

## **BYOD Ate My Network, but My Next Generation Firewall Saved It**

**Eric Crutchlow**

Senior Product Manager

*Dell SonicWALL*

# BYOD Ate My Network



But My Next Generation Firewall Saved It!

**Eric Crutchlow**

**Senior Product Manager, Network Security**

# BYOD: Bring Your Own Device



# BYOD Issues

- Security
- Security
- Security
- BYOD's effect on network performance
  - Devices increasingly geared toward media consumption (bandwidth hogs)
  - Social media and collaboration increase traffic
  - Users are holding IT accountable for the same QoS and QoE for BYOD as company supplied devices.



# A Balancing Act



# Security Challenges



As soon as devices  
are on  
the network,  
damage  
can be done!

# Smartphones and Tablets Issues

- iOS apps are “White-listed” before being available for download
- Apps for Android ... depends
- What about “jailbroken” or “rooted” devices?



# No Wires Attached

- Regardless of backbone bandwidth, wireless access point capacity is limited
- Convenience and connection speed are expected
- iPhones automatically set to poll APs and acquire IP addresses...even when they're not in use





Bring Your Own Device to Work is Happening

Need to Deal With It . . .

But Securely!!!



# BYOD and Your Business

## APPLICATIONS

ORACLE®

Microsoft®

SAP®



## COMMUNICATIONS



skype®



## DEVICES



Homogeneous

Heterogeneous



# Why Personal Devices Could Be Risky?

- **Personal Devices Can ...**
  - Download/Store/Forward Sensitive Information
  - Have Access to Corporate Networks, Systems, and Data
- **Areas of Risk:**
  - Data Loss
    - Lost Mobile Device
  - Loss of Control Introduction of Malware
    - JailBroken / Routed Phones
  - Data Leakage
    - Unauthorized Data Access & Download
  - Unauthorized Network Access
    - Compromised Device is a Backdoor to Your Network



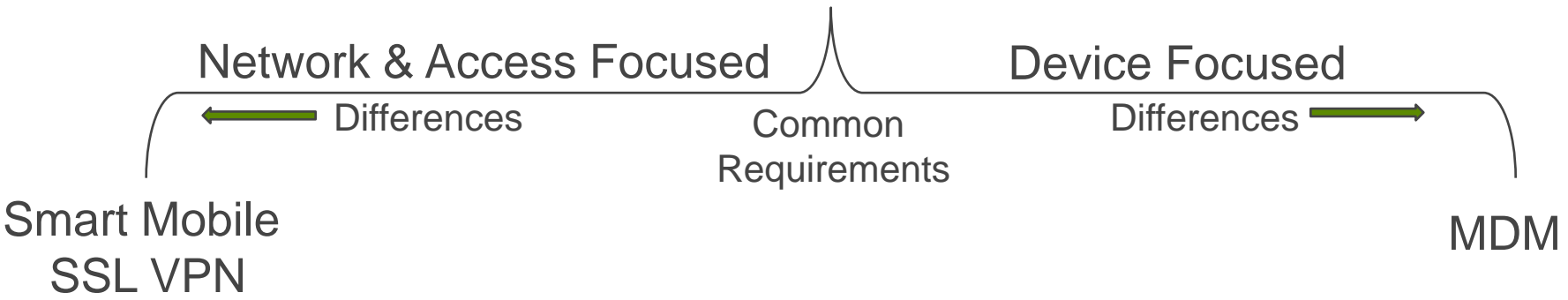


**MDM**

# The Mobile Market in 2012+

B.Y.O.D. is driving the market  
The need is mobile ACCESS  
The assumed answer is often **MDM**

For most of the market, the better answer is  
**Smart Mobile SSL VPN**



# The Real Mobile Market in 2012+

## B.Y.O.D.

Network & Access Focused

Device Focused

Differences

Differences

### Common Requirements

*Remote Access*

*Protect Company Data*

*Manage Mobile users as "Groups"*

*Password Enforcement (policies)*

MDM

Smart Mobile  
SSL VPN

### Drivers

- Leverage existing infrastructure
- JailBreak & Identity protection and policy
- Security
  - Anti-virus, intrusion prevention, anti-spyware
- Data Leakage Prevention
- Application control
- Leverage existing policy engines based on device status
- Global remote device wipe

### Drivers:

- Deployment of independent MDM infrastructure
- Over air software distribution
- IT control of settings, on device policies
- Asset inventory tracking
- App black list reporting
- Remote wipe of specific applications
- Granular IT control over personal versus work data
- Personal work space & protected workspace
- Redundant infrastructure for protected workspace (separate email server, etc.)



