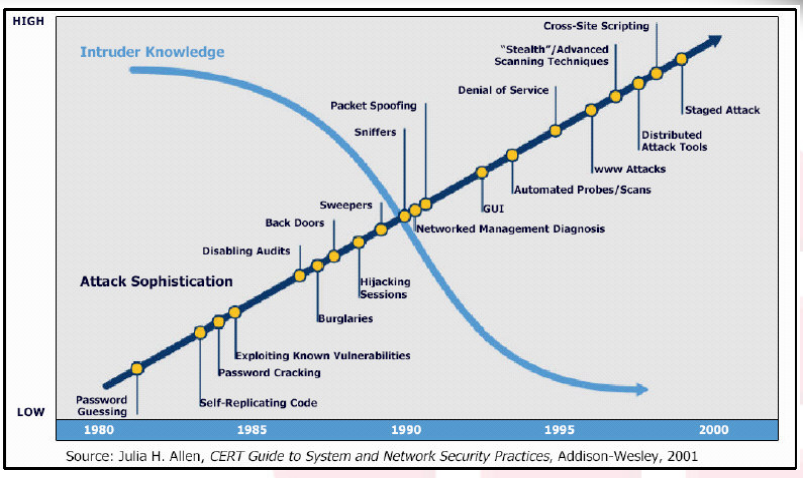
FORTINET

THE POWER IN NETWORK PROTECTION

Unified Threat Management

Benjamin Teh
Sales Director – Asia South

Increasing sophistication of threats



Source: Julia H. Allen, *CERT Guide to System and Network Security Practices*, Addison-Wesley, 2001

The elusive vulnerability window

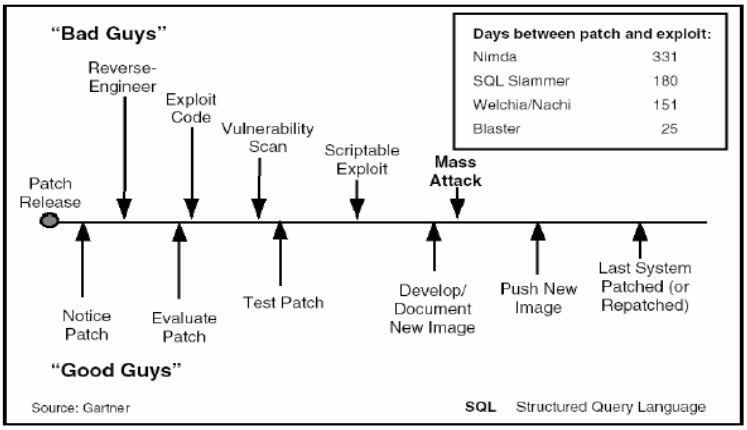
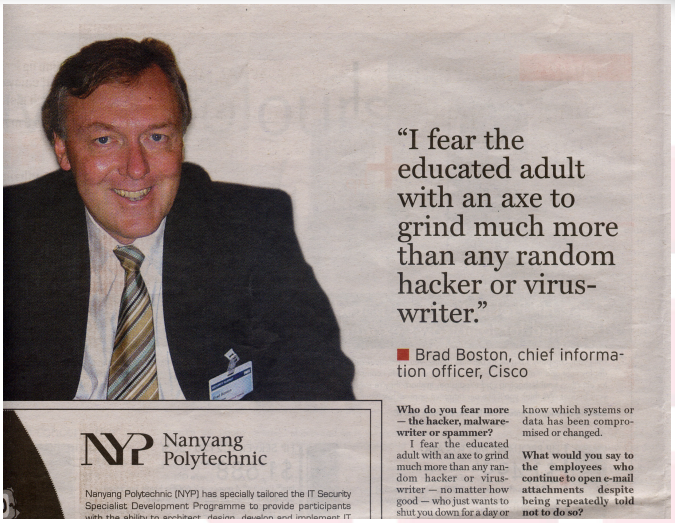


Figure 3: Gartner's Vulnerability Window

It Doesn't Take a Genius

- **"Mr. McKinnon is charged with the biggest military computer hack of all time"**
- **… crashing a network of 300 computers at the Earle Naval Weapons Station to be shut down for a week. It took a month to fully repair the damage …**
- **… cost of tracking and correcting the problems at about $1 million.**

Cisco and stolen code



NYP Nanyang Polytechnic

Nanyang Polytechnic (NYP) has specially tailored the IT Security Specialist Development Programme to provide participants

"I fear the educated adult with an axe to grind much more than any random hacker or virus-writer."

