Proč a jak splnit literu kybernetického zákona

Ondrej Stahlavsky

Regional Director, CEE

High Performance Network Security

PROBLEM: GROWING ATTACK SURFACE

PROBLEM: GROWING ATTACK VECTORS

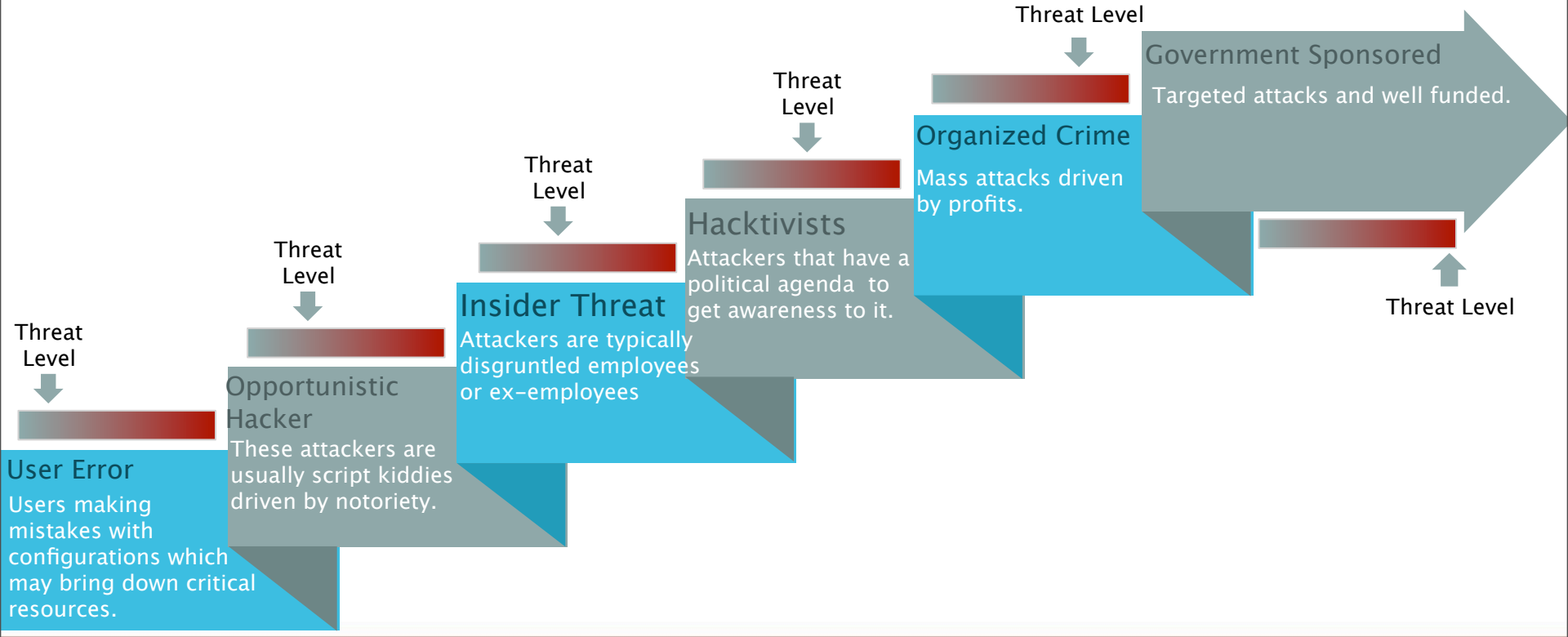
An Extensive, Poisoned, Dark, Deep Web

PROBLEM: GROWING ATTACK VECTORS

An Extensive, Poisoned, Dark, Deep Web

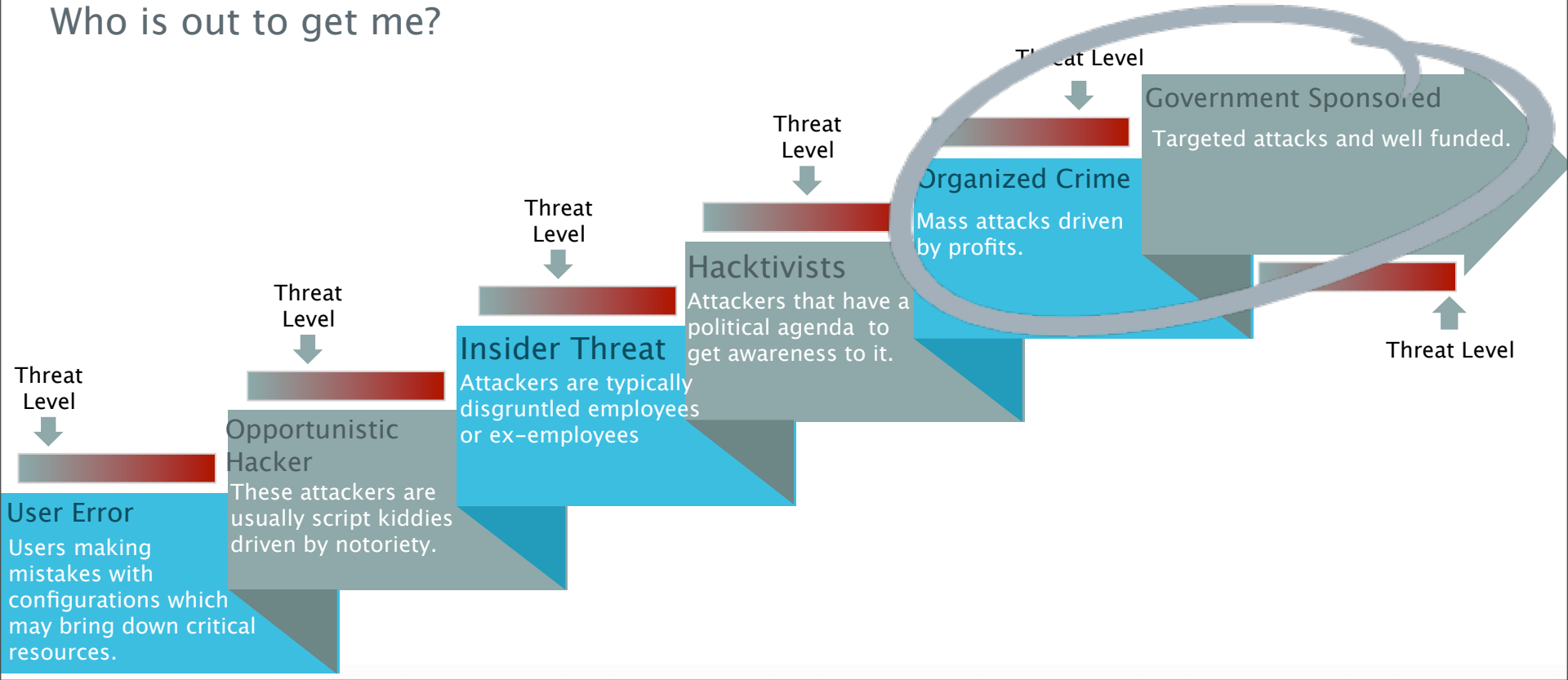
THREAT ADVERSARIES

Who is out to get me?



THREAT ADVERSARIES

Who is out to get me?



STATE SPONSORED ATTACKS - HAVEX

- What is Havex?
  - Rat (‘Remote Administration Tool’)
