



Security Without Sacrifice: Delivering Affordable IT Security Without Breaking The Bank

Nelson Da Silva
Fortinet

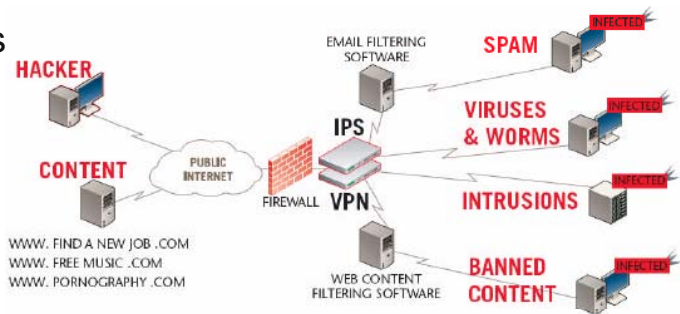
Benefits of being online

- New Education Initiatives
 - Distance education
 - Audio/Video On Demand
 - e-Learning, e-Mentoring
- Collaboration
 - Students, Parents, Faculty, Community
- Communication
 - Social Networking, Research, Administrative, The Blogosphere
- And The List Goes On and On...



Education Network Challenges

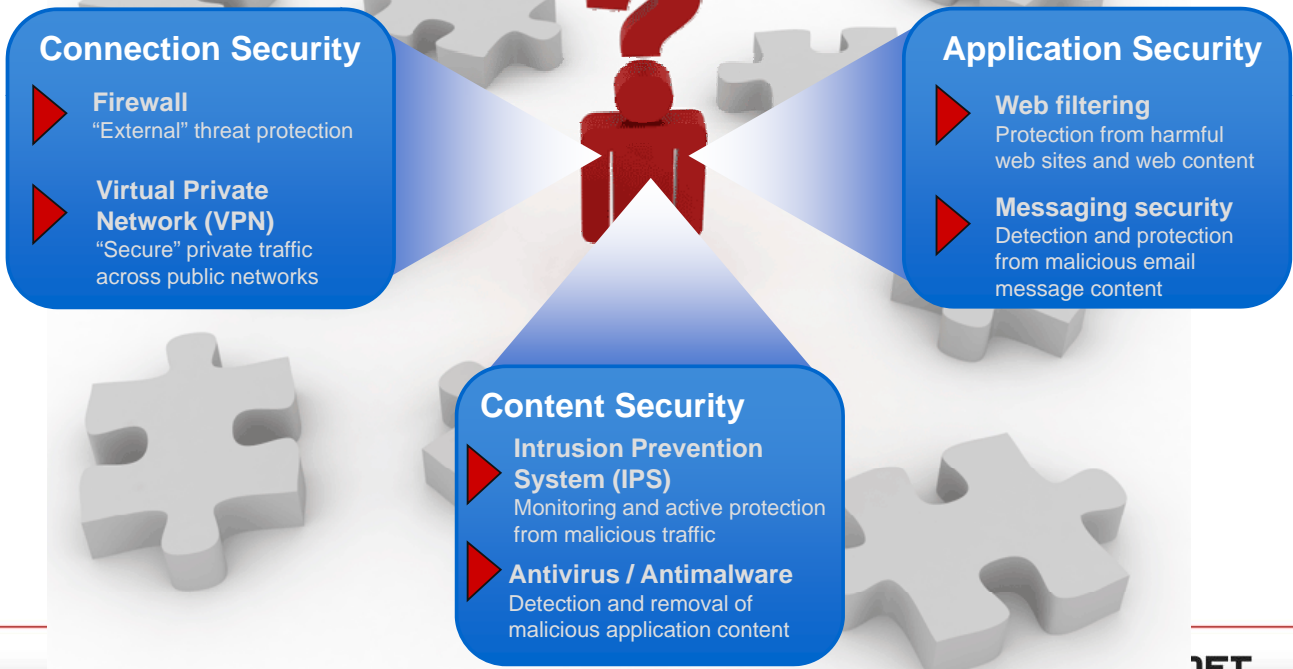
- Rapidly increasing bandwidth: 10Mb, 100Mb, 1Gb, 10Gb...
 - New initiatives: Research, Audio/Video, P2P, Mobile, Web 2.0...
- Users: Students, Parents, Faculty, Community
- New Service Models
 - Time Sharing, Out Sourcing, Virtualization, Cloud computing
- Remotes access
- Malware and Illicit Web Sites/Content
- Commitment to open networks
- Limited Funding
- Duty of care



