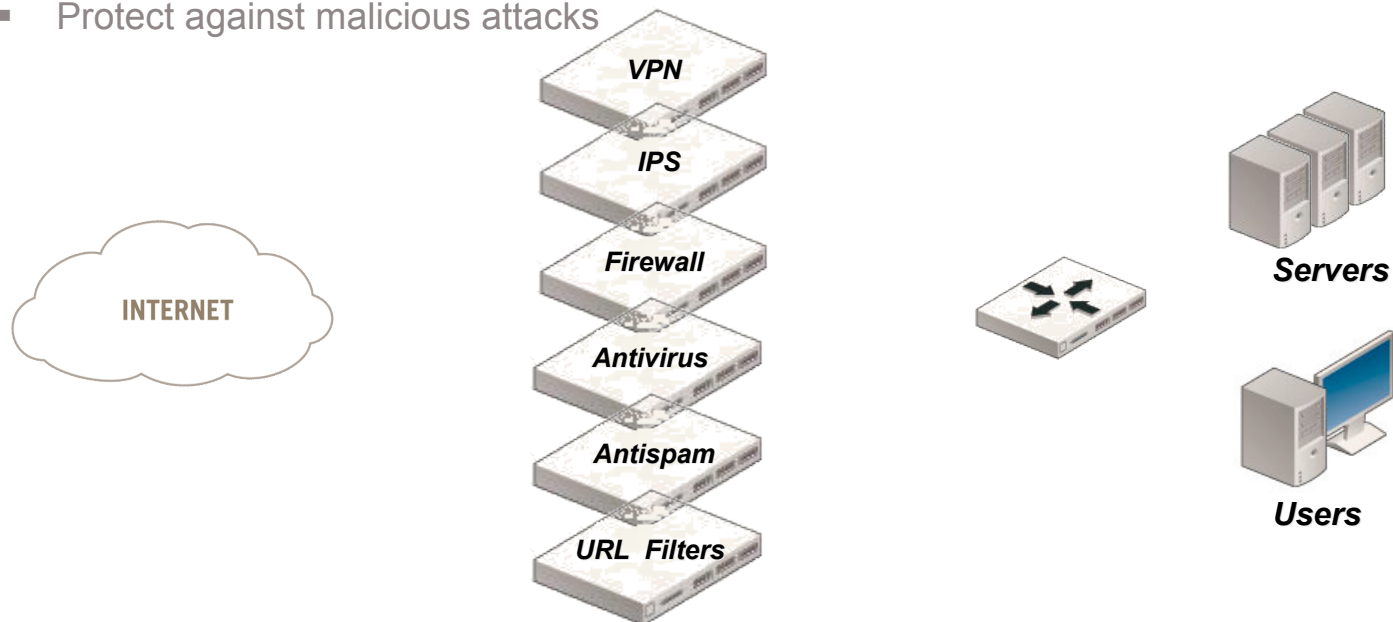
Impact

- High integration effort with multiple products and vendors
- Weak security due to lack of integration and unified configuration
- Operationally expensive to manage and operate
- **Impactical and too expensive**



A New Security Architecture Is Required

- Firewall
 - Defend against intrusions
- Antivirus
 - Protect email and web applications from virus infection
- IPS
 - Protect against malicious attacks
- Antispam
 - Reduce unwanted email
- Web filters
 - Eliminated unproductive web-browsing
- VPN
 - Delivering secure remote access



