



Application Control & Security Consolidation

Rick Basile
Senior Systems Engineer



The Threats are Apparent

The New York Times

“Malicious cyberactivity is occurring on an unprecedented scale with extraordinary sophistication. Sensitive information is stolen daily from both government and private-sector networks, undermining confidence in our information systems, and in the very information these systems were intended to convey,” said Dennis C. Blair, the director of US national intelligence.

WIRED

Advanced Persistent Threat (APT) attackers also appear to be well-funded and well-organized...No one is immune to APT attackers, who have struck defense contractors and government agencies as well as private companies and law firms.

Goldman Sachs Employee Charged with Code Theft

NEW YORK -- The U.S. Justice Department arrested a former Goldman Sachs Inc. employee and charged him with stealing computer codes related to the firm's high-speed trading platform

Security Challenges

- Blended attacks
- Application-focused attacks
- “Oldies but Goodies” still exist
 - Nothing goes away. Ever.
- “Survival instinct” of applications much higher than before
 - Built-in evasion techniques
- Must assume malicious activity occurs within trusted applications

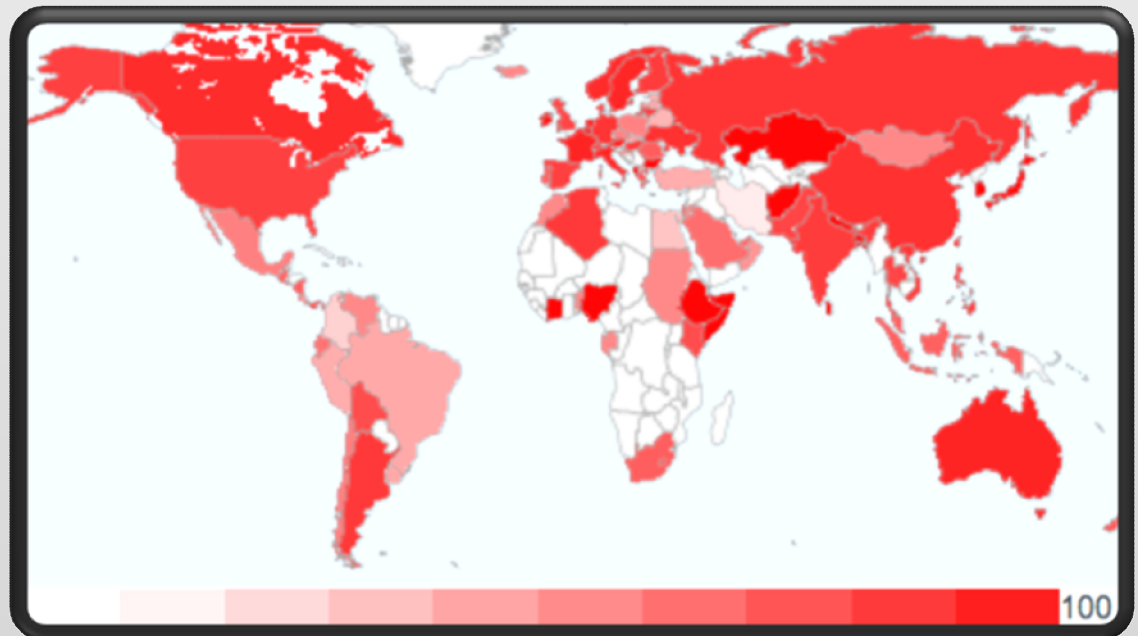


Unwanted Applications

- Well funded “freeware”
- Maintained by Dynamic Internet Technology Inc. (DIT)

