

Unified Threat Management for Wired/Wireless Security

Integrated Security for Wired and Wireless LANs

John Gmuender

Vice President of Engineering, SonicWALL, Inc.



So, Is It Really All That Bad Out There?

SONICWALL

You've Seen It On TV

CNN.com WITH FREE VIDEO
Member Center: [Sign In](#) | [Register](#)
International Edition | [Netscape](#)
MAKE CNN.com YOUR HOME PAGE

SEARCH THE WEB CNN.com SEARCH Powered by YAHOO! search

Home Page
World
U.S.
Weather
Business at CNNMoney
Sports at SL.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports
Video

TECHNOLOGY

\$1 million Web site targeted by hackers

Thursday, January 19, 2006, Posted: 5:32 p.m. EST (22:32 GMT)

LONDON, England (AP) -- A Web site that earned an enterprising British student \$1 million suffered a crippling attack by ransom-seeking hackers.

Alex Tew, 21, said Wednesday that his Million Dollar Homepage was targeted after he publicized how it had helped him raise money for his university studies.

The Million Dollar Homepage

Search Jobs MORE OPTIO...
Enter Keywords
Enter City ALL
careerbuilder.com SEARCH

Compare Mortgage Rates
✓ Refinance
✓ Home Equity
✓ Home Purchase

MSNBC Home Technology & Science Security Sponsored by **EQUIFAX**

Web virus holds computer files 'hostage'

Hackers demand \$200 in 'ransom-ware' attacks

Ap Associated Press
Updated: 4:49 a.m. ET May 24, 2005

WASHINGTON - Computer users already anxious about viruses and identity theft have new reason to worry: Hackers have found a way to lock up the electronic documents on your computer and then demand \$200 over the Internet to get them back.

FREE VIDEO

Tech / Science
Science
Space News
Tech News/Reviews
Security
Wireless
Games
Innovation
Digital Life
U.S. News
World News

BBC Home News Sport Radio TV Weather Languages

BBC NEWS

UK version International version About the versions | L

News Front Page
Last Updated: Tuesday, 30 November, 2004, 06:02 GMT
E-mail this to a friend Printable version

Surfing the net, but at what price?

Yesterday we reported on the latest scam in which a computer user's internet dialler is diverted to a premium rate or international number.

You only find out you've been affected when suddenly a massive phone bill drops on your door mat.

Follow Robert Freeman's advice don't get hi-jacked

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

Breakfast's Max Foster reported on the story for Breakfast

SDA ASIA

Software, Development & IT Architecture

Home News Magazine Events

'Really Bad' Exploit Threatens Windows

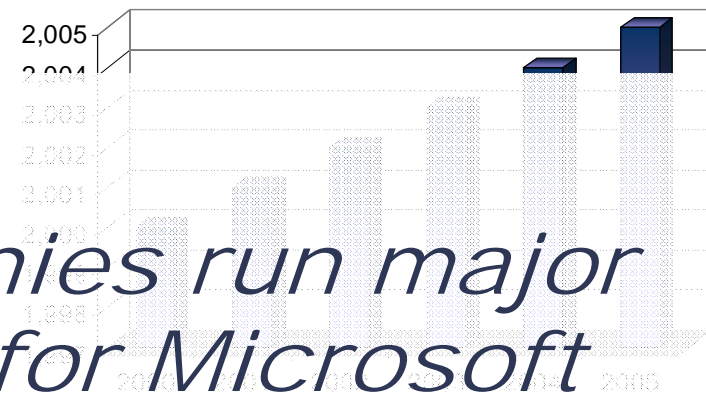
A new exploit has been discovered in the wild that affects fully patched Windows XP SP2 systems, according to reports by security firms F-Secure and Sunbelt. The malicious code takes advantage of a vulnerability in the WMF graphics rendering...

A new exploit has been discovered in the wild that affects fully patched Windows XP SP2 systems, according to reports by security firms F-Secure and Sunbelt. The malicious code takes advantage of a vulnerability in the WMF graphics rendering engine to automatically download and install malware. WMF, or Windows Metafile, is a vector based image format used by Microsoft's operating systems. SHIMGVW.DLL is loaded to render the images and contains a flaw that opens the door for a malformed WMF image to cause remote code execution and potentially allow for a full system compromise.