■ Brad Boston, chief information officer, Cisco

Who do you fear more — the hacker, malware-writer or spammer?

I fear the educated adult with an axe to grind much more than any random hacker or virus-writer — no matter how good — who just wants to shut you down for a day or know which systems or data has been compromised or changed.

What would you say to the employees who continue to open e-mail attachments despite being repeatedly told not to do so?

FORTINET

Home > Topics > Security > Opinions > **What Threat Is Posed by Stolen Cisco Code?**

Security

What Threat Is Posed by Stolen Cisco Code?

By Sean Gallagher
November 5, 2004

TALKBACK
Comment on this article
3 comments posted
Add your opinion

Opinion: The Source Code Club's offer to sell stolen source code for Cisco's PIX firewall might pose some security risks to Cisco's customers. But the real damage is more likely to be to Cisco's reputation and bottom line.

Once again, hackers are trying to sell what they purport to be the source code for Cisco's PIX firewall. But it isn't clear that there's any threat posed to customers by the code. In fact, the only people who might benefit from the code are Cisco's competitors.

RELATED LINKS
- E-gold Tracks Cisco Code Thief
- For Sale: Cisco Firewall Source Code
- Cisco Reports Multiple Security Problems

The **"Source Code Club" is offering to sell the PIX code** for $24,000. But it's not certain that anybody buying the code would be able to use it to find holes in the firewall software any more effectively than they could without it—unless they have significant software development and computing resources to examine the 37 MB of uncompiled code.

FORTINET

Fortinet's Goal

Become the dominant provider of security solutions -

EVERYWHERE

Core, edge, endpoint

IN TIME

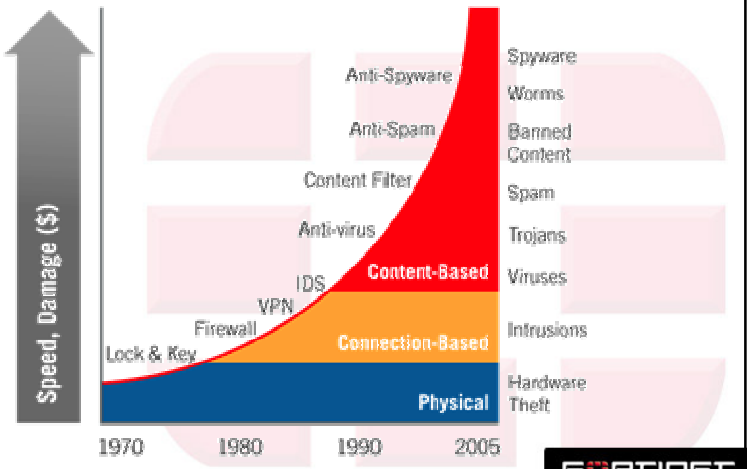
Real time performance

ALL THE TIME

Updates, services

The Nature of Threats Has Evolved…

A Multi-Layered Security Solution is Required



UTM Products Will Overtake Standalone VPN/Firewalls by 2008

"The UTM market is being created because it is quickly catching on with customers and vendors. UTM incorporates firewall, intrusion detection and prevention, and AV in one high-performance appliance." ***-- IDC, 2004***

Worldwide Threat Management Security Appliances Forecast, 2004-2008 ($M)

	2003	2004	2005	2006	2007	2008	2003 Share (%)	CAGR (%)	2008 Share (%)
Firewall/VPN	**$1,479.1**	**$1,667.7**	**$1,791.6**	**$1,804.4**	**$1,623.5**	**$1,462.3**	**93.4%**	**-0.2%**	**42.4%**
UTM Security Appliance	$104.9	$225.0	$517.5	$828.0	$1,324.8	$1,987.2	6.6%	80.1%	57.6%
Total TM Security Appliance	$1,584.0	$1,892.7	$ 2,309.1	$2,632.4	$2,948.3	$3,449.5		16.8%	

FORTINET

IDC UTM Leadership Over Point Solutions

"Fortinet, with the only ASIC based AV accelerated UTM appliances, led this UTM market in 2003, with $30.9 million in revenue and a 29.5% share of the worldwide market." ***-- IDC, 2004***