  - Harvests information on hardware control systems (SCADA)
  - First since Stuxnet

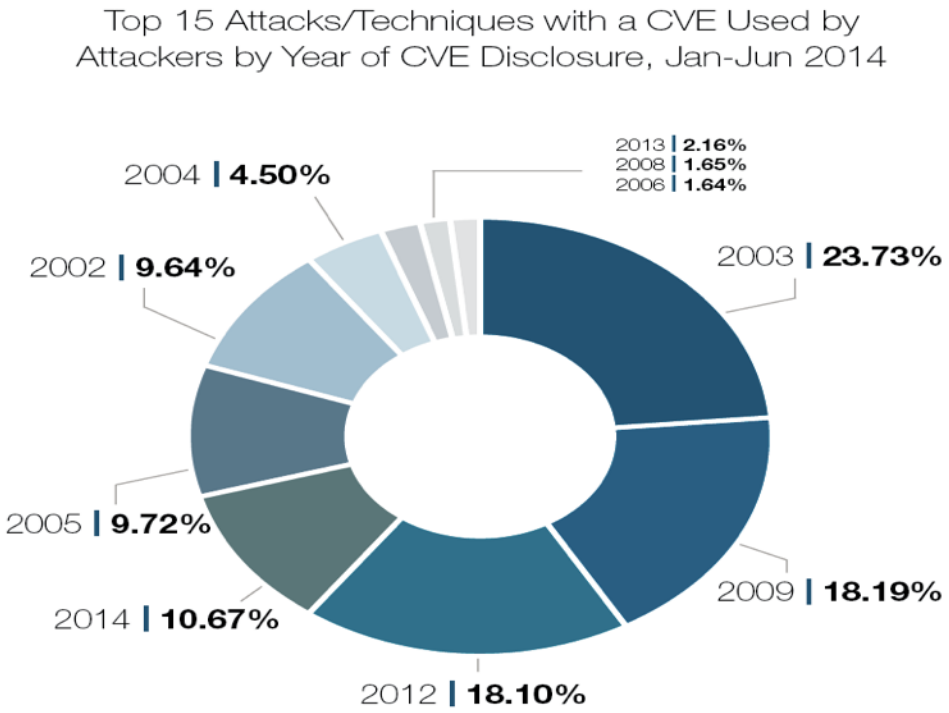
‘BLASTWARE’ BEWARE

Destructive Malware in the wild

- Disk Wipers
  - Overwrite hard-drive and MBR
  - South Korea, March 2013
    - ‘Dark Seoul’
      - 3 banks, 2 media companies
      - 50,000 systems
- Ransomware
  - Encrypts data
  - Leaves hard drive intact
  - Forensics unhampered

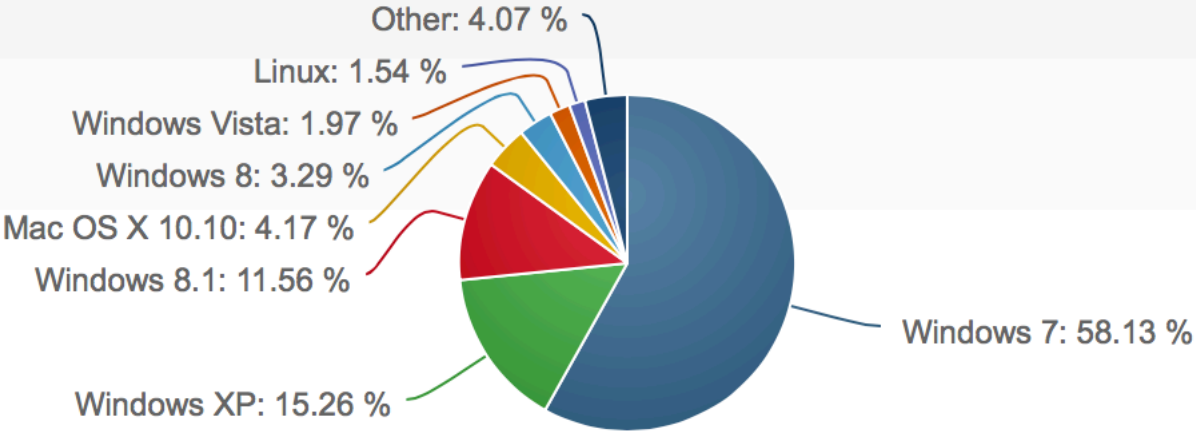
- 2014 FortiGuard Labs discovery: DorkBot
  - Erases hard drive if analysis is detected
  - New variations likely to destroy other targets