News
Magazine
Online Articles
Features
Interviews
Issue
Event Spotlight
Subscription

The Data Is Widely Available

CERT Incidents and Vulnerabilities*



- *Network Attacks are on the rise*

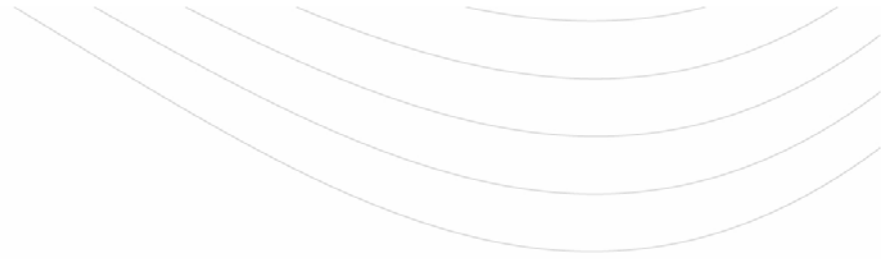
Only 7% of companies run major security updates for Microsoft

- *49% of 10 Companies Hit By Computer Crime - FBI*
use insecure applications

- *“Global Malware cost estimated at \$169-204 billion” - New York Times / Radicati Group
Vnunet*



“Only 7% of companies officially run Microsoft's major security update (SP2) released in 2004” – New York Times
“More than 85% of all enterprises report using instant messaging for business” – Radicati Group



Wrong.

Here's why...

Today's Reality

1. Organizations and people are dependant on technology
2. Attacks are now both obscured and actionable
3. Time from vulnerability to exploit is shorter

■ ***The new attackers:***

- ✓ Cybercrime Organizations
- ✓ Mafia Organizations
- ✓ Professional Hackers
- ✓ Company insiders



■ ***Perpetuated by:***

- ✓ Outdated technology
- ✓ Continual security changes
- ✓ Limited control
- ✓ Human factors

Tell me more...

The Information

- Buy: Financial Information
 - Use: Login Information
 - Extort: “Carding” – Fraud
 - Disguise: Anonymity
 - Steal: Competitive Information
- \$100-\$5000:
 - The “keys” to exploit a software vulnerability -
 - \$150-\$500
 - List of 5000 SME IP addresses of computers infected with spyware/trojan for remote control
 - \$500-\$5000
 - List of 1000 working credit card numbers -
 - \$100K-\$200K
 - Annual salary of a top-end skilled black hat hacker working for spammers or malicious mid level managers -

The Tools

- Remote control software
 - Called rootkits & botnets
 - Complete control of a computer
- Spyware & Phishing
 - Obtaining quick information
- Targeted Viruses
 - Specifically targeting a single site or organization
 - Turn off existing protection
- Internet attack tools
 - Metasploit, etc



RealTime PC Monitoring

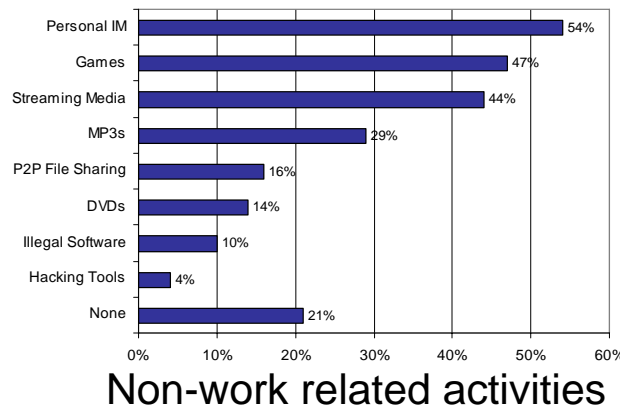
System Information Update Information Clear All Logs Adr

Timestamp	Window Title
Thu 05/16/02 @ 02:43:40 AM	SurfSecret TRIAL
Thu 05/16/02 @ 01:29:25 AM	Input Registration Code
Thu 05/16/02 @ 01:29:22 AM	Program Manager
Thu 05/16/02 @ 01:29:16 AM	Inbox - Outlook Express
Thu 05/16/02 @ 01:26:43 AM	Re: hi bryan
Thu 05/16/02 @ 01:26:37 AM	Inbox - Outlook Express
Thu 05/16/02 @ 01:26:25 AM	XML File Detail - Microsoft Internet Explorer
Thu 05/16/02 @ 01:26:16 AM	RegNow Control Panel - Microsoft Internet Explorer
Thu 05/16/02 @ 01:26:10 AM	Enter Network Password
Thu 05/16/02 @ 01:26:07 AM	doug.txt - Notepad
Thu 05/16/02 @ 01:25:58 AM	hwnd bryan's Buddy List Window
Thu 05/16/02 @ 01:25:52 AM	RegNow Control Panel - Microsoft Internet Explorer