Not Just Windows-Based Clients



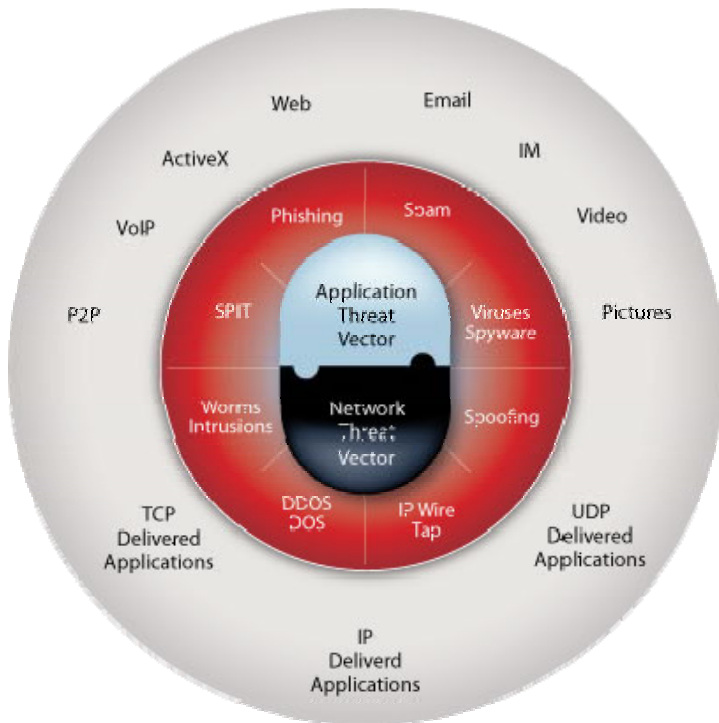
Navigating the Security Landscape



Feature Priorities

Feature	Firewall	AntiVirus	IPS	Web Filtering	VPN
Tertiary Education	4 blocks	5 blocks	6 blocks	1 block	2 blocks
K-12	5 blocks	3 blocks	2 blocks	5 blocks	1 block

Multiple Threat Vectors



Multiple Threat Types

- Various Application Entry Points
- Different Attack Functions
- Threat Payload Intent Varies
- Broad Range of Propagation Techniques

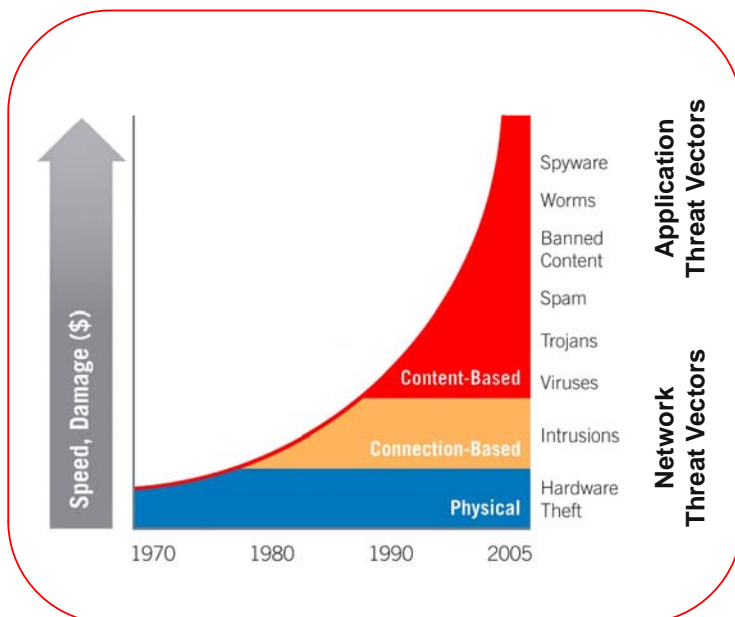
Application Threat Vector

- Viruses & Spyware
- Spam & Directory Harvest Attacks
- Web Phishing
- IM and P2P file transfers

Network Threat Vector

- Network Worms
- DDOS/DOS
- IP Packet Capture
- Spoofing & Man-In-The-Middle

Blended Threats Leverage Multiple Threat Vectors



Malicious threats lead to

- Data loss
- Identity theft
- Database espionage
- Network downtime
- Bad publicity
- Regulatory fines

The motive has changed

- From notoriety to criminal intent
- More malicious in nature
- Global in reach
- Predatory behaviors

So... What is a blended Threat?