THE HUMAN FACTOR - LAZINESS



“Old Habits Die Hard”

OPERATING SYSTEMS AND SOFTWARE REQUIRE



*www.netmarketshare.com September 2015

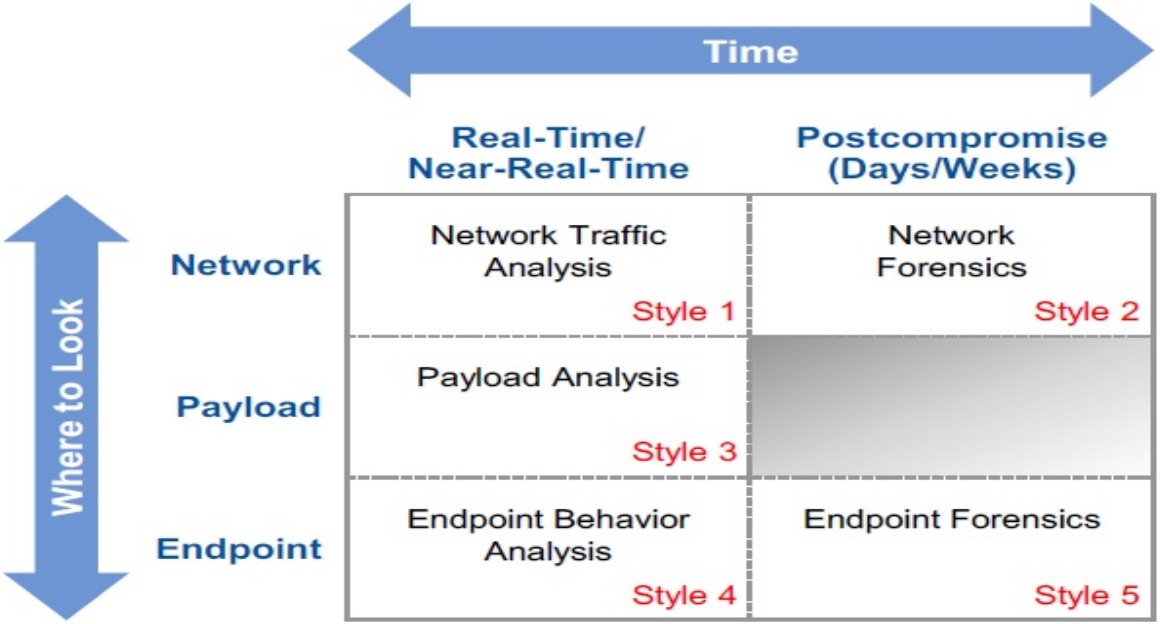
CZECH COMPANIES SIMILARLY EXPOSED...

What is the average number of all detected IT security incidents in your company in the Czech Republic during the year?

Source: IDC, 2014

APPROACH TO ADDRESS THREATS

Figure 1. Five Styles of Advanced Threat Defense

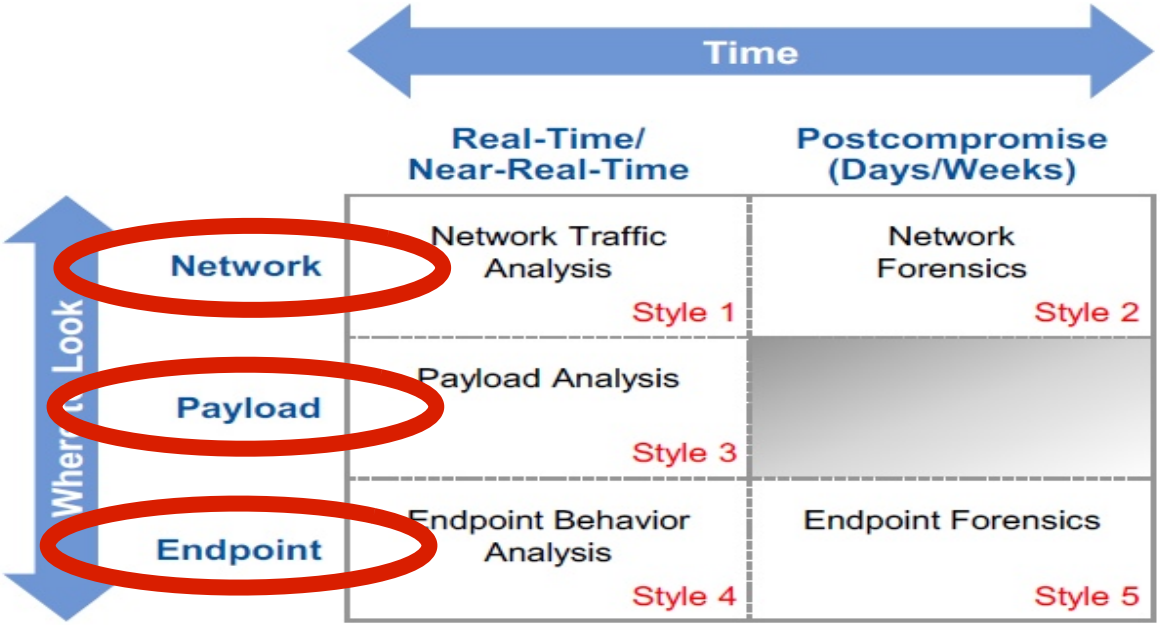


Source: Gartner (August 2013)

http://www.networkworld.com/news/2013/103013-gartner-defense-attacks-275438.html?page=2