# But how to provide Secure Connectivity?



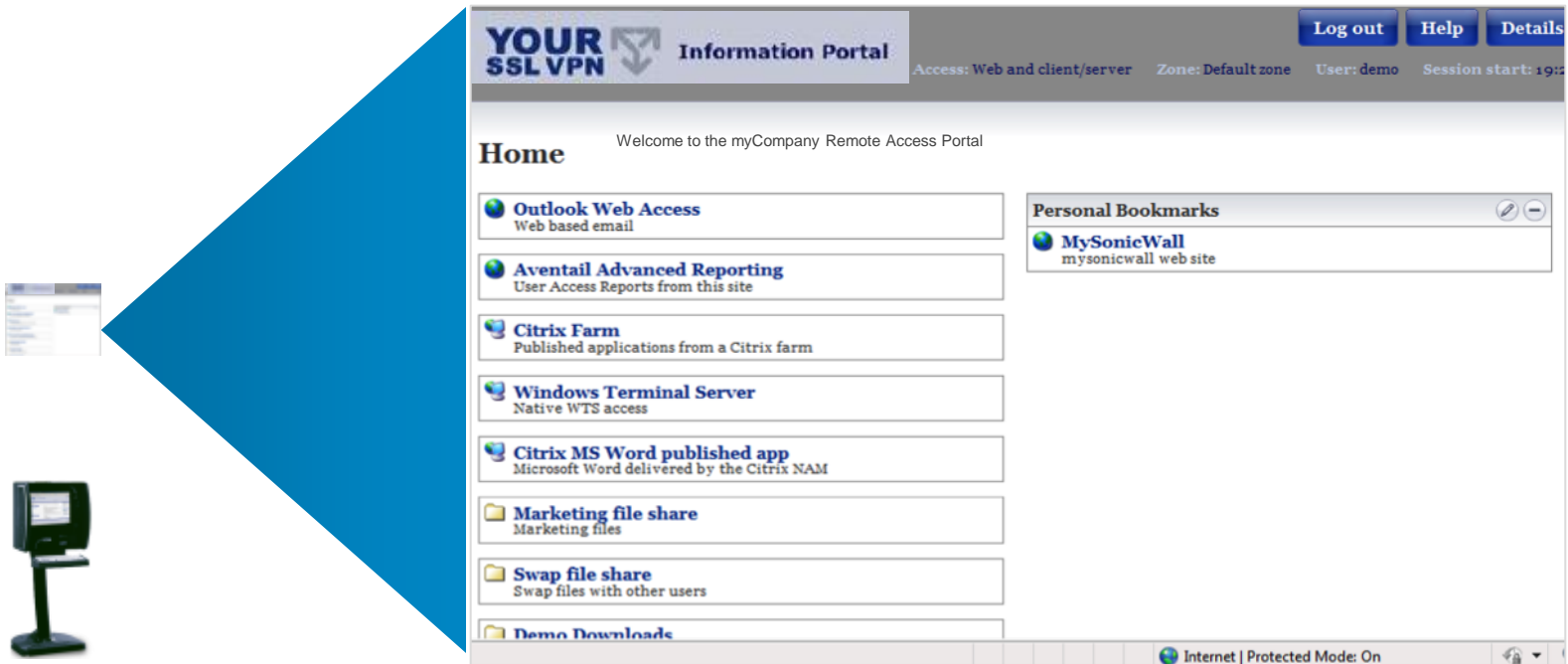
# Approaches to managing the access problem

- Treat every device as untrusted
- Use SSL VPN for strong authentication and encryption
- Utilizing NGFW to identify traffic and applications
- Ensure every packet of information is scanned without slowing down the network
- Allocating bandwidth based on users and groups
- Look at all end points to ensure that they aren't being used as hosts for outbound attacks