• Blended Threats

- use **multiple infection and attack methods** to leverage vulnerabilities found in operating systems and applications
- **harder to detect and block**, blended attacks are created with a hybrid of technologies such as **virus, worm, Trojan horse, and backdoor attacks** that are delivered with email, infected Web sites and even alternate media
- May deploy social engineering techniques such as Phishing and Grayware



Trojan

+



Virus

+



Vulnerability

=

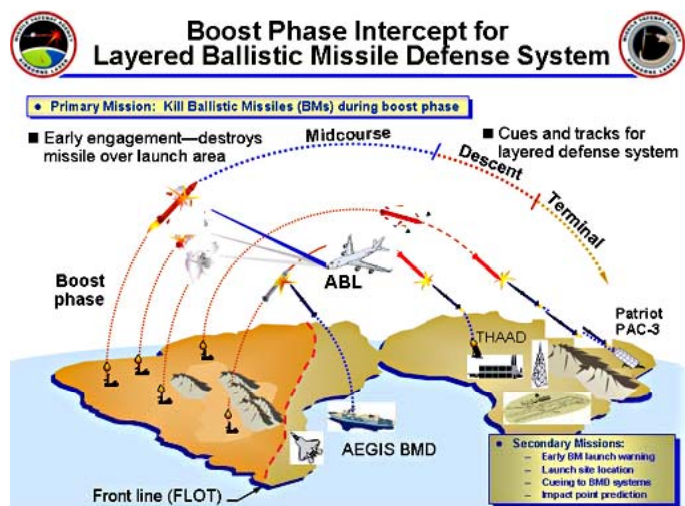


Blended Threat

Threat Life Cycle

Four Distinct Phases

- Transmission
- Penetration
- Launch
- Propagation



Transmission

Penetration

Launch

Propagation

Blended Threat – W32/Pushdo!tr



- **Multiple Attack Vectors**

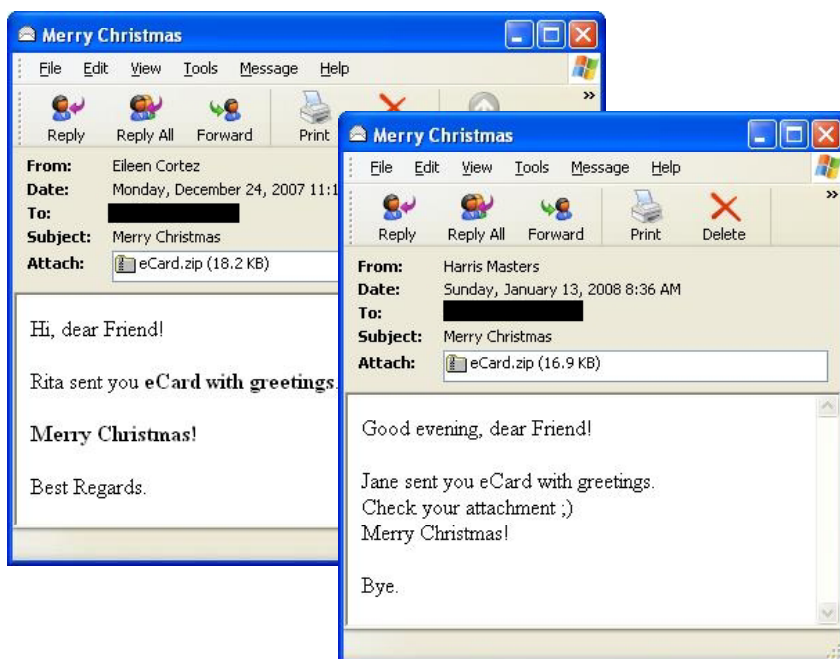
- Spam email with malicious attachment
- Email contains a trojan downloader
 - Downloads a rootkit to cover activity
 - Downloads multiple other components
- The trojan uses a command and control communication channel