APPROACH TO ADDRESS THREATS

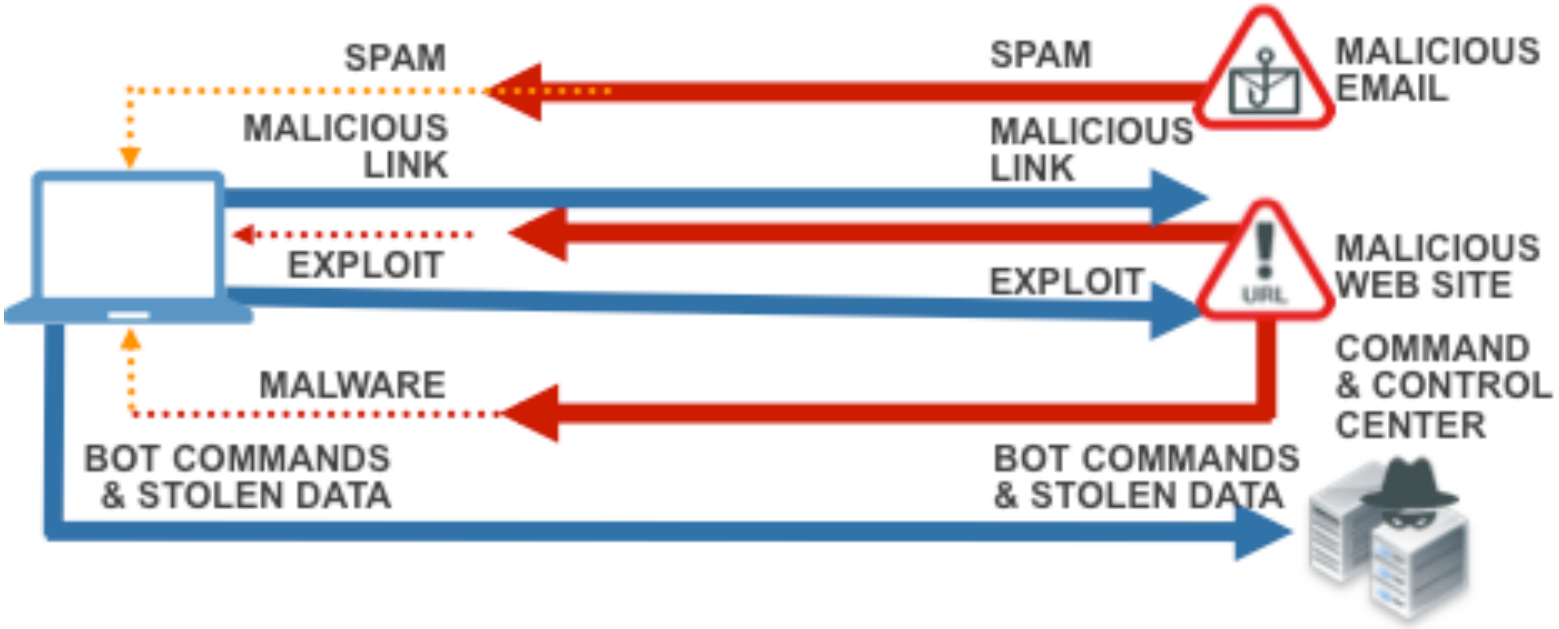
Figure 1. Five Styles of Advanced Threat Defense



Source: Gartner (August 2013)

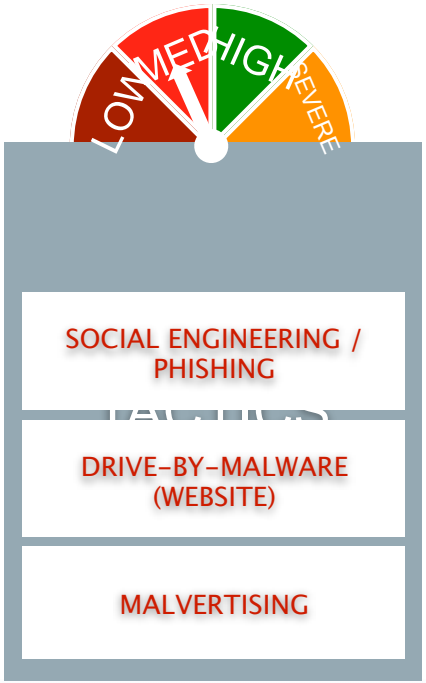
http://www.networkworld.com/news/2013/103013-gartner-defense-attacks-275438.html?page=2