# Use a Reverse Web Proxy



**YOUR SSL VPN** Information Portal

Access: Web and client/server Zone: Default zone User: demo Session start: 19:2

**Home** Welcome to the myCompany Remote Access Portal

- Outlook Web Access**  
Web based email
- Aventail Advanced Reporting**  
User Access Reports from this site
- Citrix Farm**  
Published applications from a Citrix farm
- Windows Terminal Server**  
Native WTS access
- Citrix MS Word published app**  
Microsoft Word delivered by the Citrix NAM
- Marketing file share**  
Marketing files
- Swap file share**  
Swap files with other users
- Demo Downloads**

**Personal Bookmarks**

- MySonicWall**  
mysonicwall web site

Internet | Protected Mode: On

**WorkPlace Access:** Access to Web-based and client/server applications from virtually any device.



# Establish an SSL VPN Tunnel



iOS Devices

Android Devices



# Employ Strong Authentication



# Deploy Endpoint Control (EPC)

## EPC Device Interrogation

### Interrogate by Device Profile

IT Managed	Windows
Non-Managed	Macintosh
	Linux
	Android
	iOS

### For Device Identity

- Mapped Directory
- Windows Domain Membership
- Device Watermark/Certificate
- Any Resident File
- Device ID

### And Device Integrity

- Anti-Virus
- Registry Key
- Windows O/S Level
- Personal Firewall
- Anti-Spyware
- Jailbreak or Root Detection