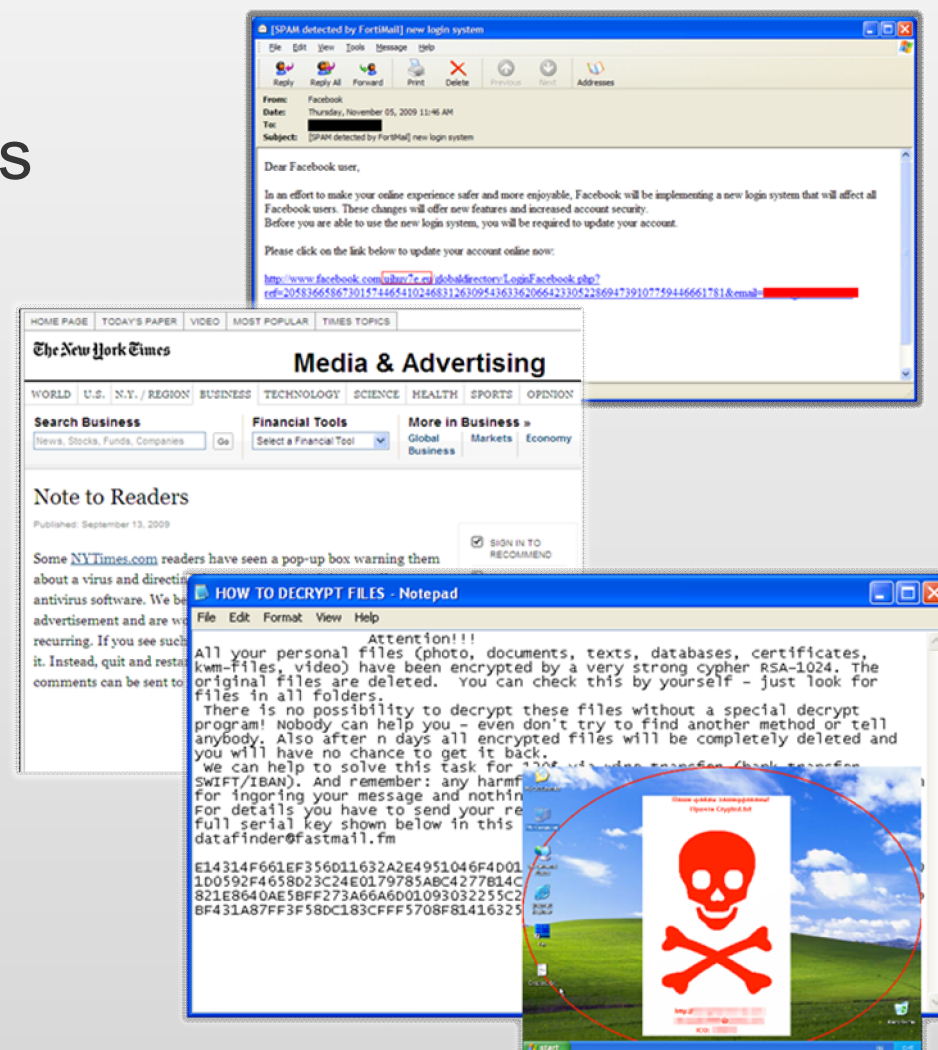


Name	Incident%
Freegate.Searching	44.79
Google.Web.Talk	10.34
HTTP.Video	3.66
HTTP.MS.ASF	3.63
Last.FM	3.55
EBay.Toolbar	3.51
NPR.Radio	3.39
YouTube.Download	3.37
Media.Player.Audio.HTTP	3.37
Dailymotion	3.33



Continued Concerns in the Security Landscape

- Phishing/Spear Phishing Attacks
 - ZEUS/ZBOT
- Legitimate Sites Compromised
 - FakeAV
- Ransomware
 - gpCode



Hiloti: the (Bot)Master of Disguise

- Click to Pay Model?
- Secure Payloads



Name	Incident%
Hiloti.Botnet	13.14
Mariposa	6.94
Pushdo	5.87
Waledac	3.31
Bredolab.Botnet	2.99
Waledac.Botnet	1.49
Danmec.Asprox.SQL.Injection	1.06
Torpig.Mebroot.Botnet	0.96
Bredolab	0.85
Koobface	0.74