The Reason: Humans

The human factor cannot be ignored:

- **30% to 40%** of employee Internet use is not work related*
- **80 Million Americans or 27%** of the US population use IM*
- **55%** of online users have been infected with spyware*
- Instant messaging security threats **double** every 6 months*



Bottom line: Network misuse provide the fuel for today's organized crime and workplace productivity issues

Understanding Impact to Business Owner

- We understand the risk, security and productivity challenges in today's cybercrime world. What relevance to they have to a business owner?
- *What are the business challenges and pain points?*
- *What should they be doing differently?*
- *How can technology ease their pain?*
- *And what should they look for in a solution?*

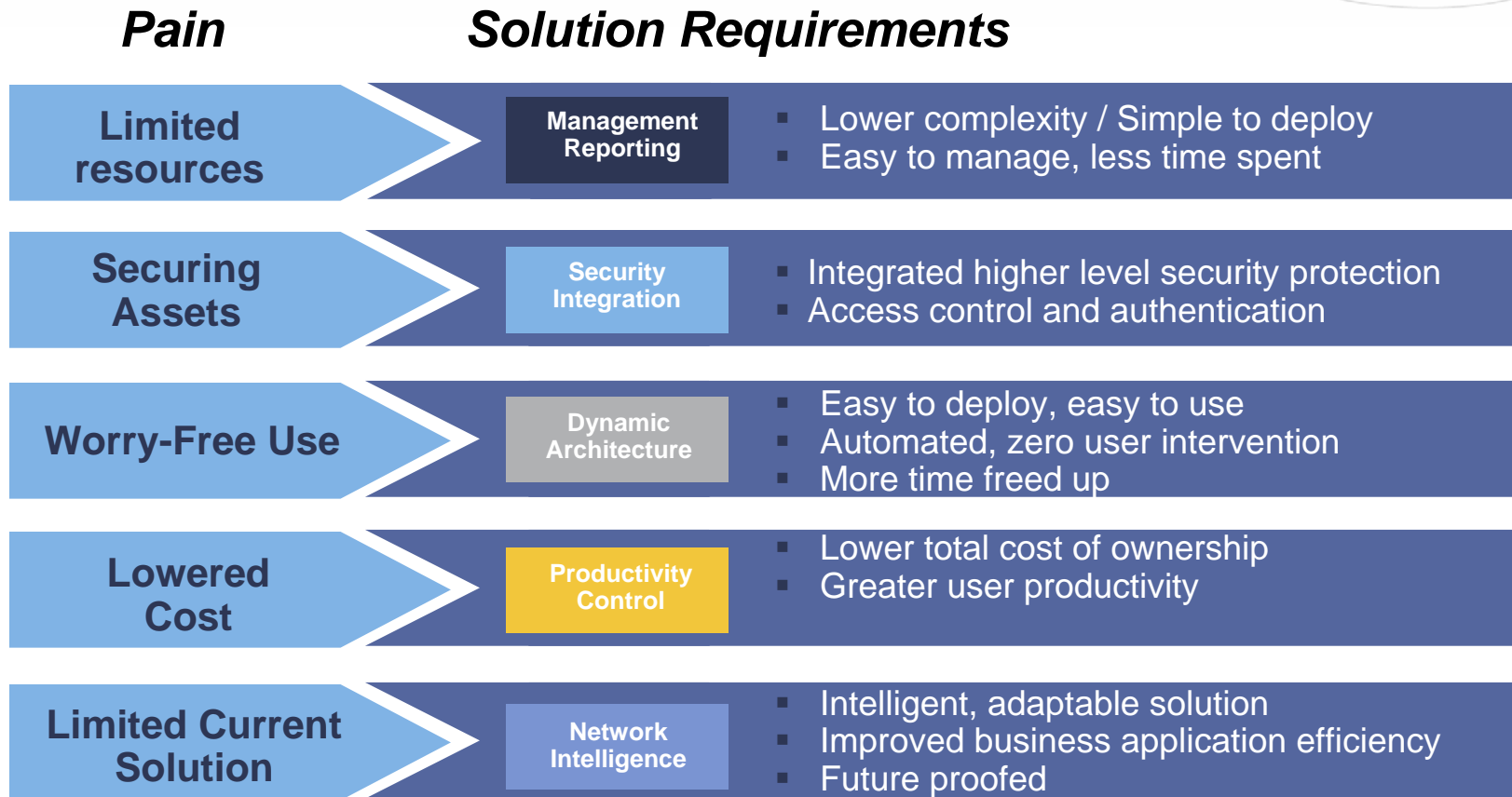
Business and Communication Trends for Wired and Wireless