WW Unified Threat Management Appliance Revenue by Vendor, 2003 ($M)

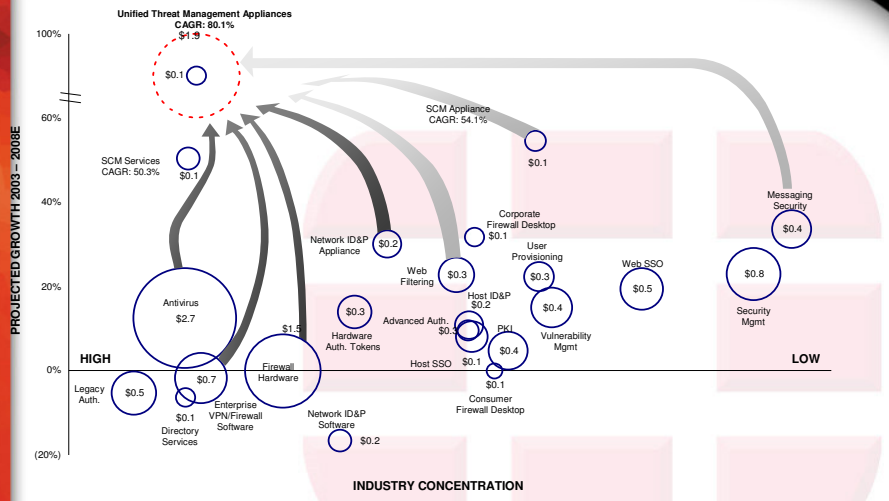
Vendor	Revenue	Units	Revenue Share	Average Vendor Revenue
Fortinet (#1)	30.9	21496	29.5%	$ 1,437.48
Symantec	24.0	13790	22.9%	$ 1,740.39
Secure Computing	22.8	5050	21.7%	$ 4514.81
ServGate	12.0	11743	11.4%	$ 1,021.89
Netscreen (acquired by Juniper)	5.2	6601	5.9%	$ 787.76
eSoft	4.0	3162	3.8%	$ 1,265.00
Pyramid Computer	1.3	509	1.2%	$ 2,554.03
Others	4.7	3680	4.5%	$ 1,227.12
Total	104.9	66031	100.0%	$ 1,588.84

Source: IDC, 2004

FORTINET

Network Security Market EcoSystem

Industry Moving Towards Appliances With Greater Functionality

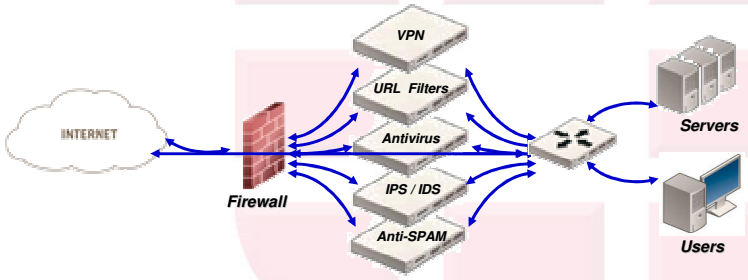


Note: Industry concentration values denote sectors where the top 3 vendors combined hold between 15% market share (low concentration) to 85% market share (high concentration). Security management market includes security information event management, patching and remediation, forensics, policy and compliance, security systems and configuration management.

Source: IDC and BAS estimates.

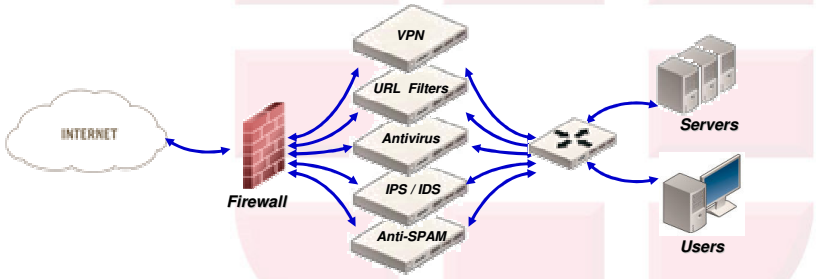
Multi-layered Security
- Approach to Complete Content Protection