Real Time Network Protection

FORTINET

W32/Pushdo!tr - Antispam



- Antispam recognizes email as spam
- Blocks message from user's inbox

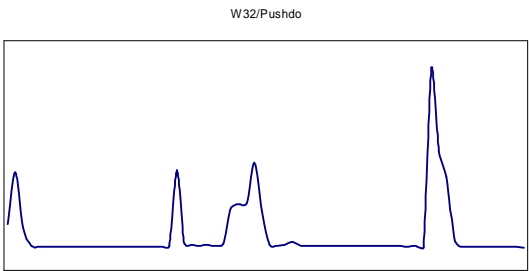
Real Time Network Protection

FORTINET

W32/Pushdo!tr - Antivirus

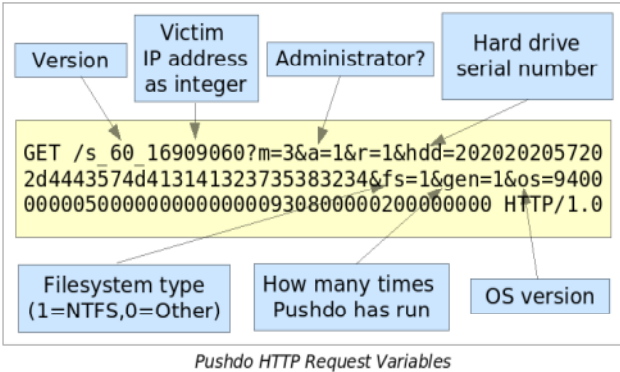
```
#epP5ppStUhc19xuuQ2Hur+HdGBA18+FuNX5IvSkjvRk1SSmpHAKqZcJf395SUpt9HRpLZ1hpQ7IEO
>ymp5H18kGd1T3gsYsdgPj4xMSKYpKkMjCggRhInor8yKQcWt0MObPNzbCDHr8ag+zMz32Cb
>QHypVzuqYdSB3c8fgtr8JukTchAmMkgmKkUIdRMfjyQ+hY76I4XYpgk6OmsB+HmZ4+Ev8TKvQgdXN
V2OkptYkd279VSL8EK9korYOVMQeMUyUq2YVIC1JAgW/ZusU002YkoadXIrAmKoEG74WRT2VH1
eFVZKsmF6bKCBORZxGoo2H2k1DhPKJgqmJDRMSyVJrdXNvRLJp0LFVZhe8W6qdd6YrDAb1U8j
JG41j0y1kxq/vgHe/rjHvypTe5PFCYpB5WbWcb/Ha0SnrKjTfH9CbJXE69MGLx16fU92YvOqLXx
j85bZ2vAOrLSeppNeh9MvMdb6sp6WYKvSvAcvawM4qIYeQkifXdeyMhOocRvIdSd3KrcQntb
<ZfV0cNOL0xVfFRP1CJAdzGcpjSsWpV5qIpD1J3S9+W2HjKRAOPmYdHST6H1VR6AmGtq6VC8s6
sR6W5UvSFIP3JMoXvLzEdhewchlbz1Bf71iKv9SvKvS5c1N8svoqVklhwaGe17/sN6Crc6K4C
a2cv1/0IKKkA3QVGLG/CgppPz8R1bJ1OPGFSptYIrh2GmXLE5UYXnkXHEHsJaGmx5SHxM17x0
15ZVhWfrn2dYnX+2aCt1nD64H6Pd5zjPn/1Qy17401V4WH+17duDHeLyJCSmqtIof45htuJ93
>J4U1AmpSaHeG5dv8gm3Dt+6VrErgIzrpyDKO/cpHBoeDIH01Wr7RbrrrIeGNw6F/X+rFnR/+R
/jQeJXwbjzwy5f/1d4P10cAvLxhzDDdK/emDxtY10ogSfWeP5voL0sLukONcbZTAU40j3vZakwU
lBc028aQ/vwFrCFEMBEubytTz2c8/Yhwz3eZJXFSLwrKJtVu2x2TKiFRJmV03xwER2Tt1w
2D+ppGvt238j1e9eXieGE+05FL52QzffURrnfobqLpUgcVrSxXpqrXrcZ2qgOEZeeQ0e3RiIjP
2N6G1P9bP10C1NyADrMabmLv33h4pGgz6Jh901AU2jdBKEQ81q6FvtXzfHD8YglwCmI+POZTVI
2C9fzvwvXIDj1jTj3rAEB/m43VseS1Ss3mh+oMdV7/9pCNDYUD:FzFz9Yn/SSAn8d/y9qYzb
/2QvfyGYEajzI+nk2UJp46urOug/krFE+GeD3AWK/pfFmCrqdrqMdtILzND+KNXkAZeUuzr+3c
/2Pp/Y3/LaqlqVx2zj3ACxtCpPC5I4CAdc4J9JZAS6C8A1Z8AdgK1eVAVXkAZeUuzr+3c
1Vz1krA/QDZA2NAyveELANyD2gocAAyAeAZU2mWbNAfOAsyNSUTuVMB3gBGAeYAgpTARNDNg3M
5wFARc410Fn8eJkK4y4DbArYANASrCrgdM41QYGZU3z0ppvrXkXUOVfZNR9TyYnlpRk4daxRT
j3P12rPuj6GE7rGdWq9V9ndLVYK2837+H7FyF8mfhZLqqrIzP+svCBXDjrcJMPo7KZb0E7jvLn+
+AMhmf187KwXAhHMYqx2TiaECXK/TR3JVA4Zczk987HbdagmWAg9e9QE/jxk7Qnruc1Q31uHPX
2X110AcJXTSufZQDeVXY11mlByT9b0uIjFfIeg3Irg9Qq06K5EPxPul9HtuCP1/MdrWQch3Qn
lKvMmaipq8uMhKf/zt13n3Ekw+1F2ESZwKzKt1Lsr1Vgkx041uukwX1/1ALsv0Blnep9B8q
H/DEUE604V4OnGEXIDIPwE5wppRjKdUL+BeT157qzTqMfbpVwEYf6G0U0uQxQL0VnG3sLqY
fvkzsg9g1zXIfjseW/LN4nqyyqA+Jy4F5EPKMaTmTcm4EKKG7BP3hH2DyU/InwlpJFC3D0cc
2bF8069r9089p0H6W2A0hK+1Vmt1ug9wnXKvfsy2xc718enTkpdyFXQ70gmkmX182X0qB3ja
22U4y9vD90Hk+40BD1PQPKsv1QUX2+RzHPK+bcQY+83G00He92c37G3Dr9zIHdVUF42h12k
K50wF86hwAaX0X0/aNjX9A5eaAPHRIR3Ij0y1V6L0Y+HCE+k+dvV05f0WXj7PjKrbOYH4ZV54f
3J9b95+kK1c4y/yFUP5DC1/QLJPJeYp108+pr/PfkhNhsKfWnqaHwP14zm011Yn48Flq11BV5Q3d
2g7mc30soPofw4qE11UDLL6y2fdSOZIDL+3mPq11H6o++ENS87ZXumcF0u87ZaZr1k1SMEITN
5uP0H13j8e01555493ubQD/erT1wo7cB3gmcbQkfjmkJ52mlpv4W0KpQLL+1Hr0276czA7574W
7YV1u9TxU1r6hR6I8ySe8YHF4L9jeS00dFwQBcvxdhqrj00P0sg5vEpF1ggTc#4q1y7cJeg9
fVHL5YWAhNznTtM6EXDX16RYpC3c7QLpLnTnpN4TboxYb1hwh3yRNaW1x6cgjx/zVwVw/HaL
314r1936TuvOL/Ip5c0eGexX/IXHqoZ1jAOHvS2mE40HnNFcnxXLIj5G651qfyyvSg246V5Zme
21+kwK1v9E6SNOHPWkNCog3yH65V99ScpFwBTr1EQH3m2UhsYX7cYEvsIEQoPv1X26DT/wagP
110y1oTSdrV8rXKw75sYsBdlr07uKWwYxf1744rEQqyKAF1ZnEZYkPQxcTt1q0Cvmk1vD2YE6G0a
5yhm9Cg8W1zF7j3mBnLQ6P8yszH1nc1v/ZG0RrQ0TbQF+KpT9bHXq4hNulYUUPC867D//uYWh
```