### WorkPlace Access (Clientless Web Access)



### Connect Access (Client-Installed Access)



SonicWALL



End Point  
Control

### Corporate Network



VoIP  
Applications



File  
Shares



Traditional  
Client/Server  
Applications



# Enterprise Remote Access

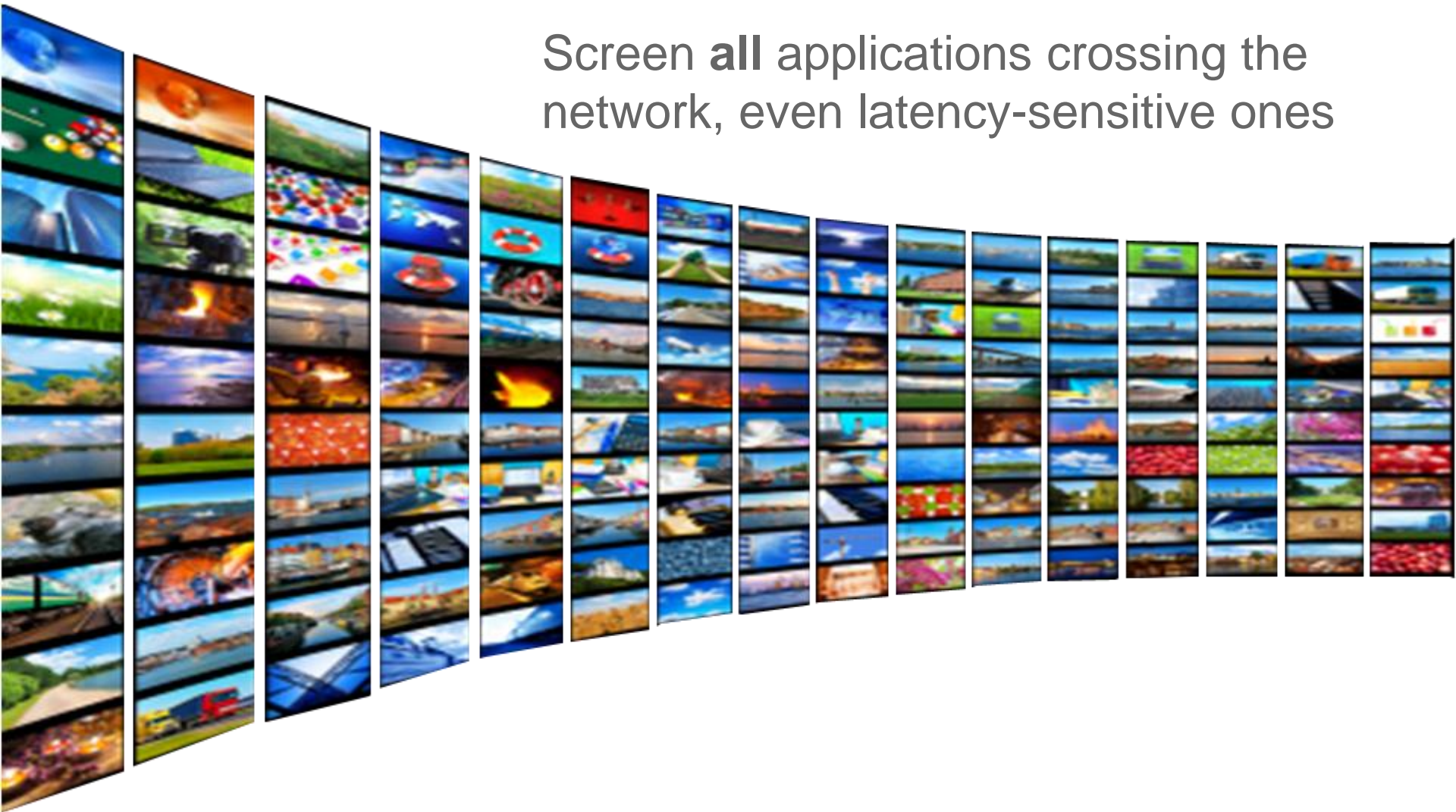
## Mobile Connect for iOS & Android

- True *native network level security client*
  - *1 of only 4 companies in world*
- Differentiation:
  - **Policy**
    - In-depth policy control by on device status: EPC *jailbreak detection controls, certificate, UUID, and others*
  - **Security**
    - **Gateway anti-virus, intrusion prevention and anti-spyware** on SSL connection
  - **Control**
    - *Application control* on mobile SSL connections