- Networks are getting more complex with more dependency on technology
- Employees with little technical knowledge use company technology, introducing risk
- Less resources to work with
- High price of security problems, downtime and productivity loss
- Competitors are rapidly integrating newer technology to get ahead

Businesses today must continually achieve more while using limited resources and controlling costs

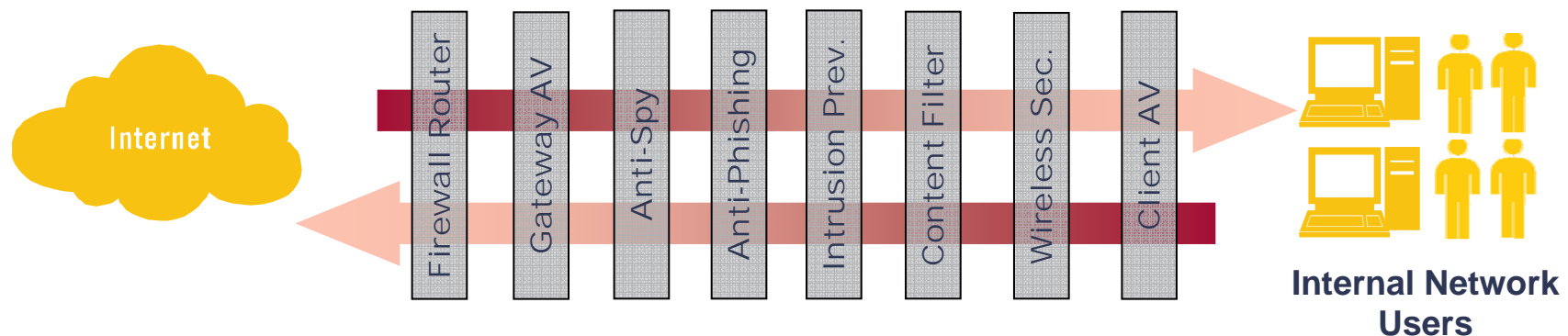
Business Pain Points & Requirements for Wired/Wireless Solutions