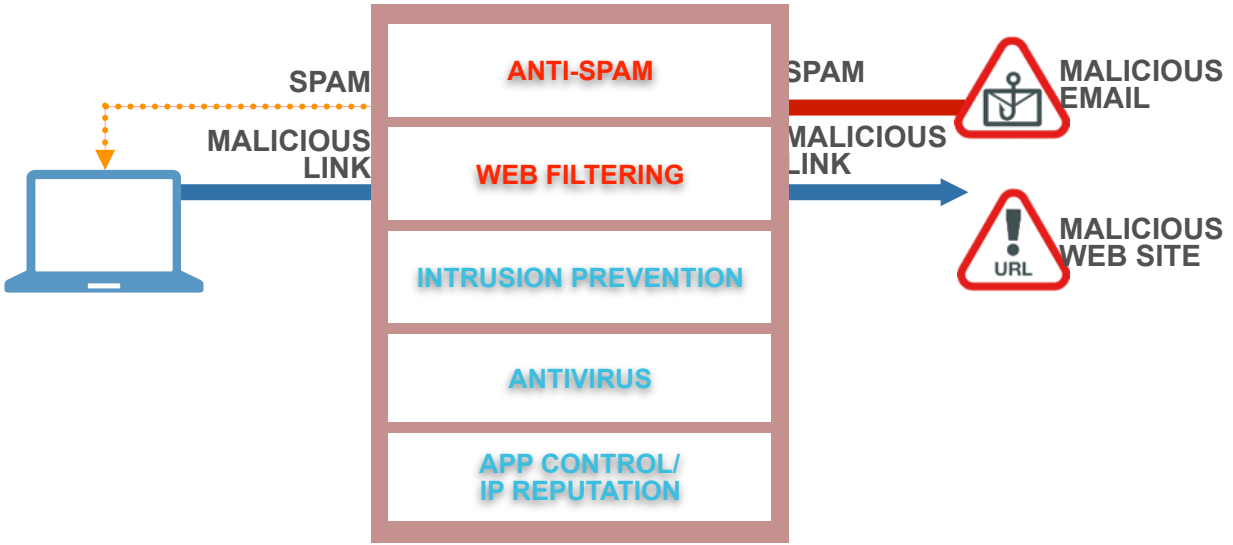
ATTACK ANATOMY



DELIVERY

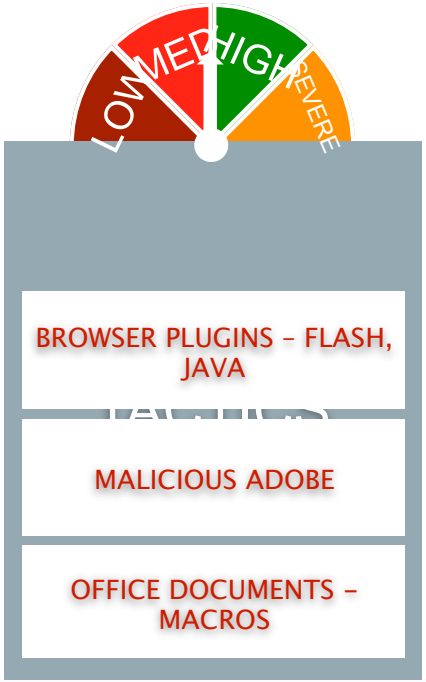
Goal: Choose the best delivery mechanism as possible to deliver the exploit.

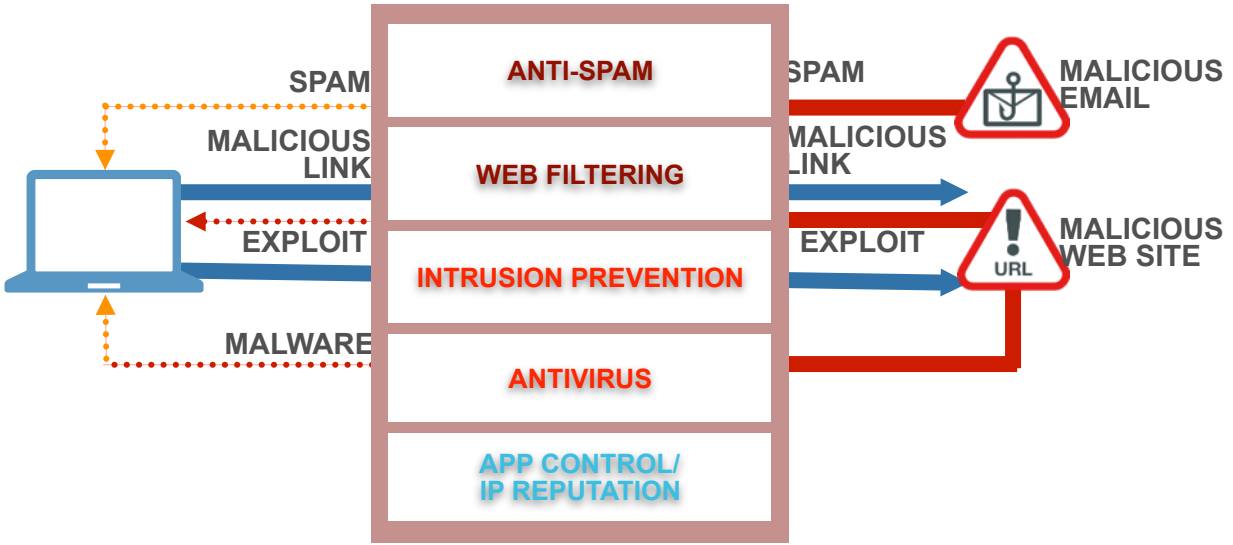




EXPLOITATION

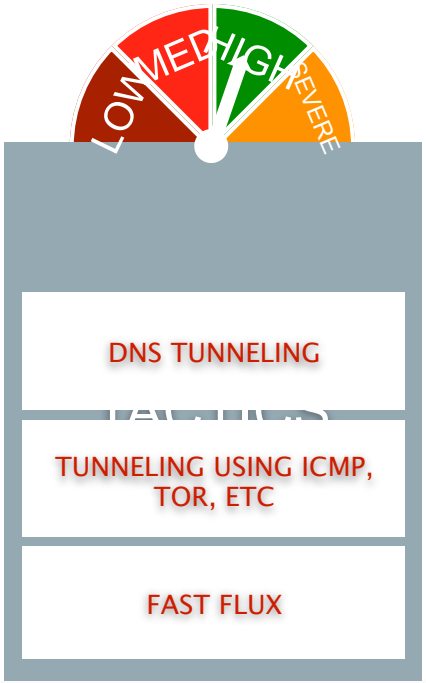
Goal: Successful, stable exploitation of the system without being detected.