- **Firewall**
  - Defend against intrusions
- **Antivirus Gateway**
  - Protect email from virus infection
- **IPS / IDS**
  - Protect against malicious attacks
- **Anti SPAM**
  - Reduce unwanted email
- **Web filters**
  - Eliminated unproductive web-browsing
- **VPN**
  - Delivering secure remote access



Multi-layered Security
- Approach to Complete Content Protection

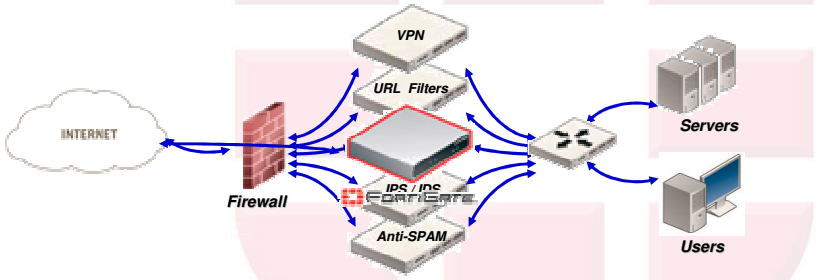
- **Advantage**
  - Provides comprehensive security approach
  - Minimizes down-time from individual threats
- **Disadvantage**
  - Requires multiple products
  - Increases network complexity and operational cost
  - Does not defend against "blended threats"



FORTINET

Multi-layered Security
- The Fortinet Approach

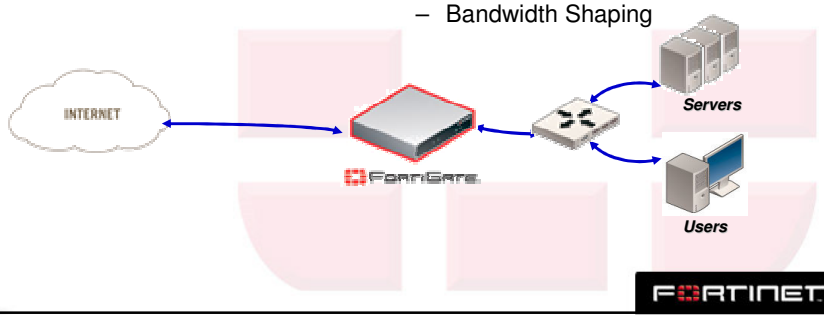
- **Advantage**
  - Provides comprehensive security approach
  - Minimizes down-time from individual threats
- **Disadvantage**
  - Requires multiple products
  - Increases network complexity and operational cost
  - Does not defend against "blended threats"



FORTINET

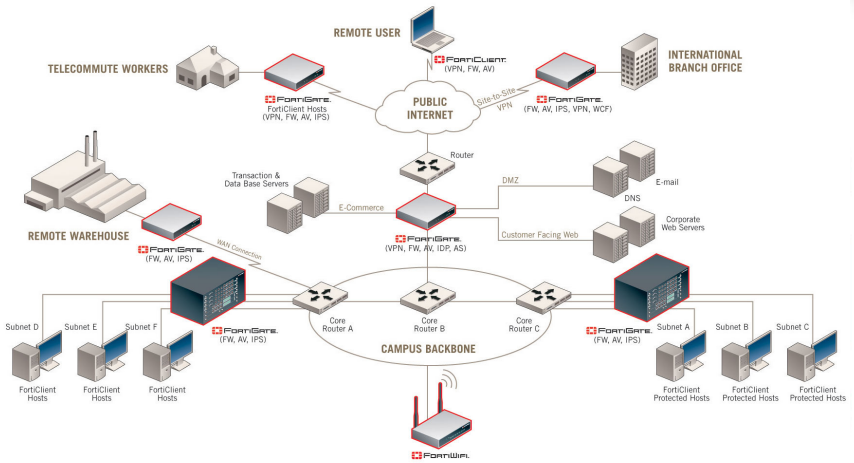
FortiGate
- A New Generation of Security Platform

- **Advantage**
  - Provides comprehensive security approach
  - Minimizes down-time from individual threats
- **FortiGate Unified Solution**
  - Firewall
  - Antivirus
  - IPS / IDS
  - URL filtering
  - Anti-SPAM
  - VPN
  - Bandwidth Shaping