Businesses want reliable communications and lower total cost of ownership

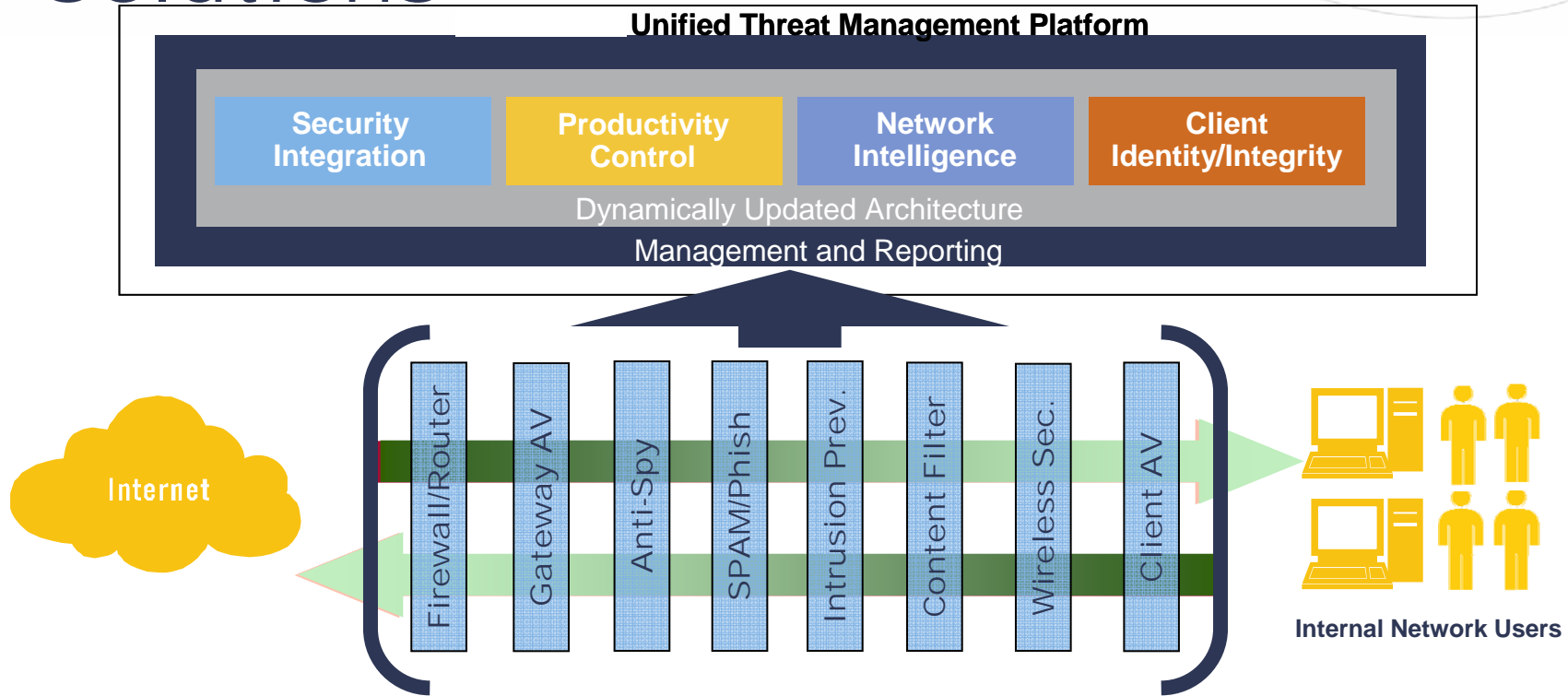
Current Solutions

- Current wired/wireless firewall technology is limited & cannot effectively prevent today's threats or network misuse
- For complete protection many have cobbled together wired/wireless security solutions from multiple vendors with little to no integration



However, the net result is higher overall cost of ownership and increased resource demand & performance concerns

Unified Wired/Wireless Platform Solutions



Unified Wired/Wireless platform solution integrates deep inspection to:

Solve business pain points, offer more reliable business communications, lower TCO & greater overall performance

Unified Wired/Wireless Platforms Provide Better Solution for Business

Security Integration

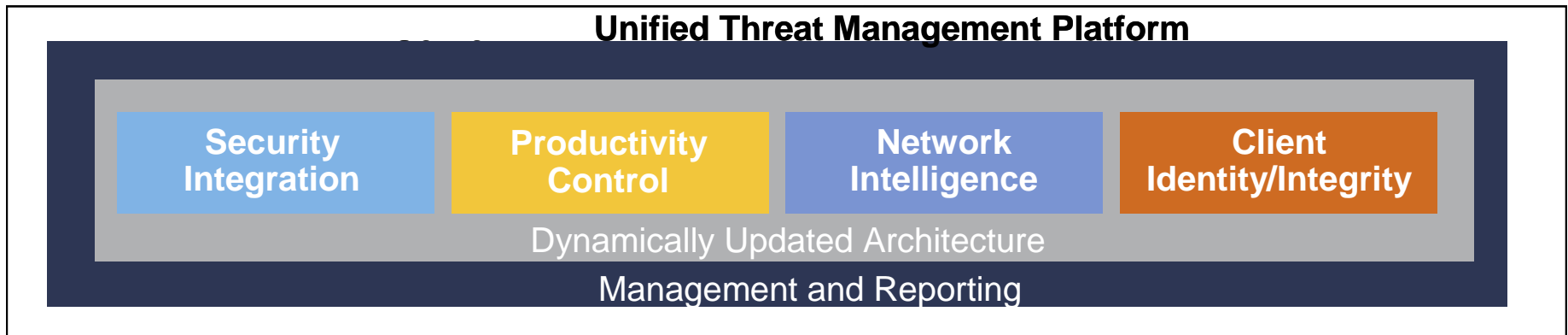
- Complete Protection
- External Prevention
- Internal Network Security
- “Clean VPN”