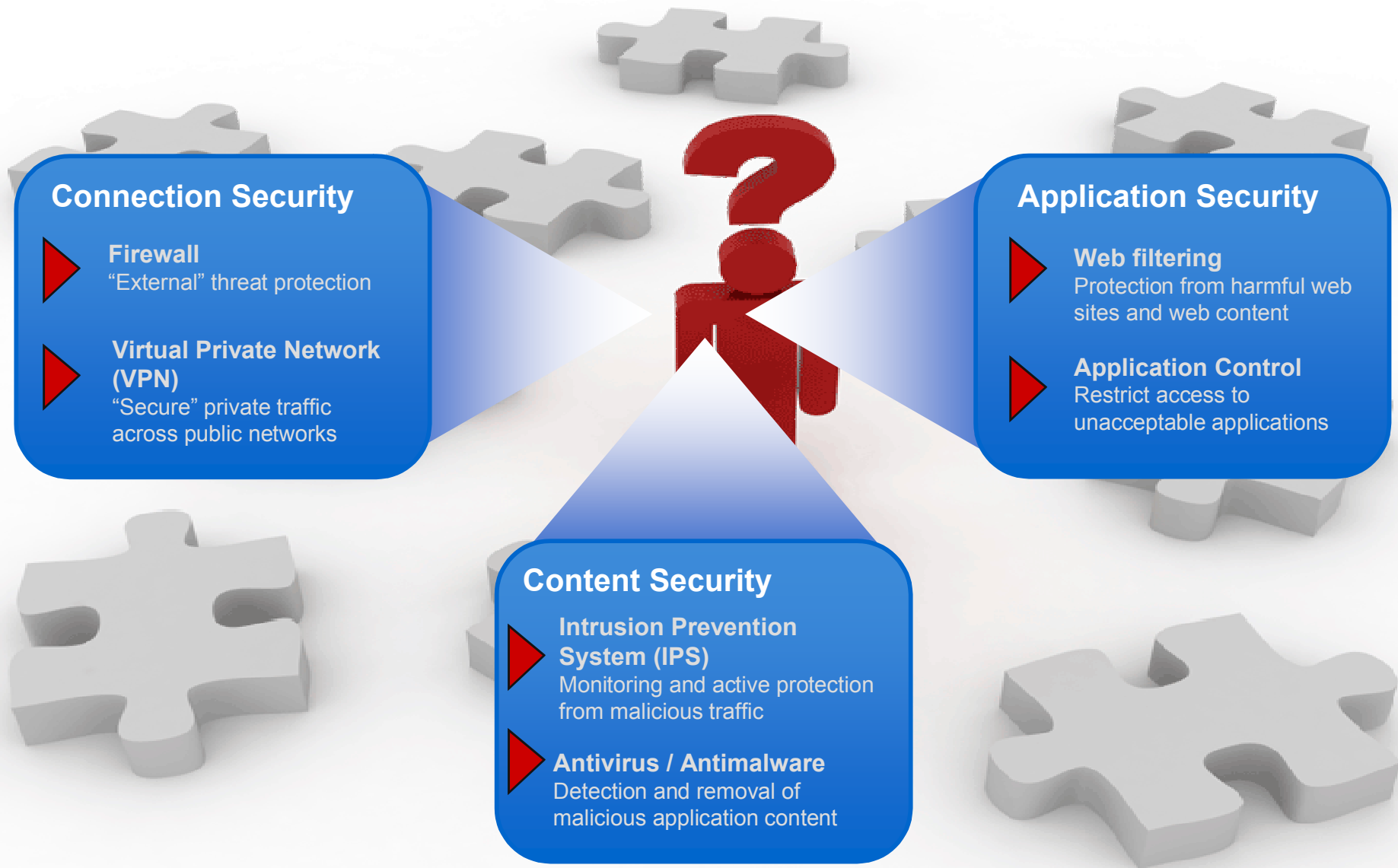


Advanced Persistent Threat

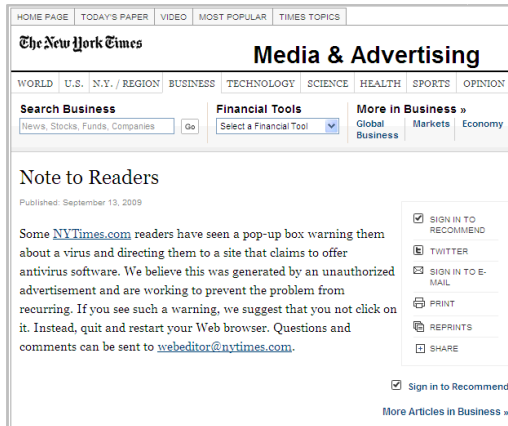
- Advanced
 - Threat that identifies the target before the access method
- Persistent
 - Tailored determined techniques based on the target or task
- Threat
 - Skilled, motivated, and well funded operators with specific objectives