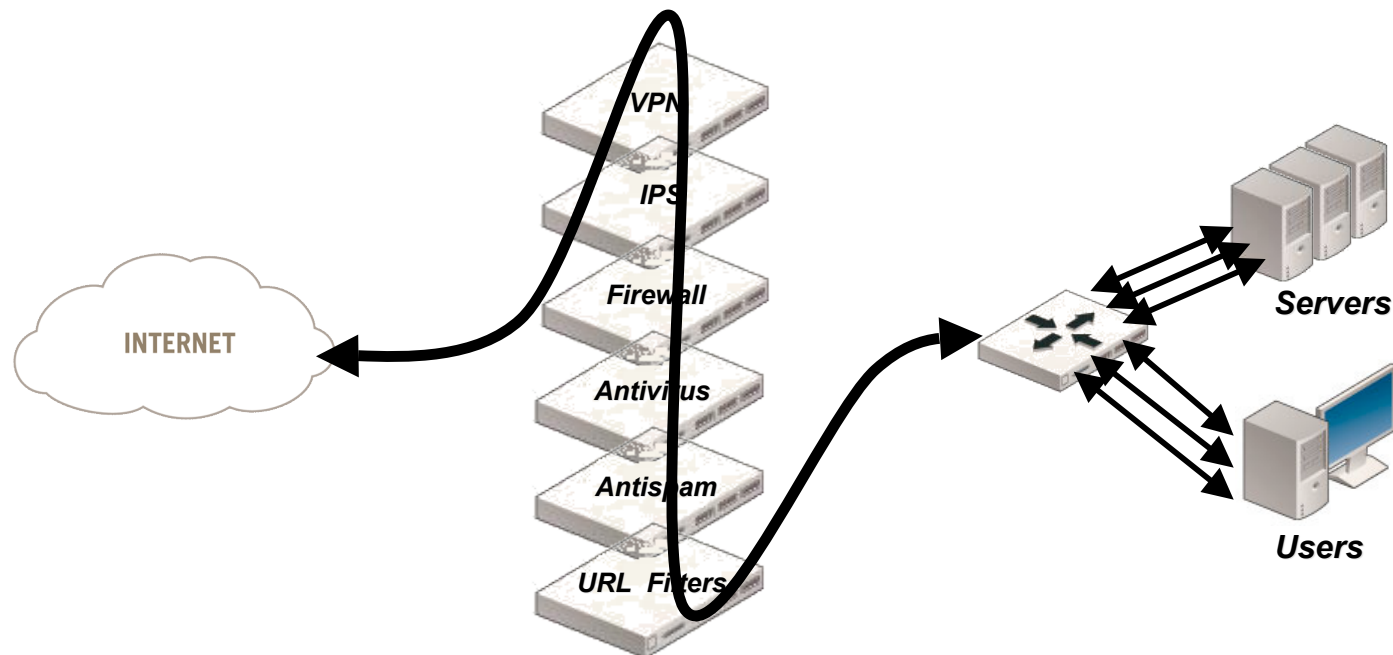
Multiple Point Solutions Add Complexity

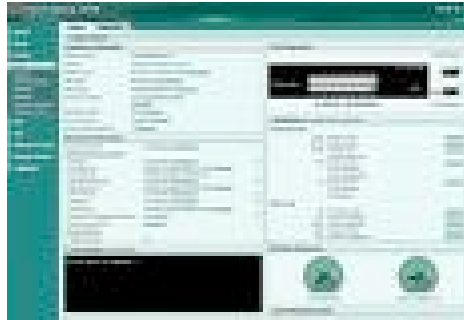
- **Perceived Advantages**

- Comprehensive security approach
- Quickly react to individual threats

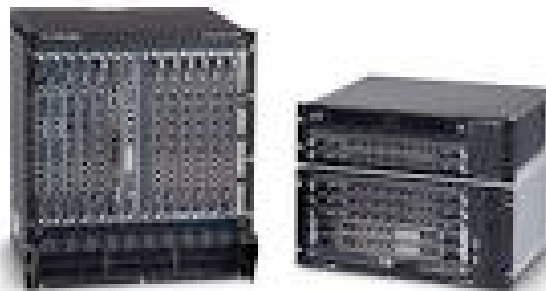
- **Real Disadvantages**

- Requires multiple products that don't talk to each other
- Increases network complexity and operational cost
- Non optimal security implementation





Unified Threat Management



Security Market Evolution

Unified Threat Management

- Firewall
- Antivirus
- IPS
- Antispam
- Content Filtering
- VPN

Firewall + VPN

- ▶ Firewall
- ▶ Virtual private network (IPSec and SSL)



Intrusion Detection & Prevention

- ▶ Intrusion detection system
- ▶ Intrusion prevention system



Secure Content Management

- ▶ Antivirus
- ▶ Antispyware
- ▶ Web filtering
- ▶ Messaging security





UTM - Best treatment for Applianceitis

- Single hardware platform
- Unified management interface
- One vendor contract / contact
- Single licensing agreement (..sometimes)
- Reduced data center footprint
- Power consumption reduction
- Minimized point of failure/latency
- *Simplified* network security architecture
 - Speeds and simplifies support and problem resolution
 - Allows for more accurate policy development
 - Quickly correlates events between components
- Blended threat protection!

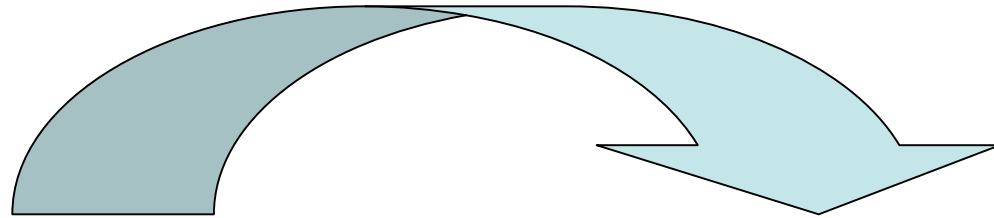
From:



To:

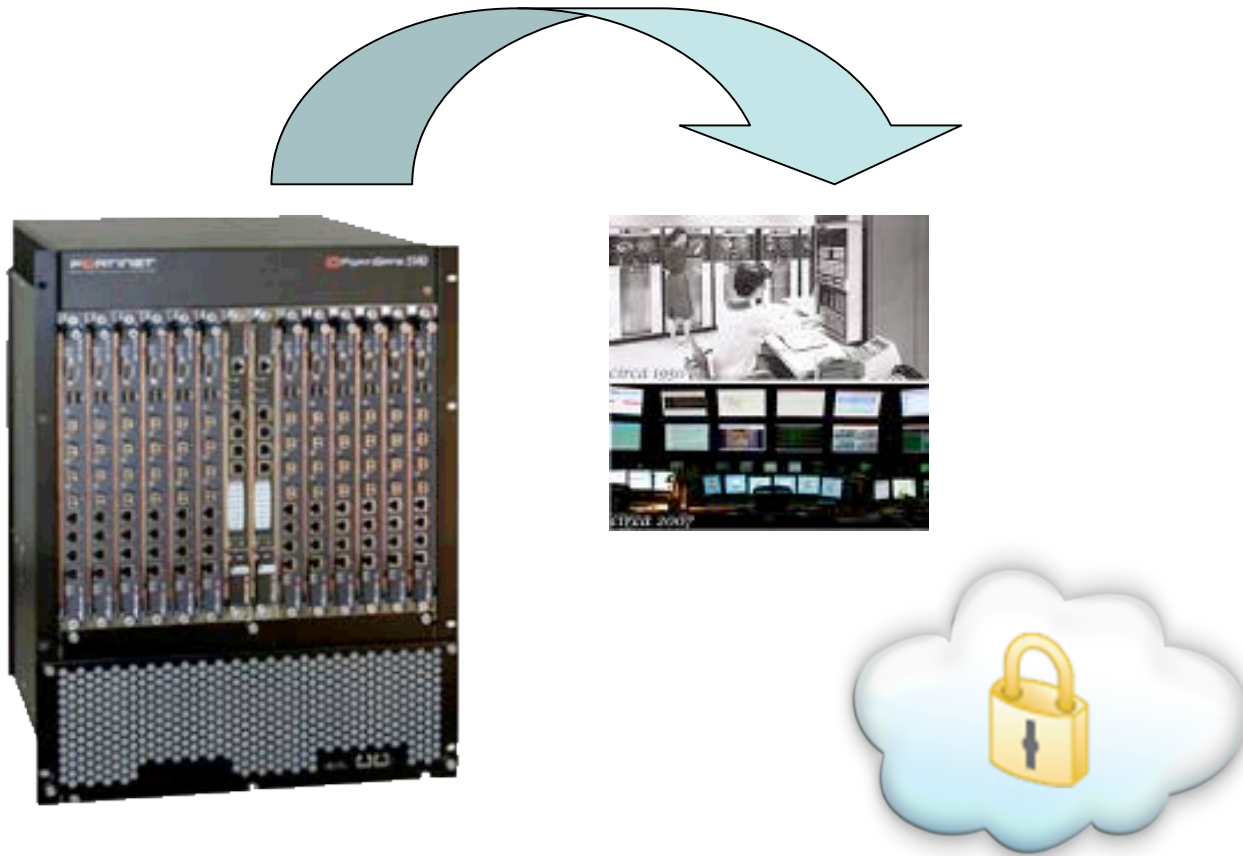


UTM Box



(Small enterprise)

UTM Box for MSS and Clouds...



The logo for SecureWorks, featuring the word "SecureWorks" in a blue, sans-serif font with a registered trademark symbol.The logo for SOLUTIONARY, featuring a stylized blue bird-like graphic above the word "SOLUTIONARY" in a blue, sans-serif font.The logo for Trustwave, featuring a stylized blue and green graphic to the left of the word "Trustwave" in a blue, sans-serif font, with the tagline "Information Security & Compliance" below it.The logo for perimeter eSecurity, featuring a green diamond icon above the word "perimeter" in a blue, sans-serif font, with "eSecurity" below it and the tagline "Complete. On Demand. Affordable." at the bottom.

Managed Security Services

The logo for at&t, featuring the AT&T globe icon to the left of the text "at&t" in a black, sans-serif font.The logo for verizon business, featuring a red checkmark icon above the text "verizon" in a black, sans-serif font, with "business" in a smaller font below it.The logo for HUGHES, featuring the word "HUGHES" in a bold, blue, sans-serif font.The logo for INTERNET SECURITY SYSTEMS, featuring a blue circular icon above the text "INTERNET SECURITY SYSTEMS" in a blue, sans-serif font, with a registered trademark symbol.

What is/are MSS?



Wikipedia defines Managed Security Services as simply...

“...network security services that have been outsourced. A company providing such a service is a Managed Security Service Provider (MSSP)”

Typical reasons for engaging an MSSP to manage your IT Security...