- Gateway antivirus detects the malicious attachments
 - The trojan downloader
 - The rootkit
 - The various other components
- Removes malicious payloads, preventing accidental execution

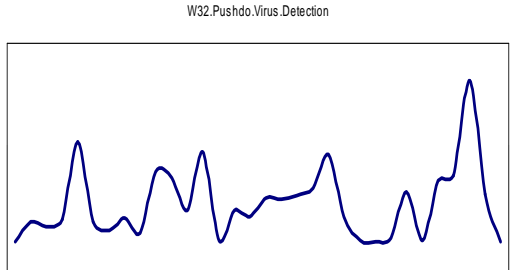


Real Time Network Protection **FORTINET**

W32/Pushdo!tr – Intrusion Prevention



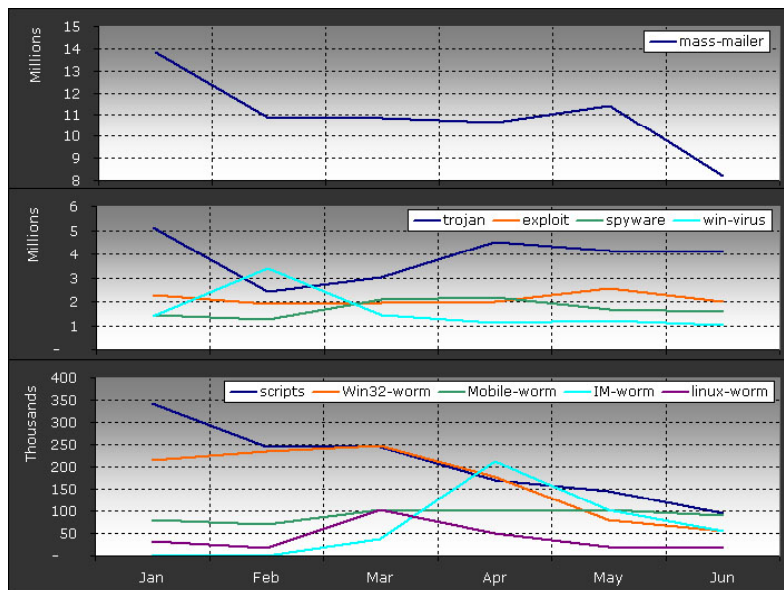
- IPS detects communications on the command and control channel
- Blocks the transmission of the infected host's communication