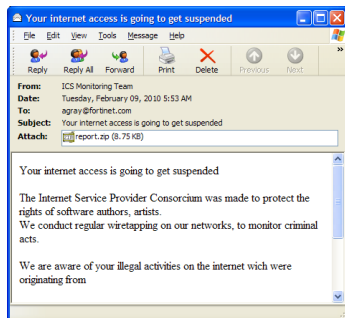
Navigating the Security Landscape



Complete Content Protection is Required

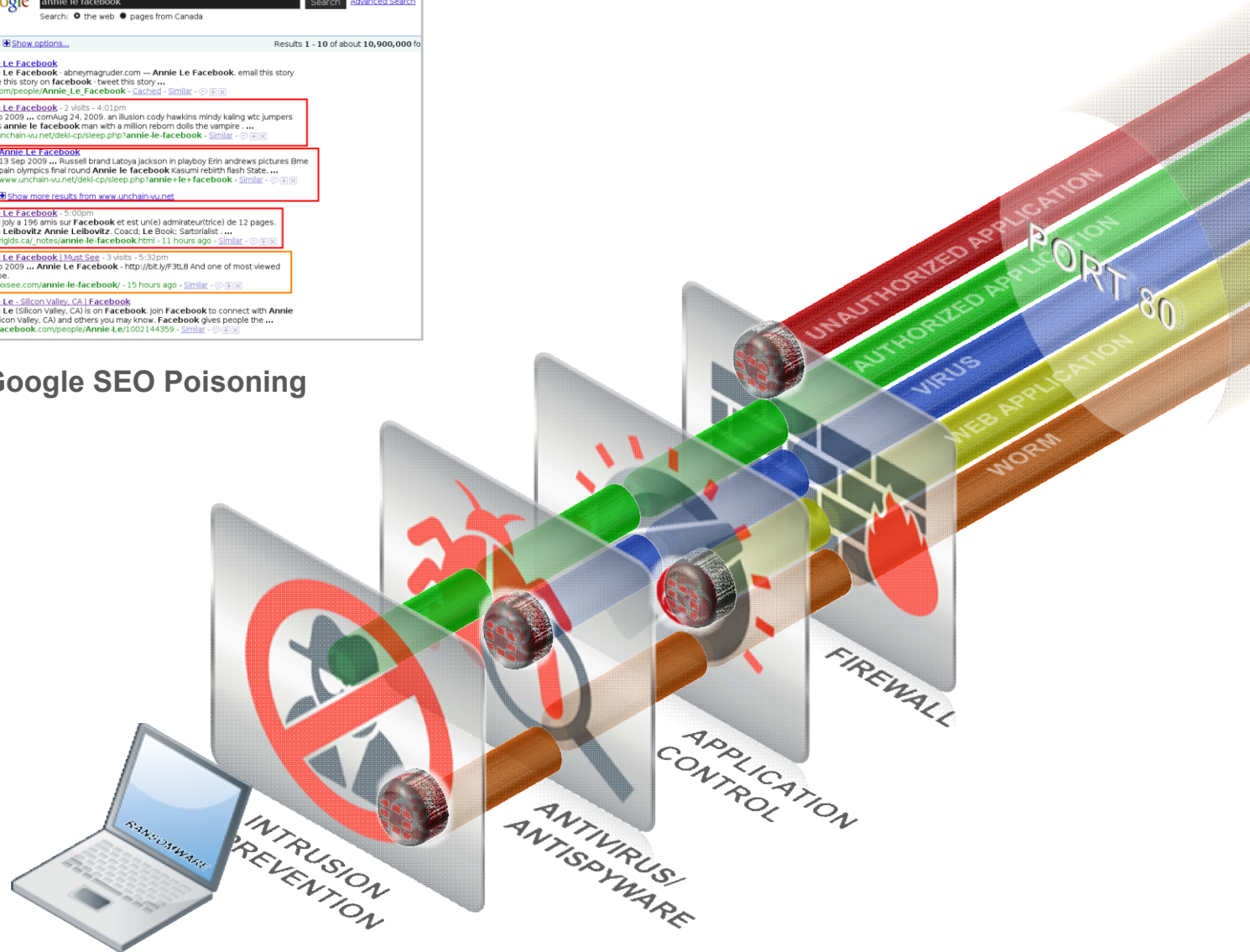


Malicious SWF Banner: NY Times



Countless spam campaigns

Google SEO Poisoning





What is Application Control?

Application Control:

- Identifying & enforcing security policy for applications, regardless of port or protocol used for communication

Objective:

- Flexibility and fine-grained policy control
- Increased security
- Deeper visibility into network traffic