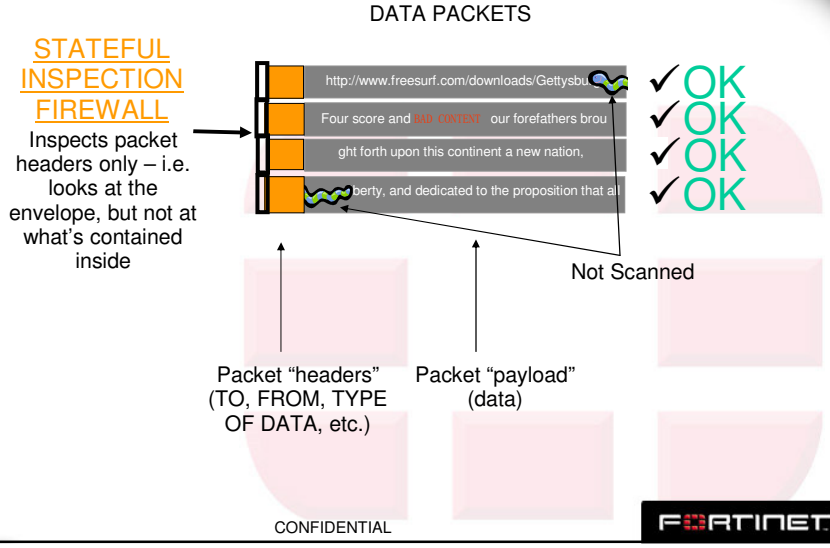
FORTINET

Fortinet Delivers UTM Solutions for the Enterprise



FORTINET

Stateful Inspection Firewalls Don't Analyze Payloads so they Miss Content Attacks



Deep Packet Inspection

DEEP PACKET INSPECTION

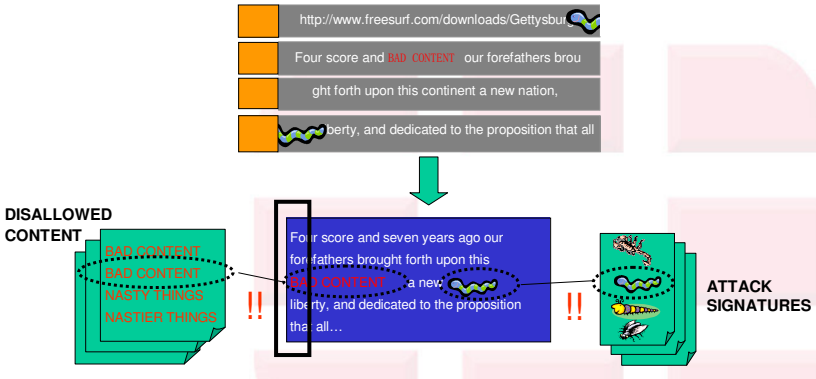
Performs a packet-by-packet inspection of contents
But can easily miss complex attacks that span multiple packets

- **Fragmentation can hide malicious content**
- **True security relies on multiple security layers**

Complete Content Inspection

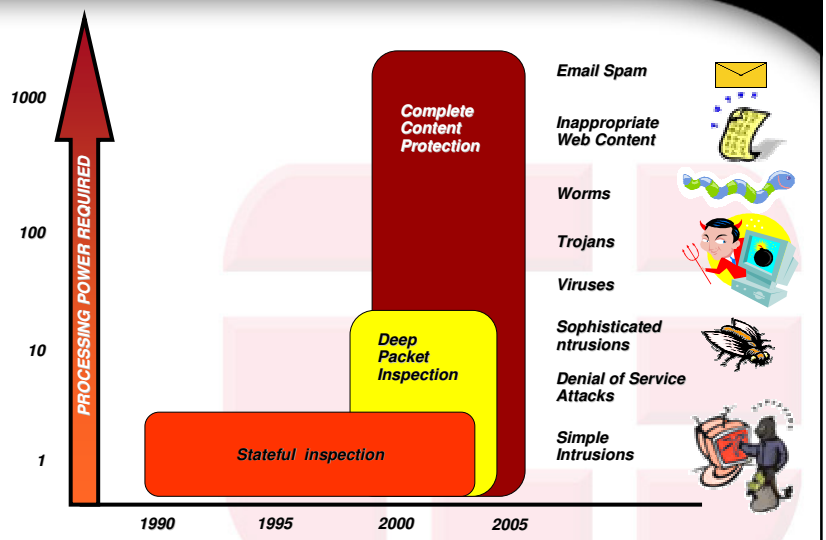
COMPLETE CONTENT PROTECTION

1. Reassemble packets into content



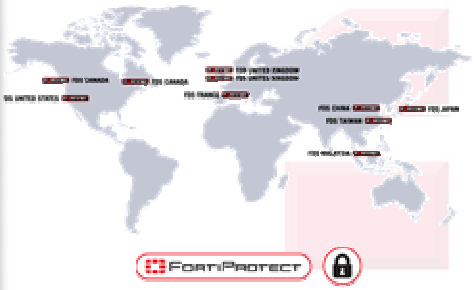
2. Compare against disallowed content and attack lists