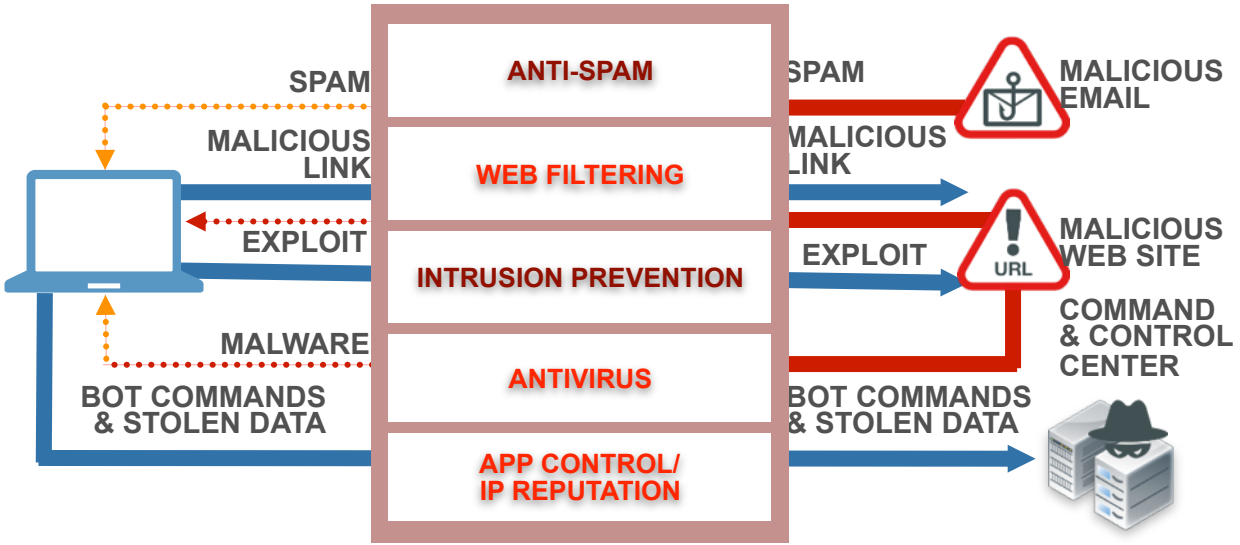




COMMAND AND CONTROL

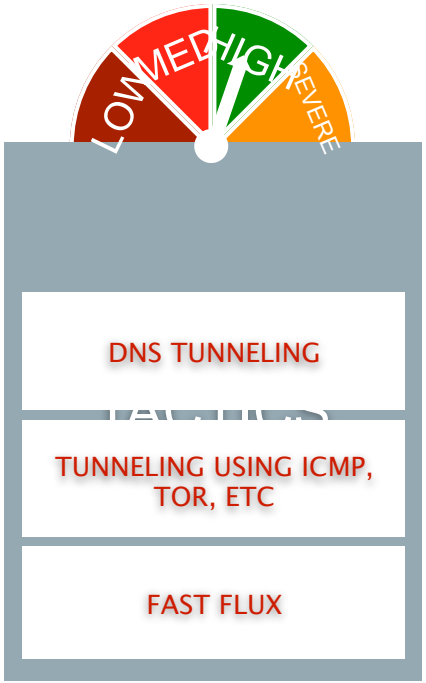
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