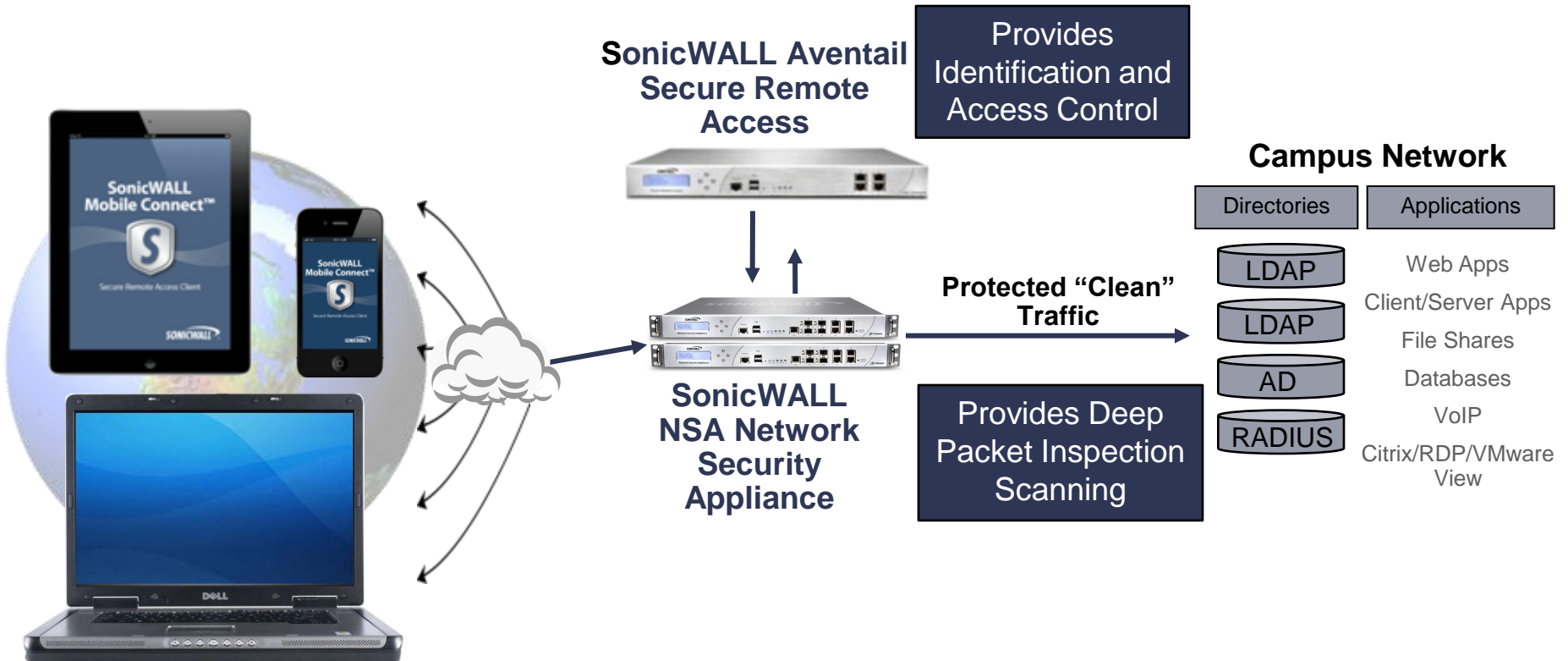


# The Challenge

Screen **all** applications crossing the network, even latency-sensitive ones



# Scan All Traffic through a Next-Generation Firewall



# Next-Generation Firewalls

## Application Intelligence, Control and Visualization

### Identify

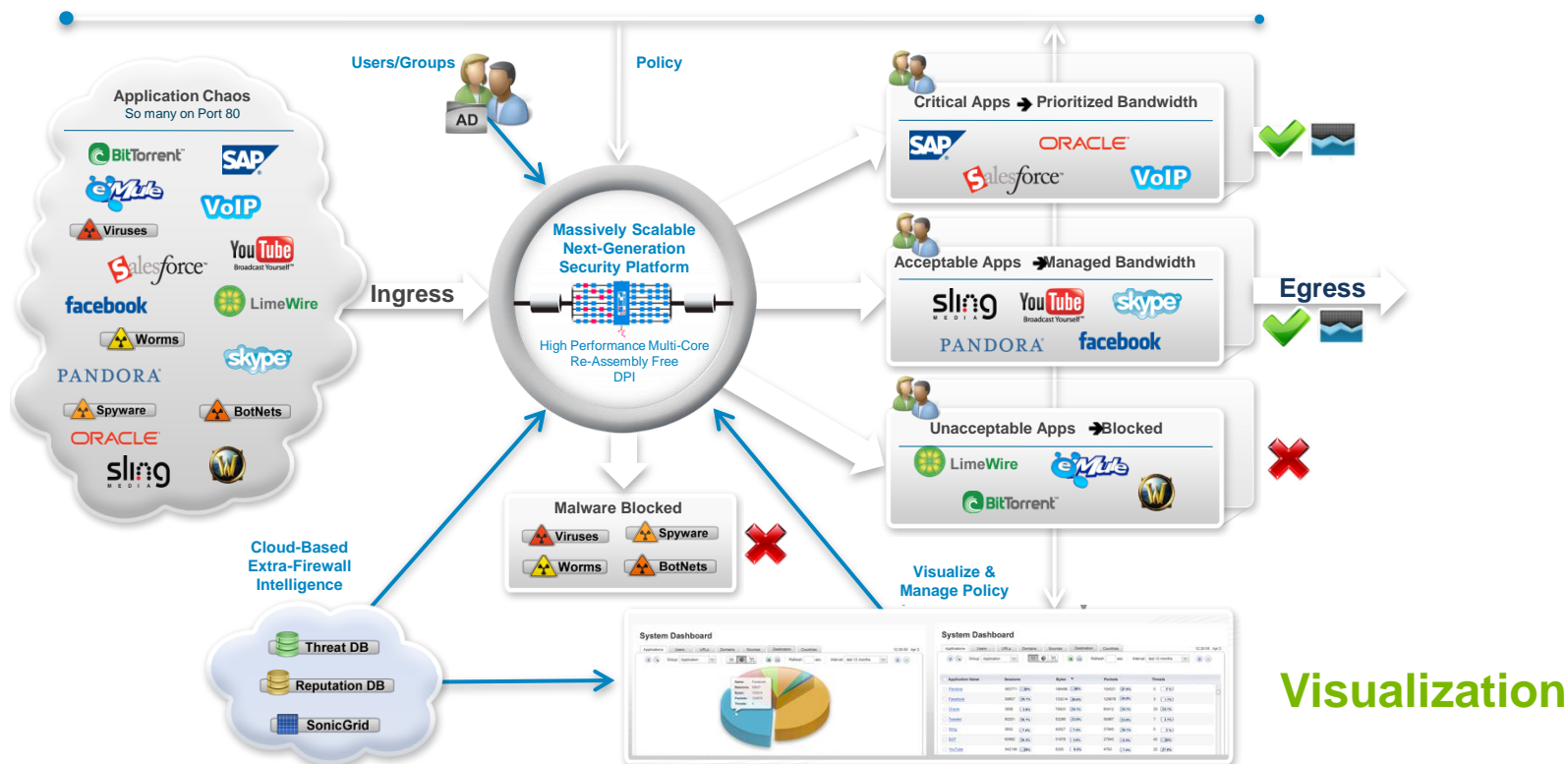
- By Application
- Not by Port & Protocol
- By User/Group
- Not by IP
- By Content Inspection
- Not by Filename