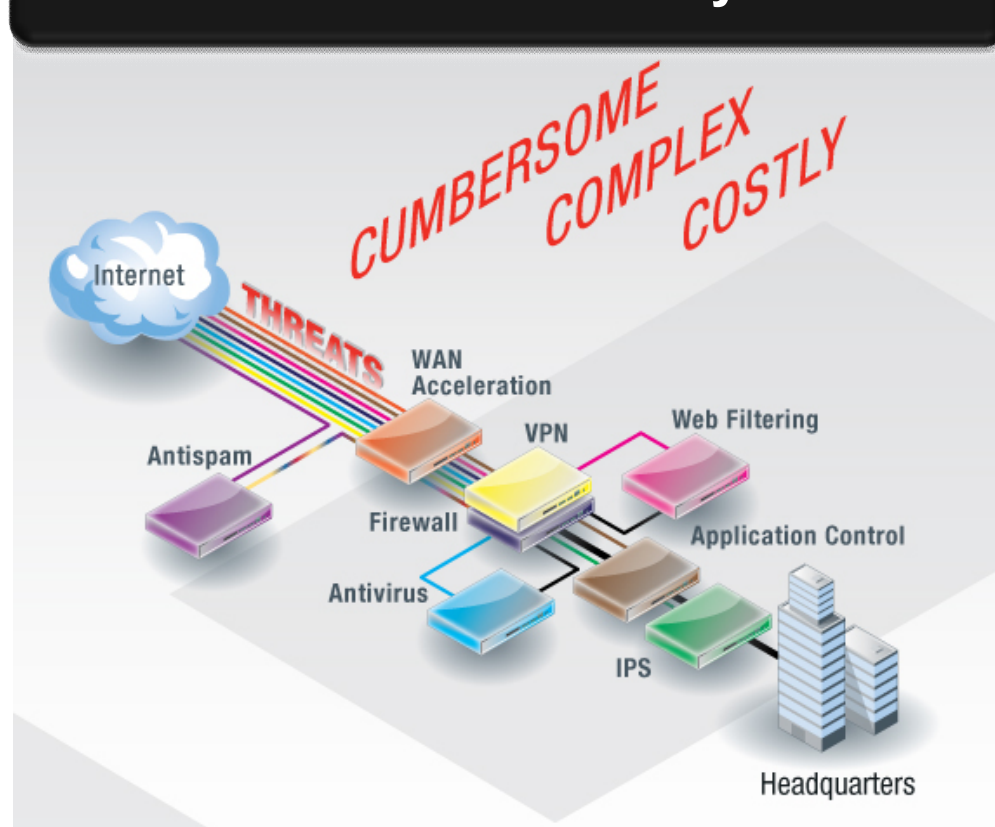
Today's Network Security Requires Application Detection, Monitoring, and Control

- Allowing access to Web 2.0 applications has made enforcing data security policies far more complex
 - User-created content embeds threats in content, pages, links, comments to blogs...
- Protection against effects of social media applications
 - Data loss
 - Threat propagation
 - Bandwidth consumption
 - Inappropriate use
- Endpoint to the Core
- “Single pane of glass” management for visibility & control