Real Time Network Protection **FORTINET**

The Changing Threat Landscape

- Threats vary and evolve over time
- Consolidated appliances provide broad coverage for consistent protection



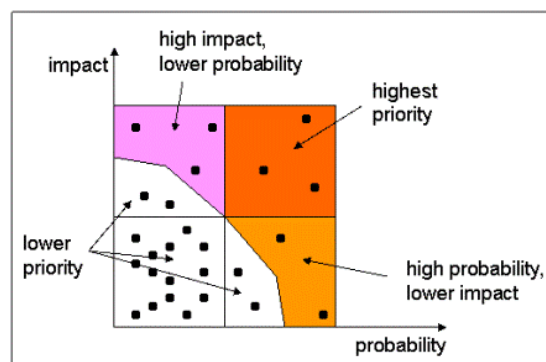
Source: FortiGuard Research

Real Time Network Protection

FORTINET

Assessing Your Risk

- Business Impact Assessment
 - What's the Impact of a negative event?
 - What's the probability of it occurring?
- Threat and Vulnerability Assessment
 - What threats and vulnerabilities exist?
- Risk Assessment
 - Over Simplified:
 - Risk = Threat x Vulnerability x Impact
- Keep It Real
 - Compare with others
 - Does it make sense?



Defense in Depth

- Strategy
 - Layer defenses against threats
 - Not just multiple vendor point solutions
 - Vendor agnostic strategy
 - Consolidation is your friend
 - Increase the difficulty for attacker
 - Ease of administration
 - Simplify enforcement
 - Educate faculty and students

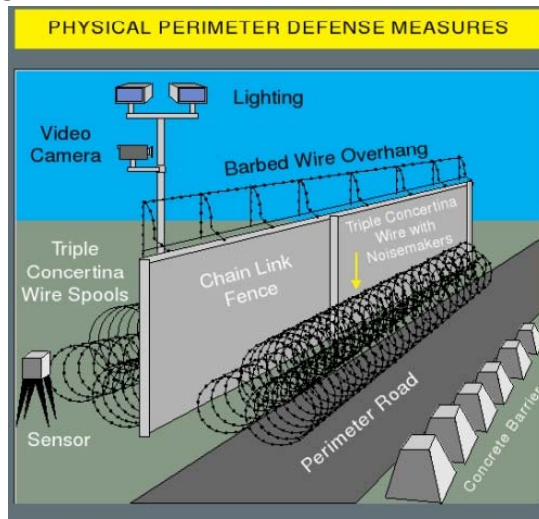


Figure IV-7. Physical Perimeter Defense Measures

Are You Maximizing Your Investments?

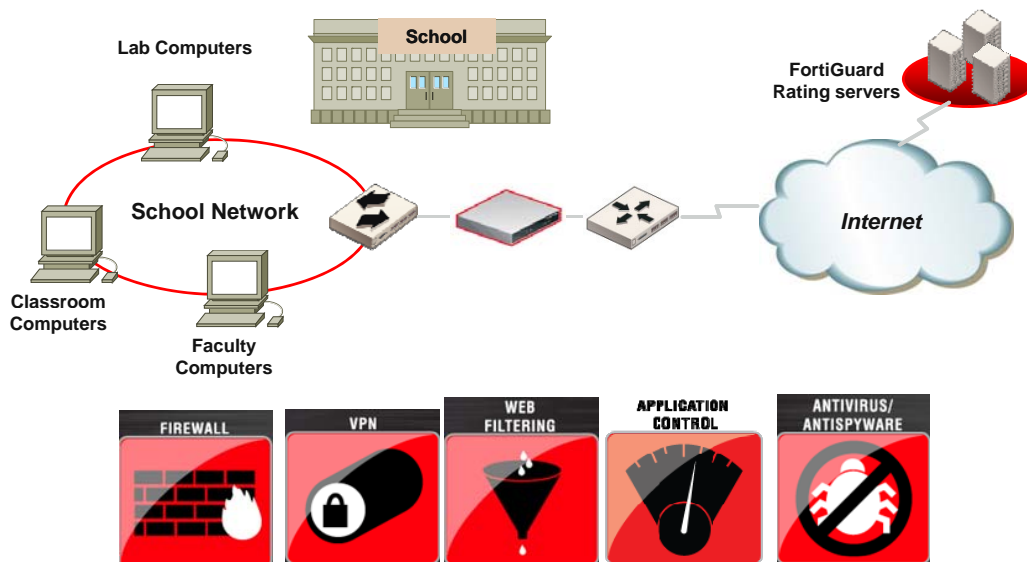
- Observe resources required to maintain systems
 - Moves, adds, changes, training, maintenance
- Re-Architect and/or Redeploy where needed
 - Media sharing and segregation
- Shape your traffic
 - Network and application level
- Consolidation
 - Infrastructure, Data, Web Services
 - Virtualization