- Improve IT Security and Compliance
- Reduce Security Capex and Opex expenditures
- Focus on core business initiatives and competances

MSS Value Added Services

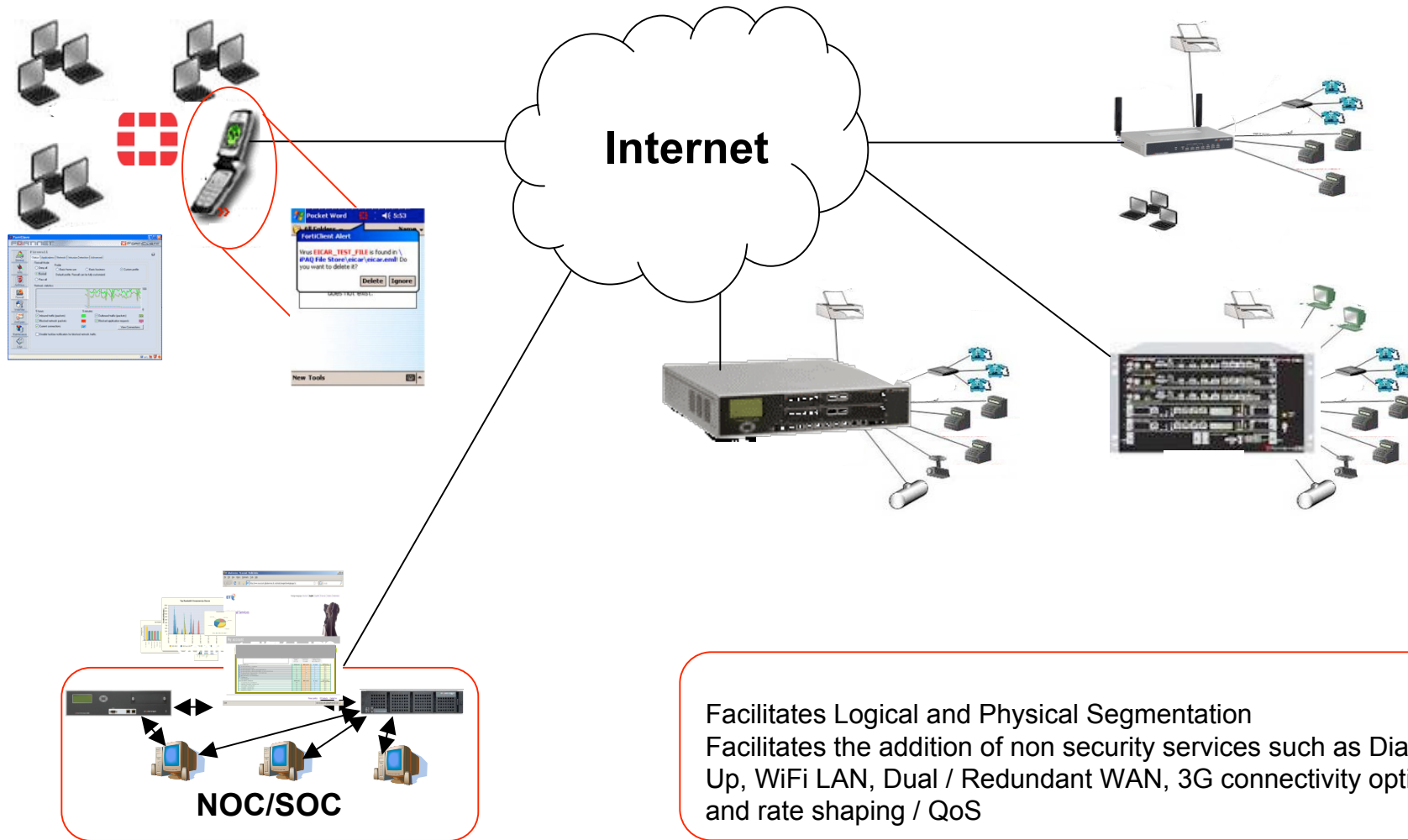
Services that MSSPs typically offer:

- Vulnerability Assessments
- Penetration Tests
- FW Management
- IDS Management
- VPN Management
- Event Mitigation Services
- Data Archival



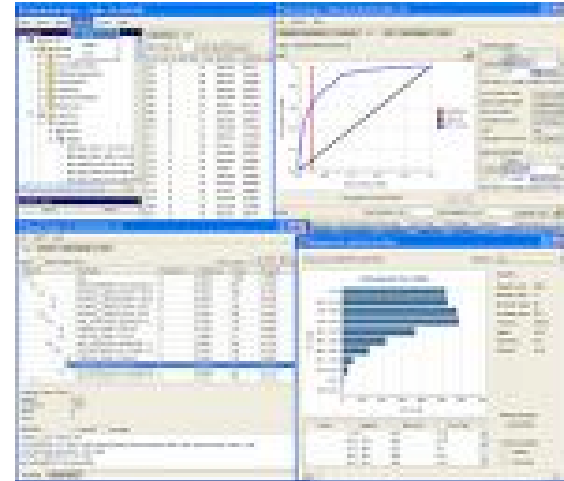
Managed UTM

Traditional MSS - Customer Premise Equipment (CPE)



MSS benefits / concerns

- Who sees my data?
- Compliance responsibilities?
- I want access to my FW/Logs!
- Will people lose their jobs?