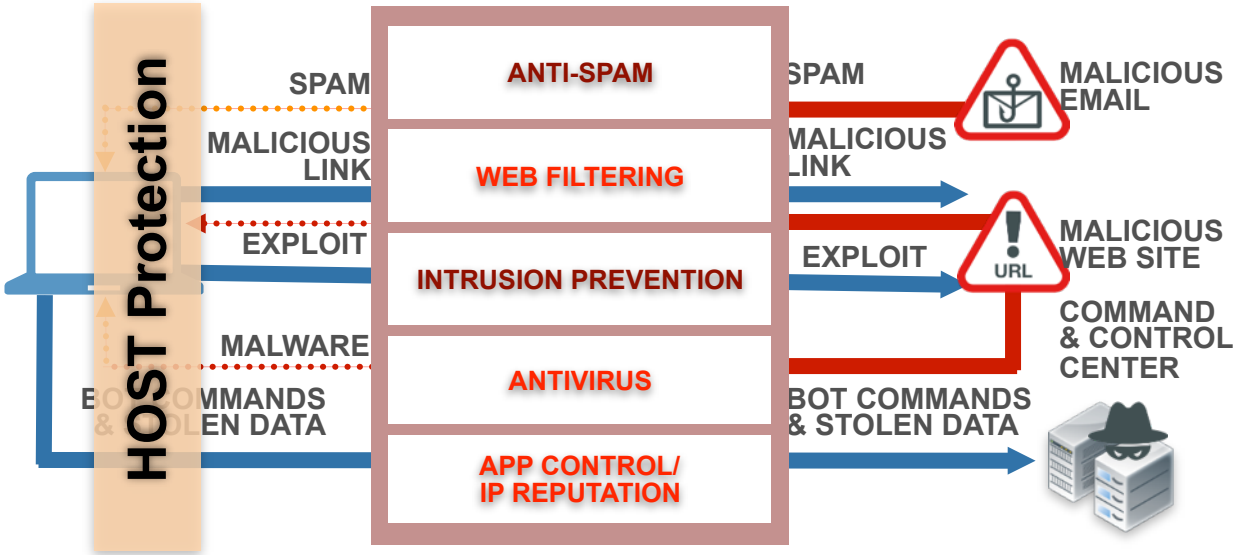




COMMAND AND CONTROL

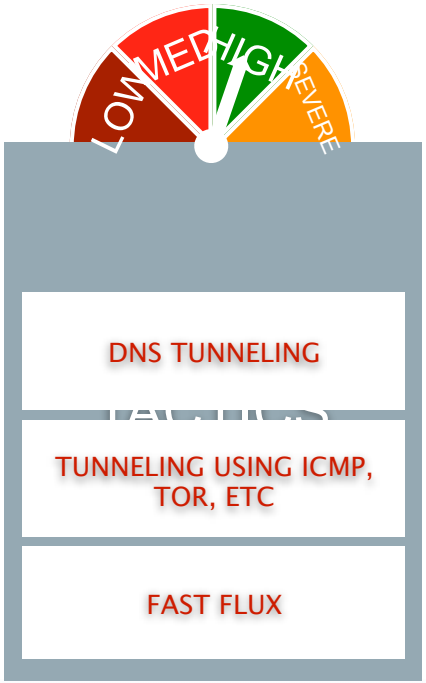
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

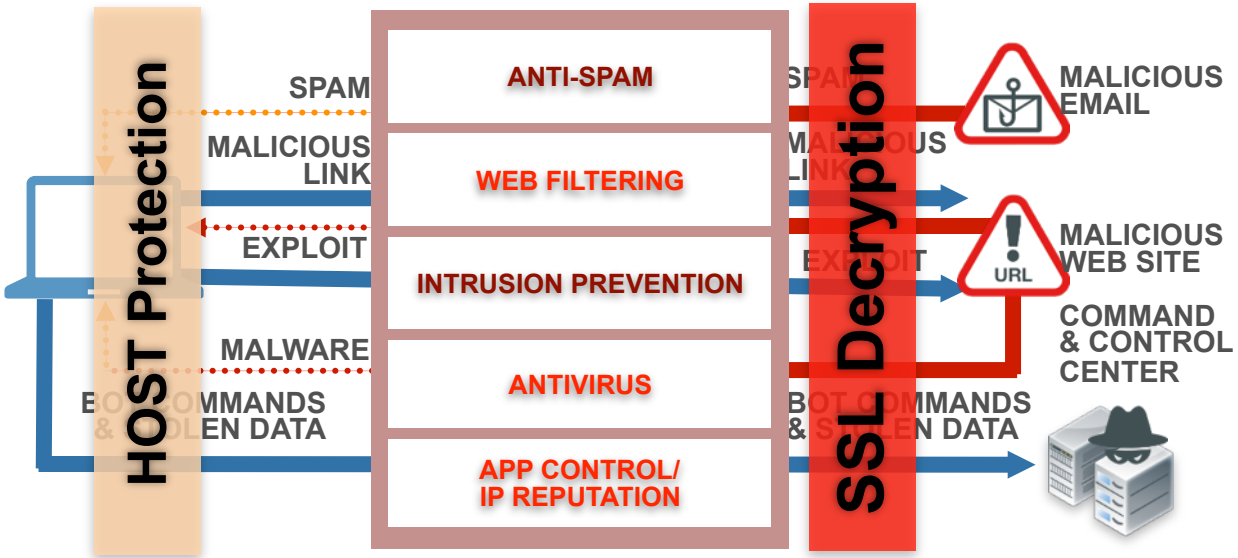




COMMAND AND CONTROL

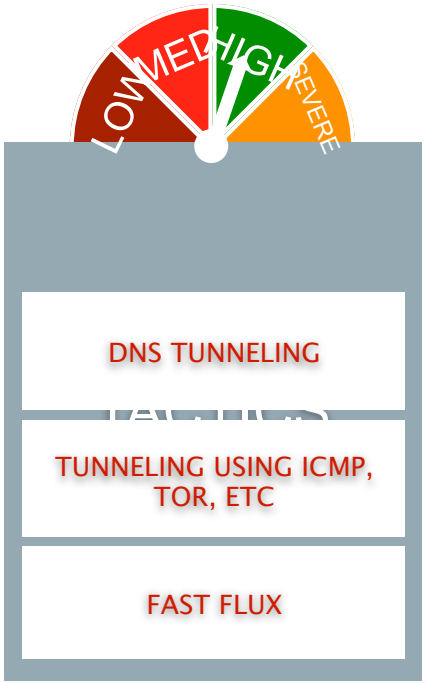
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