Some Case Studies



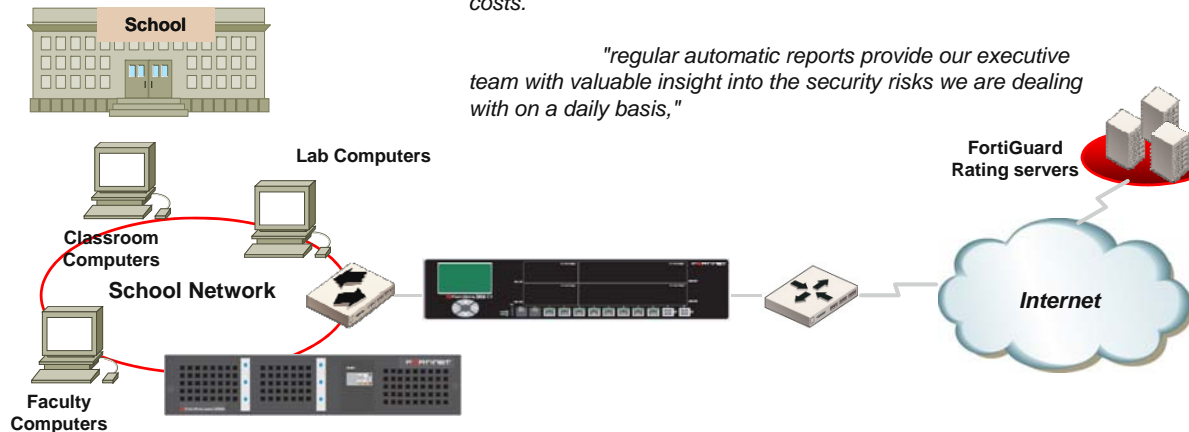
School Deployment



TAFE College Deployment

"The \$1.5 million savings will be achieved by reducing costs associated with outsourcing agreements, savings on equipment costs and software licenses, and reduced ongoing support costs."

"regular automatic reports provide our executive team with valuable insight into the security risks we are dealing with on a daily basis,"