### Categorize

- By Application
- By Application Category
- By Destination
- By Content
- By User/Group

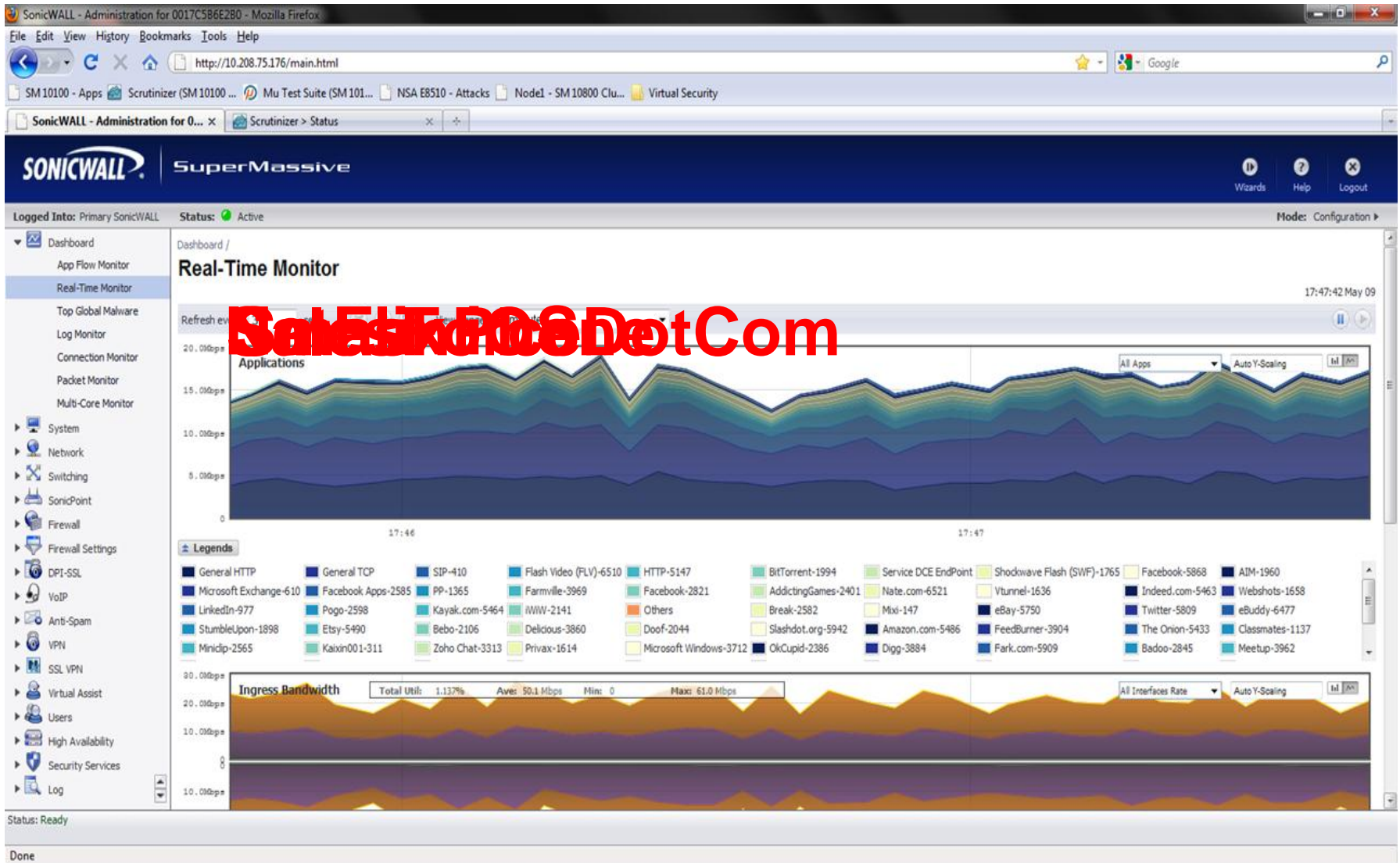
### Control

- Prioritize Apps by Policy
- Manage Apps by Policy
- Block Apps by Policy
- Detect and Block Malware
- Detect & Prevent Intrusion Attempts