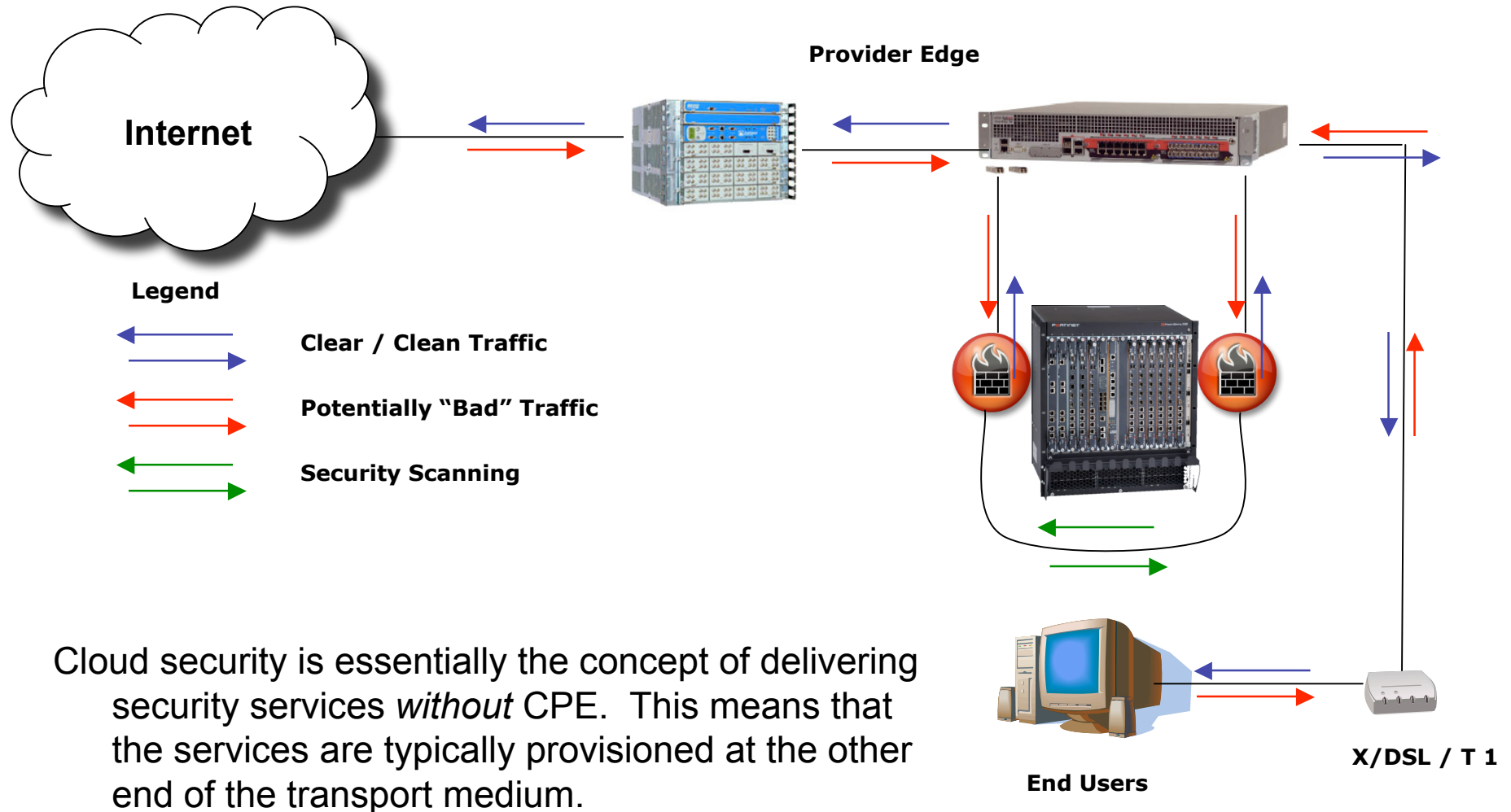
- Reduced CAPEX
- Economies of Scale around security services
- Top security analysts reviewing log material
- Enhanced correlation and automated security intelligence available
- All updates and patches done!