Connectivity

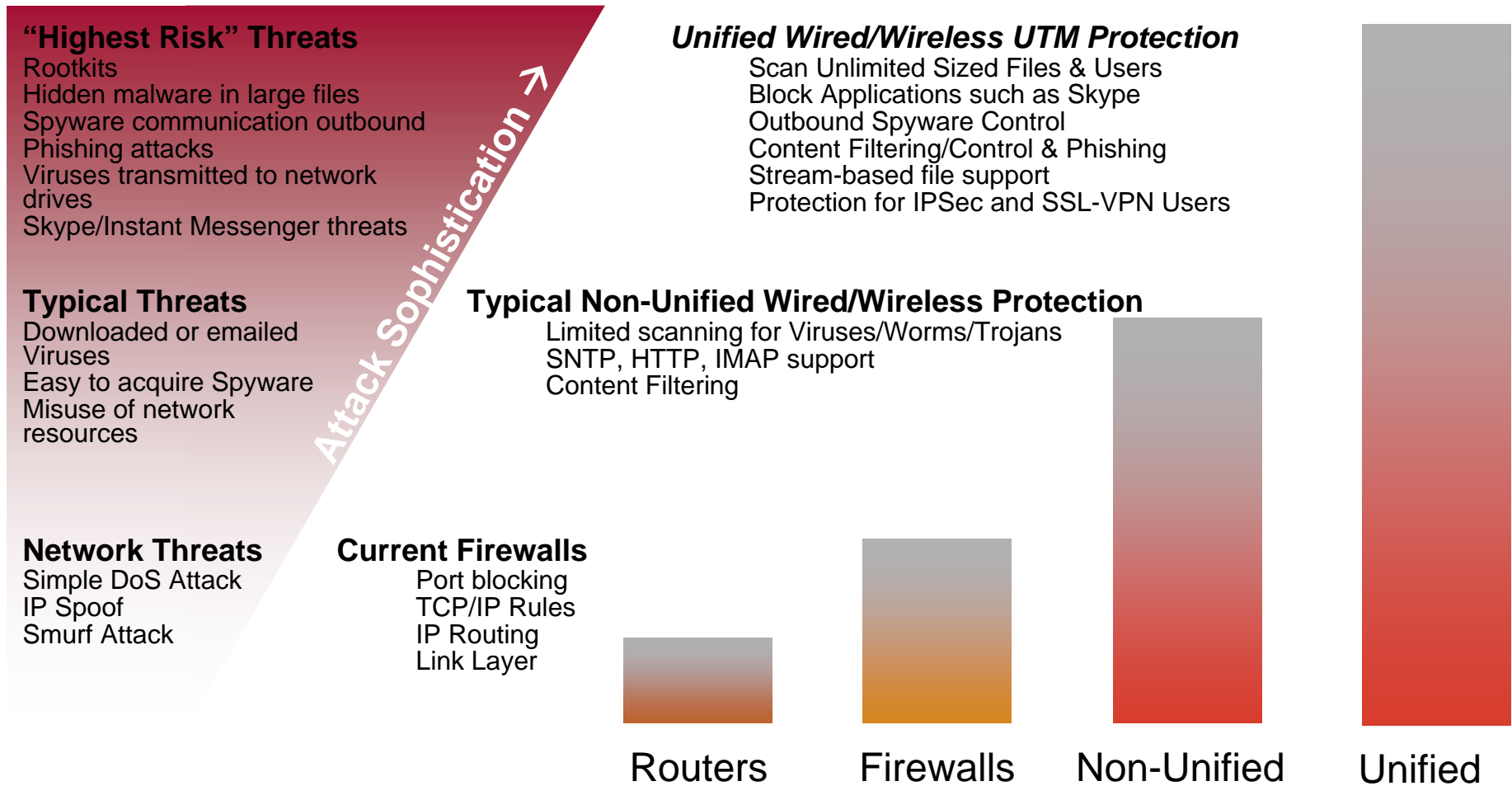
- Secure connectivity
- Access to resources
- Wireless mobility
- Network availability

Intelligence & Optimization

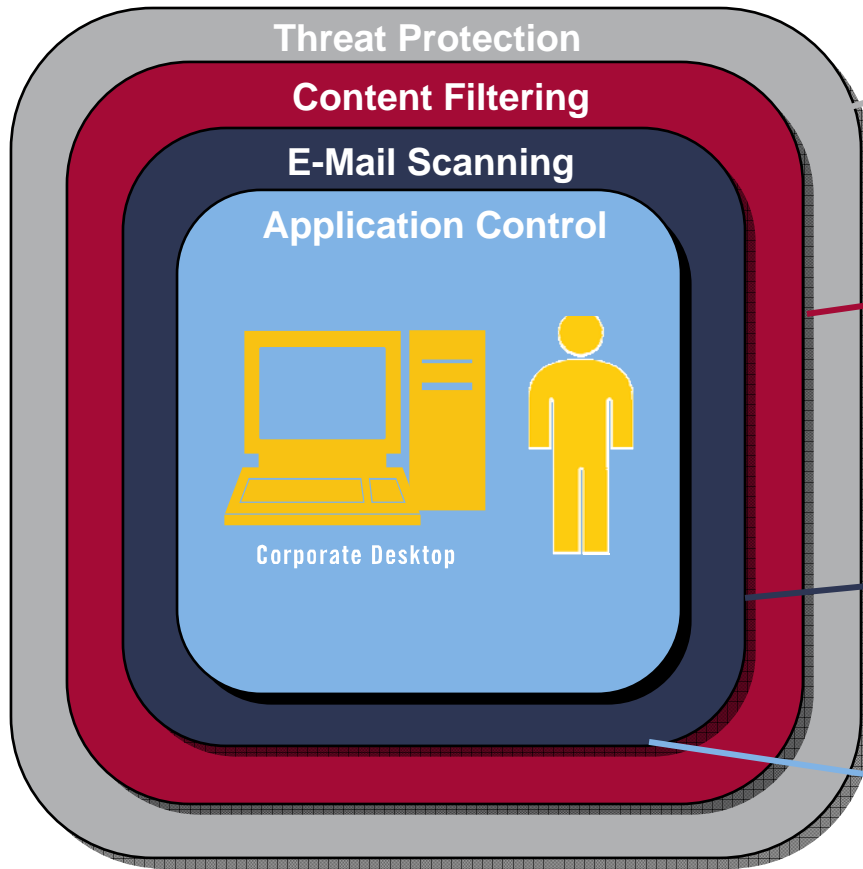
- One point of network control
- Content & application filtering
- Business application prioritization
- Ease of deployment & management