# Network Traffic Visualization



## Real-time Traffic Breakdown



# Identify and Control Applications

Create Match Object

Match Object Name:

Auto-generate match object name

Application Category

Category	Threat Level	Technology	Attributes
<input checked="" type="checkbox"/> APP-UPDATE	<input type="checkbox"/> LOW	<input checked="" type="checkbox"/> None	
<input checked="" type="checkbox"/> BACKUP-APPS	<input type="checkbox"/> GUARDED	<input checked="" type="checkbox"/> Application	
<input checked="" type="checkbox"/> BROWSING-PRIVACY	<input type="checkbox"/> ELEVATED	<input checked="" type="checkbox"/> Network Infrastructure	
<input checked="" type="checkbox"/> BUSINESS-APPS	<input type="checkbox"/> HIGH	<input checked="" type="checkbox"/> Browser	
<input checked="" type="checkbox"/> DATABASE-APPS	<input checked="" type="checkbox"/> SEVERE		
<input checked="" type="checkbox"/> DOWNLOAD-APPS			

Name	Category	Technology	Threat Level	Attribute	Application Group
<input checked="" type="checkbox"/> BearShare	P2P	Application	SEVERE		BearShare
<input checked="" type="checkbox"/> eMule	P2P	Application	SEVERE		eMule
<input checked="" type="checkbox"/> iMesh	P2P	Application	SEVERE		iMesh
<input checked="" type="checkbox"/> Kazaa	P2P	Application	SEVERE		Kazaa
<input checked="" type="checkbox"/> LimeWire	P2P	Application	SEVERE		LimeWire
<input checked="" type="checkbox"/> Shareaza	P2P	Application	SEVERE		Shareaza
<input checked="" type="checkbox"/> The Pirate Bay	P2P	Application	SEVERE		The Pirate Bay
<input checked="" type="checkbox"/> WinMX	P2P	Application	SEVERE		WinMX

Cancel Save Application Match Object

Application Library with  
over **4000** unique  
Application Uses

## Granular Control

Allow Facebook, Block Farmville  
Allow Chat, Block File Transfer

- Group/User Based
- Schedule Based
- Exceptions

## Bandwidth Shaping

By Application  
By User/Group  
Scheduled



# Mobile Reporting

Implementing a good BYOD security solution should include reports that allow tracking of who is using what BYOD device and how many of each type of device are on the network

## NetFlow/IPFIX support

- Username, host, host OS and data details
- End to End visibility

Questions answered:

- How much bandwidth are all these additional devices collectively using and is it impacting business critical applications?
- What applications and web sites are users hitting and what impact are these distractions having on productivity and how often?
- What are the security implications introduced by allowing these devices onto the net?



# Dell SonicWALL NGFW Portfolio

## SuperMassive™ E10000 Series

Data centers, ISPs



E10800



E10400



E10200



E10100

## E-Class NSA Series

Medium to large organizations



NSA E8510



NSA E8500



NSA E6500



NSA E5500

## NSA Series

Branch offices and medium sized organizations



NSA 4500



NSA 3500



NSA 2400



NSA 250M/220

## TZ Series

Small and remote offices



TZ 215 Series



TZ 205 Series



TZ 105 Series



# Market Maturity of SSL-VPN and Firewalls

# Next-Generation

Independent lab tests  
validating testing  
products extensively

Major Magazines  
conducting shot outs

Renown organizations  
providing certifications



BYOD doesn't need to eat your network or  
break your budget

Adopt either Smart Mobile SSL VPN Strategy  
or MDM

Make the move to Next-Generation Firewalls

The result is GREAT access, HIGH Security,  
Lower Cost, Happy Users