Complete Content Protection Requires Enormous Processing Power

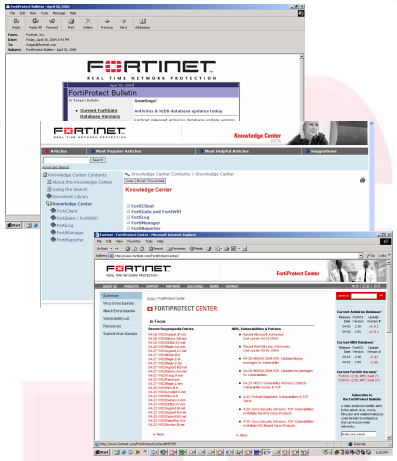


Global Infrastructure Ensures Rapid Response to New Threats

More than 10 Fortinet Threat Response Teams and FortiProtect Distribution Servers



FortiProtect Center Web Portal & email Bulletins



Automatic AV & IDP Updates Can Reach All FortiGate Units Worldwide in Under 5 Minutes

Sample FDN server updates

Measured in minutes from the Primary Server update

		FG Update Times							
		Primary Server	Secondary Server						
			Vancouver	US	Ottawa	France	UK	Japan	Shanghai	Tiangin
Week 10 (2005/03/14 09:00:00 - 2005/03/21 09:00:00)									
March 17, 2005	NIDS Version - 2.191	0	8	8	8	5	8	8	5	5
March 17, 2005	NIDS Version - 2.190	0	8	4	5	6	8	5	4	5
Week 10 (2005/03/07 09:00:00 - 2005/03/14 09:00:00)									
March 11, 2005	NIDS Version - 2.189	0	5	5	8	5	2	8	4	5
March 11, 2005	NIDS Version - 2.188	0	5	6	8	4	4	8	4	4
March 9, 2005	NIDS Version - 2.187	0	0	0	2	19	0	18	5	5
March 8, 2005	NIDS Version - 2.186	0	1	3	1	3	3	2	4	5