The Point Solution Syndrome

- Difficult to manage
 - Multiple management interfaces
 - No integration between vendors
 - No single vendor for issue resolution
- Expensive to deploy and maintain
 - Multiple vendor contracts
 - Costly support licensing
- Lack of integration
 - Leads to reduced security
- Performance challenges
 - Multiple inspection points
 - Software only solutions

Traditional Network Security Solutions



Consolidation is all Around Us

Just a few examples:

- Mobile Phones
- Companies
- Telecommunications / Video

And more importantly:

- Network Security

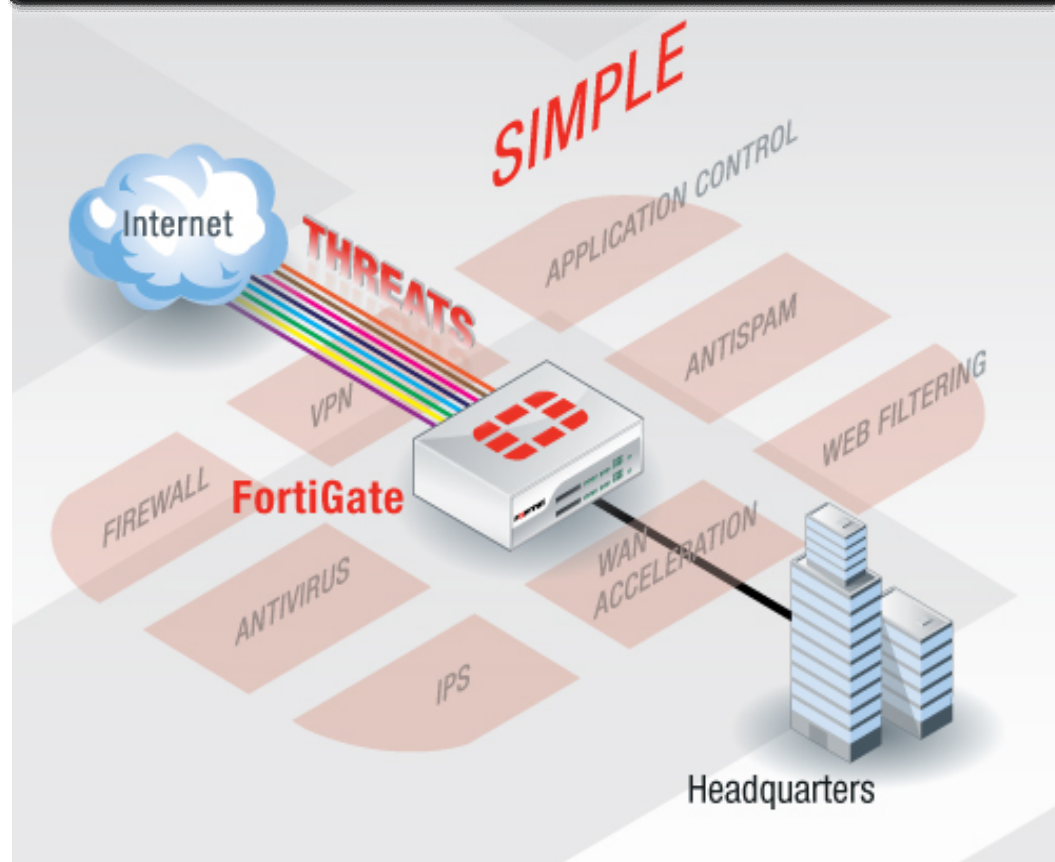


Consolidated Network Security



- Reduces number of vendors
- Provides comprehensive security
- Minimizes down-time
- Simplifies security management
- Coordinates security reporting
- Improves detection capabilities

The Fortinet Solution



Thinking Strategically

- Future-proof your security infrastructure
 - Anticipate change in threat scape & technology
- Look for opportunities to consolidate without compromise
 - Reduce complexity
 - Increase protection
 - Decrease risk
 - Lower CapEx and OpEx
- Move beyond tactical responses to threats



Thank You