Cloud Security Services

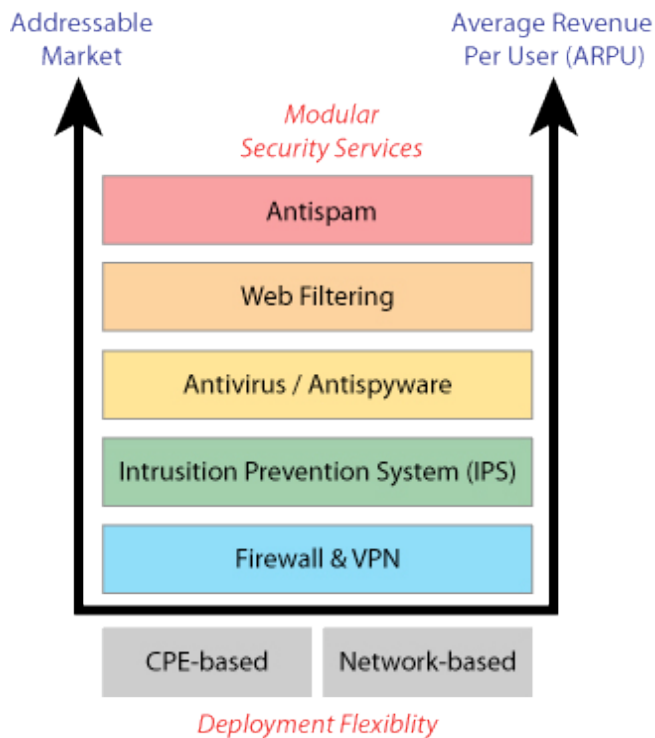


What is Cloud Security



UTM in the Cloud

Many carriers and cloud services companies are offering Managed Security in the Cloud via Unified Threat Management platforms. Why?

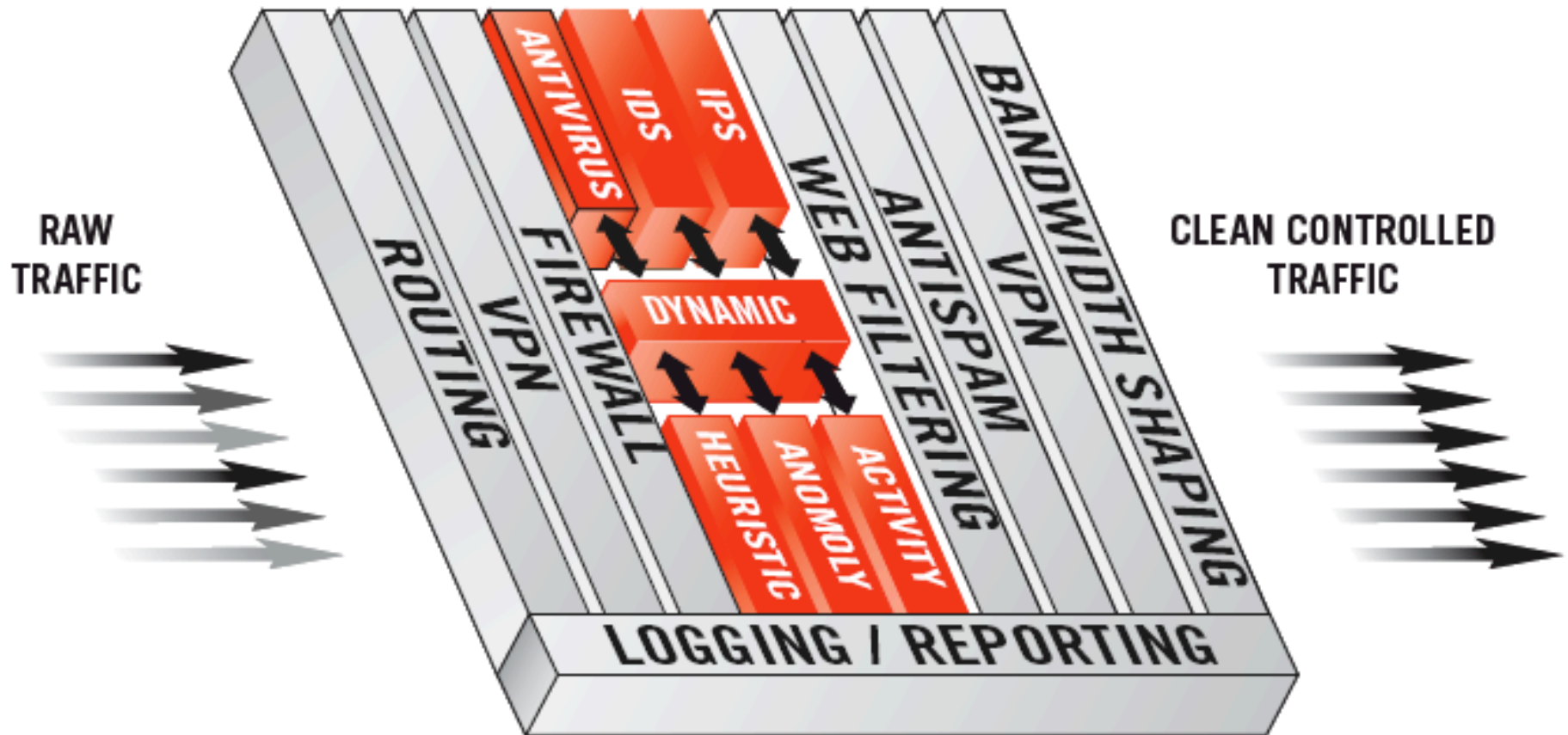


- Rapid Portfolio Creation
- Seamless Provisioning
- Increased Operational Efficiencies
- Single Vendor Contract
- Simple Licensing
- Easy correlation and alerting
- VIRTUALIZATION!