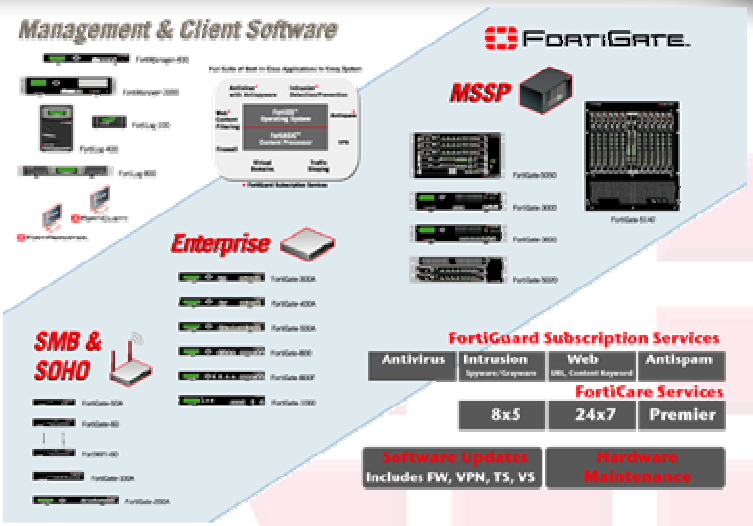
FORTINET

Random sampling of discovered viruses

W32/Fatso.A-net	Trend 3/7/05 6:18 AM	Sophos 3/7/05 6:47 AM	Fortinet 3/7/05 6:55 AM	Symantec 3/7/05 8:11 AM	McAfee 3/7/05 9:06 AM	Eprot 3/7/05 9:34 AM	Kaspersky
W32/Sober.M-mm	Eprot 3/7/05 9:34 AM	Sophos 3/7/05 10:57 AM	Fortinet 3/7/05 11:05 AM	Trend 3/7/05 12:08 PM	Symantec 3/7/05 5:21 PM	Kaspersky 3/8/05 5:20 AM	McAfee 3/8/05 9:26 AM
W32/Mitglieder.CB-tr	Kaspersky 2/28/05 7:26 PM	Fortinet 2/28/05 8:48 PM	Eprot 2/28/05 9:04 PM	Sophos 2/28/05 10:07 PM	Trend 3/1/05 4:22 AM	McAfee 3/1/05 4:46 AM	Symantec 3/1/05 8:21 AM
W32/Mydoom.BE-mm	Symantec 2/5/05 16:39	Sophos 2/20/05 20:47	Fortinet 2/21/05 0:02	Trend 2/21/05 1:40	Kaspersky 2/22/05 17:53	McAfee 2/23/05 8:17	Eprot 2/23/05 12:26
W32/Sober.K-mm	Eprot 2/20/05 23:06	Fortinet 2/21/05 0:02	Sophos 2/21/05 1:27	McAfee 2/21/05 4:27	Symantec 2/21/05 12:41	Kaspersky 2/22/05 17:53	Trend
W32/Mydoom.BD-mm	Eprot 2/18/05 16:25	Sophos 2/18/05 16:37	McAfee 2/18/05 16:37	Fortinet 2/18/05 13:19	Trend 2/18/05 19:49	Symantec 2/18/05 21:50	
W32/MyDoom.BB-mm	Sophos 2/16/05 14:56	Trend 2/16/05 16:29	Eprot 2/16/05 16:45	Fortinet 2/15/05 17:19	McAfee 2/16/05 20:27	Symantec 2/17/05 3:30	
W32/MyDoom.BA-mm	McAfee 1/20/05 11:45	Trend 1/28/05 0:47	Fortinet 2/8/05 16:58	Symantec 2/10/05 5:40			
W32/Bropia.G-net	Symantec 2/7/05 11:19	Trend 2/7/05 2:08	Fortinet 2/7/05 20:32	McAfee 2/8/05 9:36			
W32/Bropia.F-net	Fortinet 2/2/05 21:30	Sophos 2/3/05 7:25	Eprot 2/3/05 9:54	McAfee 2/3/05 11:06			
W32/ForBot.SQL-net	Symantec 1/26/05 16:28	Fortinet 1/27/05 19:35	Trend 1/28/05 0:47	Sophos 1/28/05 1:25			
W32/Sagle.BL-mm	Sophos 1/6/05 0:37	Eprot 1/27/05 11:34	Fortinet 1/27/05 12:13	Symantec 1/27/05 16:01	Trend 1/27/05 16:07		
W32/Sagle.BK-mm	Sophos 1/6/05 0:37	Kaspersky 1/26/05 20:05	Fortinet 1/26/05 21:15	Trend 1/27/05 1:17	Symantec 1/27/05 1:38	McAfee 1/27/05 1:45	Eprot 1/27/05 8:25
W32/Sagle.BJ-mm	Sophos 1/6/05 0:37	Kaspersky 1/26/05 13:04	Eprot 1/26/05 14:04	Trend 1/26/05 14:07	Fortinet 1/26/05 14:50	Symantec 1/26/05 16:28	McAfee 1/27/05 1:45

FORTINET

Fortinet Differentiators
- Products, Technology, Service & Support



And Lowest Total Cost of Ownership

FORTINET

Fortinet Company Overview

- Founded October, 2000
  - Founder, former Pres. & CEO of NetScreen (NASDAQ: NSCN)
- 600 employees; HQ in Sunnyvale, CA
- Offices throughout Americas, EMEA and Asia
  - Belgium, France, Germany, Italy, Sweden, UK
  - Tokyo, Seoul, Beijing, Shanghai, Hong Kong, Taipei, Singapore, KL, etc.
- Creators of world's only ASIC-powered antivirus systems
  - Addressing the need for real-time network protection
  - More than 80,000 FortiGate units shipped to 2,000 customers
- Achieved >10x revenue growth in 2003 vs. 2002
  - Among the fastest growing network security companies in history
- Completed $50 million mezzanine financing Feb 2004
  - Total equity raised $93 million

FORTINET


questions
THE POWER IN NETWORK PROTECTION
Thank You