Wired/Wireless Protection Solutions Options



Unified Wired/Wireless Solutions Provide Granular Control



✓ End-User Security Protection

- Spyware / Viruses / Rootkits
- Malicious Code and Trojans
- Enforced client

✓ Productivity Control

- Inappropriate Websites
- Spyware infested sites
- Fraudulent sites

✓ Messaging Protection

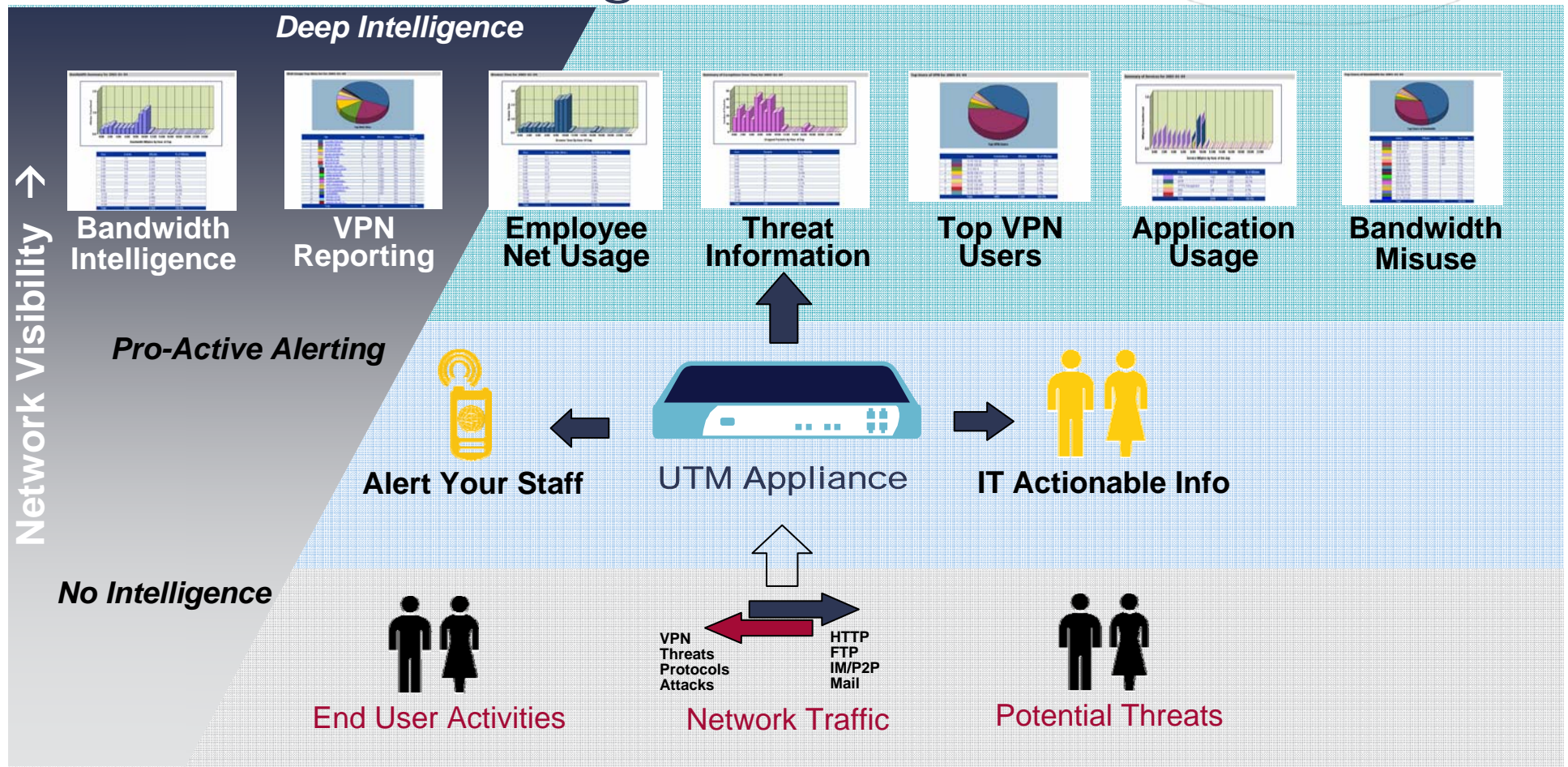
- Virus email scanning
- Phishing
- Pharming