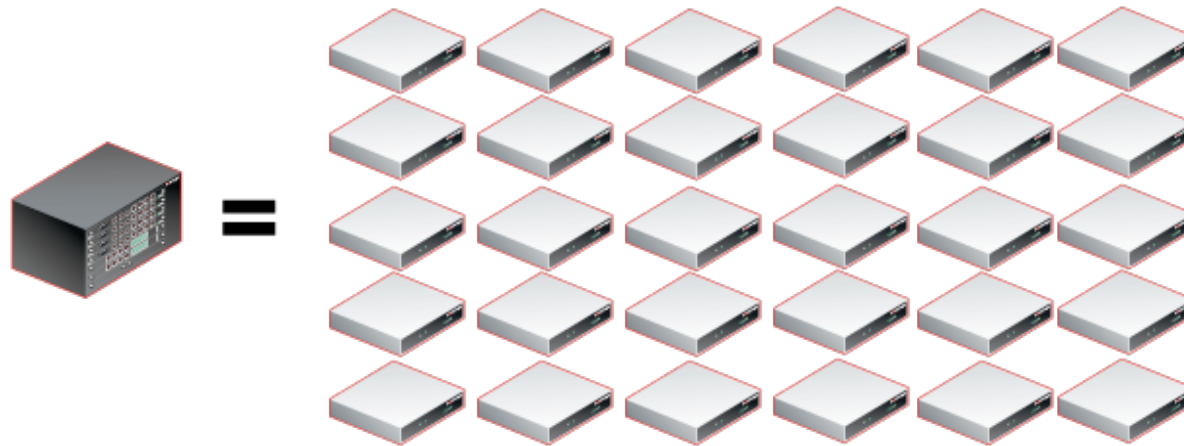
Value Added Services Delivery Model

Customer Wins!

Delivering “Clean Pipe” with UTM



Virtualization



Providing virtual UTM services from a single platform to multiple customers and applications.

Cloud Computing Security

The Amazon logo, featuring the word "amazon" in a lowercase, sans-serif font with a yellow curved arrow underneath it.The Google logo, consisting of the word "Google" in its characteristic multi-colored, rounded font.The IBM logo, featuring the letters "IBM" in a bold, blue, sans-serif font with horizontal stripes.The Sun Microsystems logo, featuring a blue square icon with white lines and the word "Sun" in a blue serif font, with "microsystems" in a smaller, blue sans-serif font below it.The Microsoft logo, featuring the word "Microsoft" in a bold, black, sans-serif font.

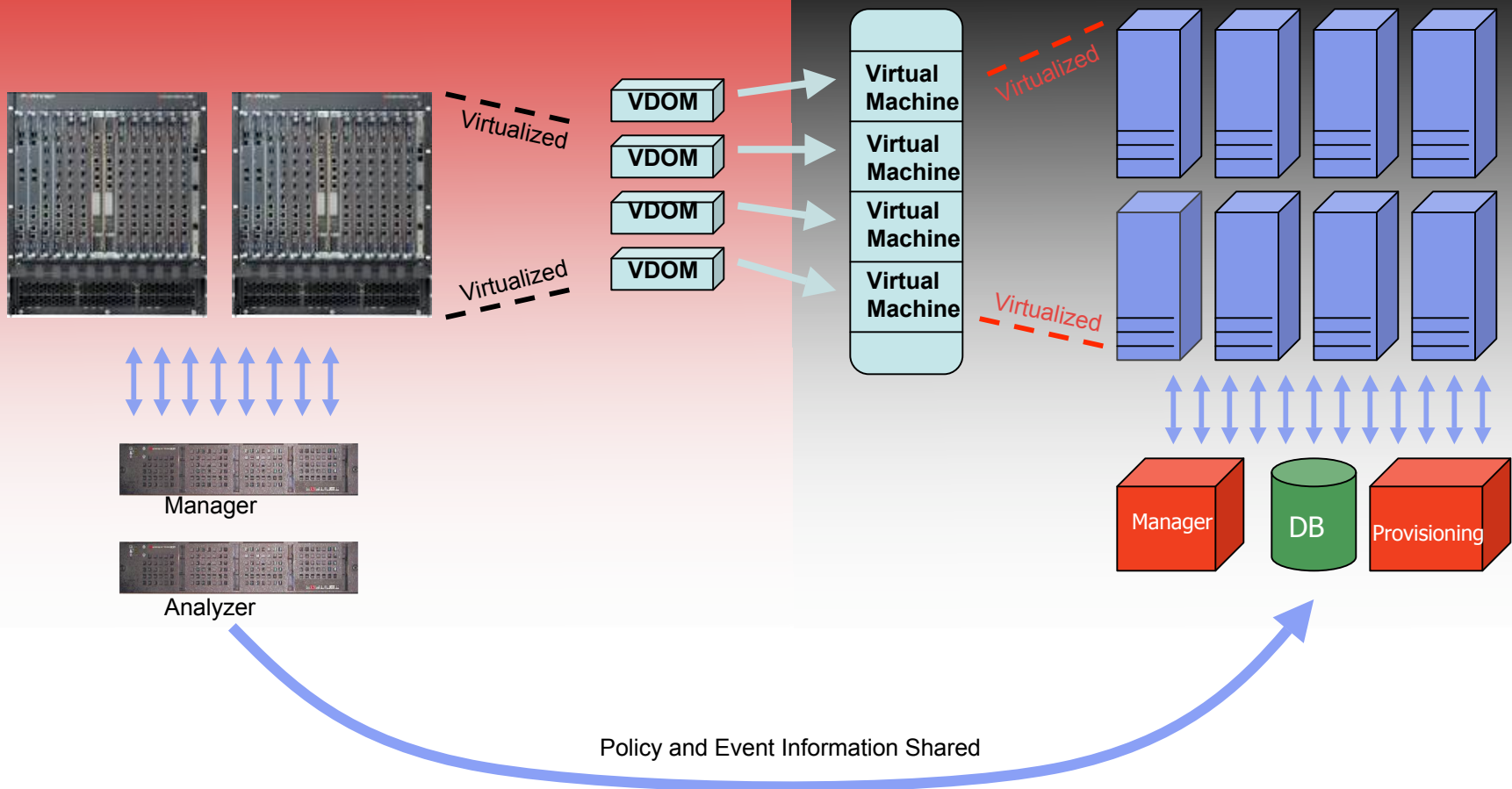
These companies want to deliver your:

- Applications
- Desktops
- Storage
- High Powered Computing (HPC) Services

...from the *internet* to your office.

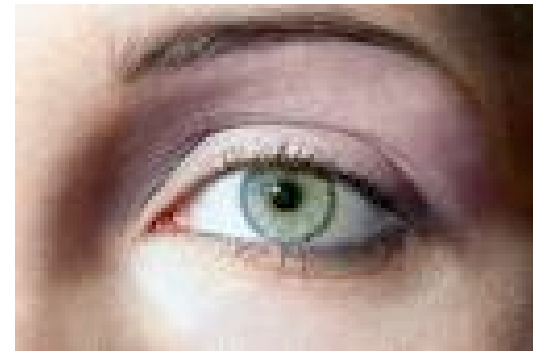
And well they should...but how do we secure it?

Cloud Computing Security Architecture Example



Cloud benefits / concerns

- Who sees my data?
- Compliance responsibilities?
- Internet reliable?



- Reduced OPEX/CAPEX
- 0 point of failure
- Disaster recovery / business continuity outsourced!
- Infinitely and instantly scalable
 - Supports “burst”
 - Scales down for economy



About Fortinet

Company Overview

- Leading provider of ASIC-accelerated **Unified Threat Management (UTM) Security Solutions**
- Company Stats
 - Founded in 2000
 - Silicon Valley based with offices worldwide
 - Seasoned executive management team
 - 1,000+ employees / 500+ engineers
 - 300,000+ FortiGate devices shipped worldwide
- Strong, validated technologies and products
 - 11 patents; 80+ pending
 - Six ICSA certifications (first and only security vendor)
 - Government Certifications (FIPS-2, Common Criteria EAL4+)
 - Virus Bulletin 100 approved (2005, 2006, 2008)



The Integrated Security Platform

Integrated Network Security Appliance

Application Aware,
Identity Based Firewall

Routing, Traffic Shaping,
Quality of Service,
Server Load Balancing

IPSec VPN &
SSL VPN Termination

Network
Application
Control & Recording

Network Anti-Virus
Anti-Malware
Anti-Spyware

Network
Intrusion
Prevention

Network
Data Loss
Prevention

Web URL & Content
Filtering

Vulnerability Management Appliance

- Auditing
- Patch Management
- Reporting and Compliance
- Smart Automation

Email Security Appliance

- Anti-spam, anti-malware
- Server, gateway & transparent
- Quarantine, user self service
- Archiving, logging & reporting

Database Security Appliance

- Database vulnerability assessment
- Security monitoring & auditing
- Monitor all access, users, methods
- Compliance reporting

Web Application Firewall Appliance


- XML router & accelerator
- XML firewall & intrusion prevention
- XML denial of service protection
- SQL injection & malware protection

Security Research & Development

- Streaming security updates for appliances
- Worldwide deployment infrastructure
- All original security research & development
- Updates for application intelligence, web filtering, intrusion prevention, anti-virus, anti-malware, anti-spyware, vulnerability assessment & database security

Worldwide Update Service





Q&A



Thank You.

Kurtis E. Minder CISSP

Kminder@fortinet.com - kurtis@kurtisminder.com

847-563-4272 - kurtisminder (skype)

<http://www.fortinet.com>

<http://www.linkedin.com/in/kurtisminder>

<http://www.kurtisminder.com>