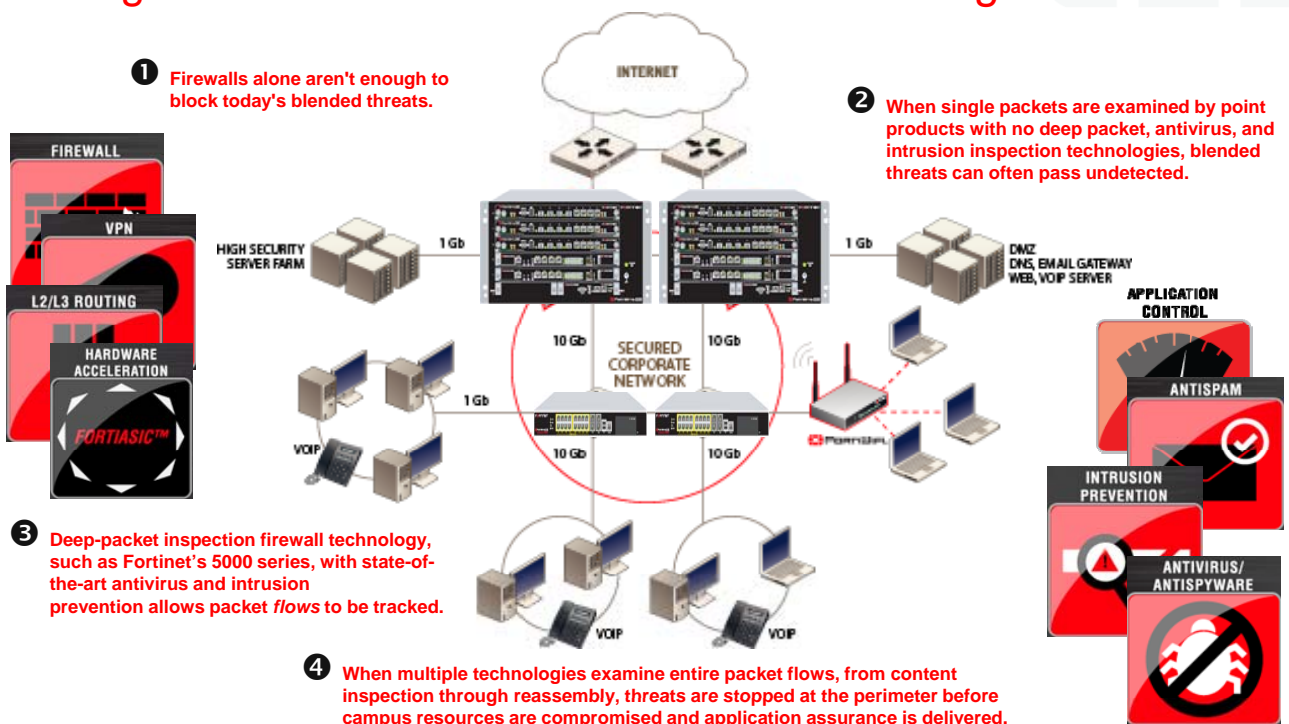
Fortinet Confidential

Real Time Network Protection

FORTINET

Campus Perimeter Security

Using Firewall + IPS + Antivirus + Web Filtering



Fortinet Confidential

Real Time Network Protection

FORTINET

Fortinet 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
 - 1,100+ employees / 500+ engineers
 - 400,000+ FortiGate devices shipped worldwide
- Strong, validated technologies and products
 - 24 patents; 85+ pending
 - Six ICSA certifications (Firewall, AV, IPS, IPSec VPN, SSL VPN, Anti-Spam)
 - Government Certifications (FIPS-2, Common Criteria EAL4+)
 - Virus Bulletin 100 approved (2005, 2006, 2007, 2008)



Fortinet Confidential

23

Real Time Network Protection



FORTINET FortiGuard Center fortiguardcenter.com

Threat Research and Response

Advisories & Reports

FortiGuard Services

Security Tools

Resource Library

Contact Us

APPLICATION CONTROL POPULARITY AND RISK LEVEL

Use the table below to narrow down the 1,000+ applications based on category, technology, popularity, potential risk level and date last released.

Results 1 - 20 of 1044 matching applications

Clear filters

Application Name	Category	Technology	Popularity	Risk	Date Last Released
100Bao	Peer-to-peer	peer-to-peer	Not Popular	High	2008-12-09
126.Mail	Web-based email	browser-based	Popular	High	2008-12-24
163.Alumni	Web	browser-based	Popular	Low	2008-12-16
163.BBS	Web	browser-based	Popular	Low	2009-02-13
18900.Com	Web	browser-based	Not Popular	High	2008-12-16
250.Eu	Internet Proxy	browser-based	Not Popular	Low	2008-12-24
2ch	Web	peer-to-peer	Not Popular	Low	2009-06-30
2ch.Posting	Web	peer-to-peer	Not Popular	Low	2009-06-30
360buy	Web	browser-based	Not Popular	High	2008-12-16
360quan	Web	browser-based	Not Popular	Low	2008-12-16
360safe.Update	System Update	client-server	Popular	Low	2009-01-22
3PC	Internet Protocol	network-protocol	Not Popular	Low	2009-01-13
4shared	Web	browser-based	Not Popular	Low	2008-12-10
51.Com	Web	browser-based	Popular	Low	2008-12-16

UPDATE CENTER

Application Control
Database Version » 2.659
Date Release Jul 02

THREAT LEVELS

Vulnerabilities: Normal

Virus/Spyware: Normal

Spam: Normal

FORTIGUARD SERVICES

Learn more about FortiGuard Security Subscription Services

- » Analysis & Management
- » Antispam
- » Antivirus
- » Application Control



Thank You.

What other vendor can generate this type of feedback!



-----Original Message-----

From: xxxxxxx@k12.sd.us [<mailto:xxxxxxx@k12.sd.us>]

Sent: Friday, September 14, 2008 6:30 AM

To: Info@AVFirewalls.com

Subject:

fortiguard is next to the *&\$(#\$% thing i have ever seen, or experienced...whoever created this stupid program seriously has no friends and hates fun...you suck