✓ Prevent Non-Business Apps

- Productivity Loss
- Errant Application use
- Misuse of Network Resources

***Wired/Wireless UTM Provides Greater
Administrator Control & Flexibility***

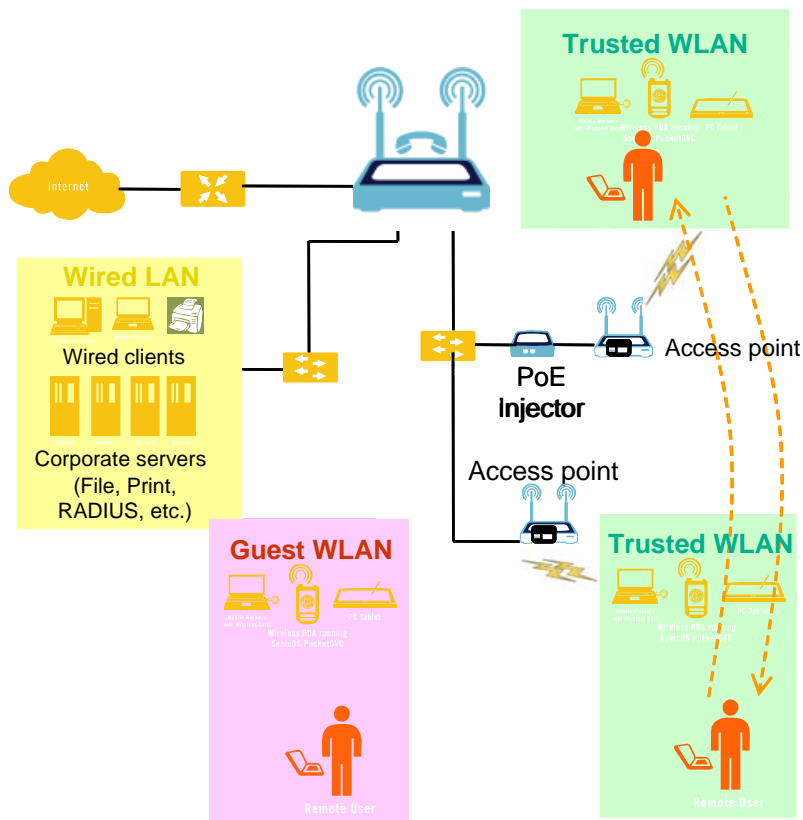
Unified Wired/Wireless Solutions Provide Business Intelligence



Unified Wired/Wireless UTM Can Deliver Deeper Business Intelligence

Unified Small Office Deployments

Integrating advanced Unified Wired/Wireless UTM services within the existing network and security architecture



Provides:

- **UTM** solution for wired and wireless networks
- **Enforced wireless security** through VPN and SSL VPN
- **Granular control** of wireless user network access
- **Standards-based** WPA, IPSec and 802.11i encryption options
- **Rogue access point detection** minimizes backdoors
- **Wireless guest services** allow easy Internet access for guests

A series of thin, light gray wavy lines that originate from the left side and curve across the top of the slide.

Thank you.

John Gmuender

Vice President of Engineering, SonicWALL, Inc.

The SonicWALL logo, featuring the word "SONICWALL" in a bold, white, sans-serif font. A white swoosh underline is positioned above the letters "WALL", starting from the right side of the "W" and curving under the "L".

SONICWALL