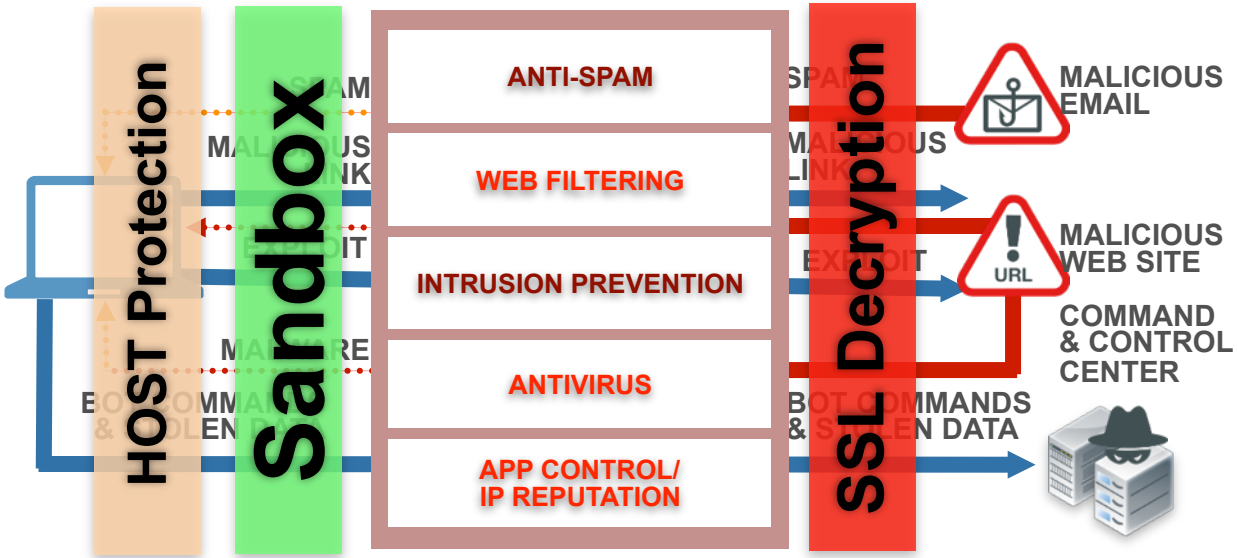




COMMAND AND CONTROL

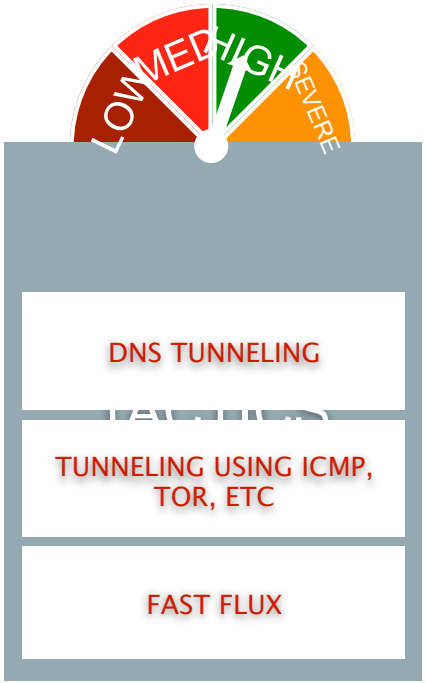
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

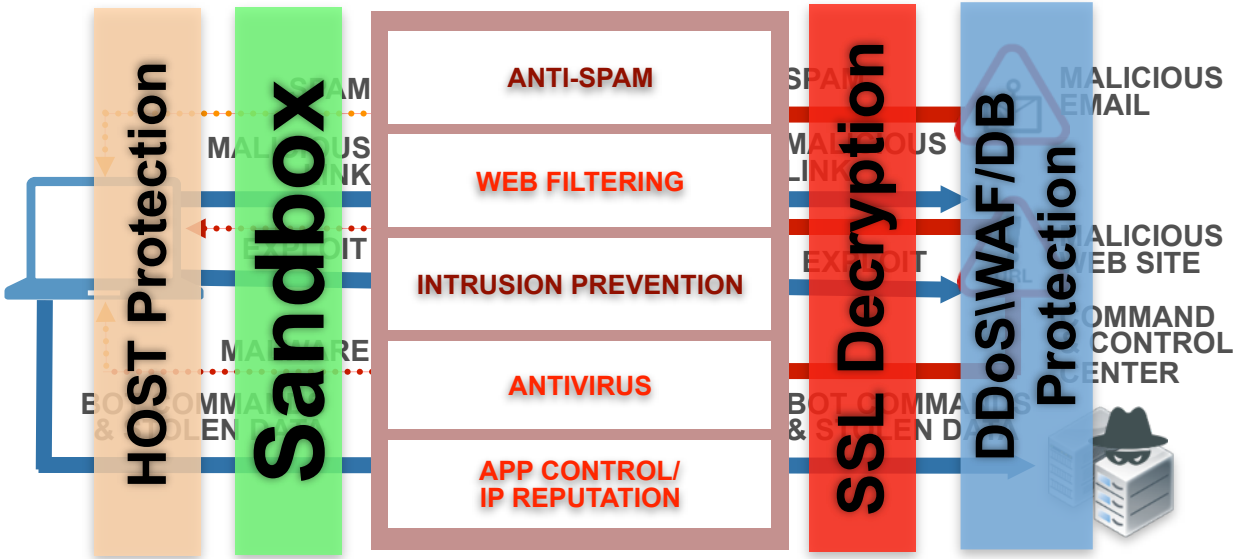




COMMAND AND CONTROL

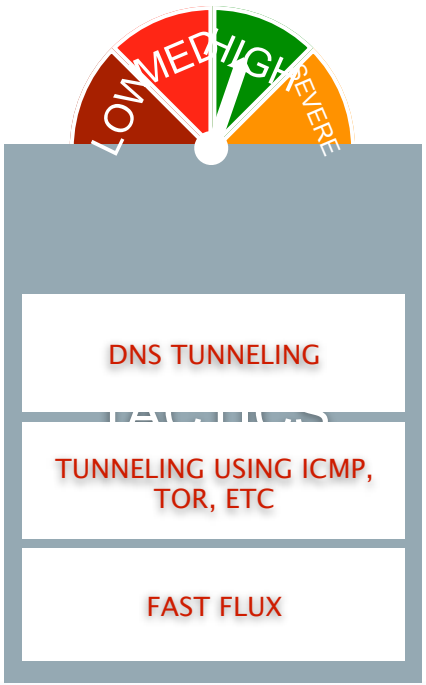
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

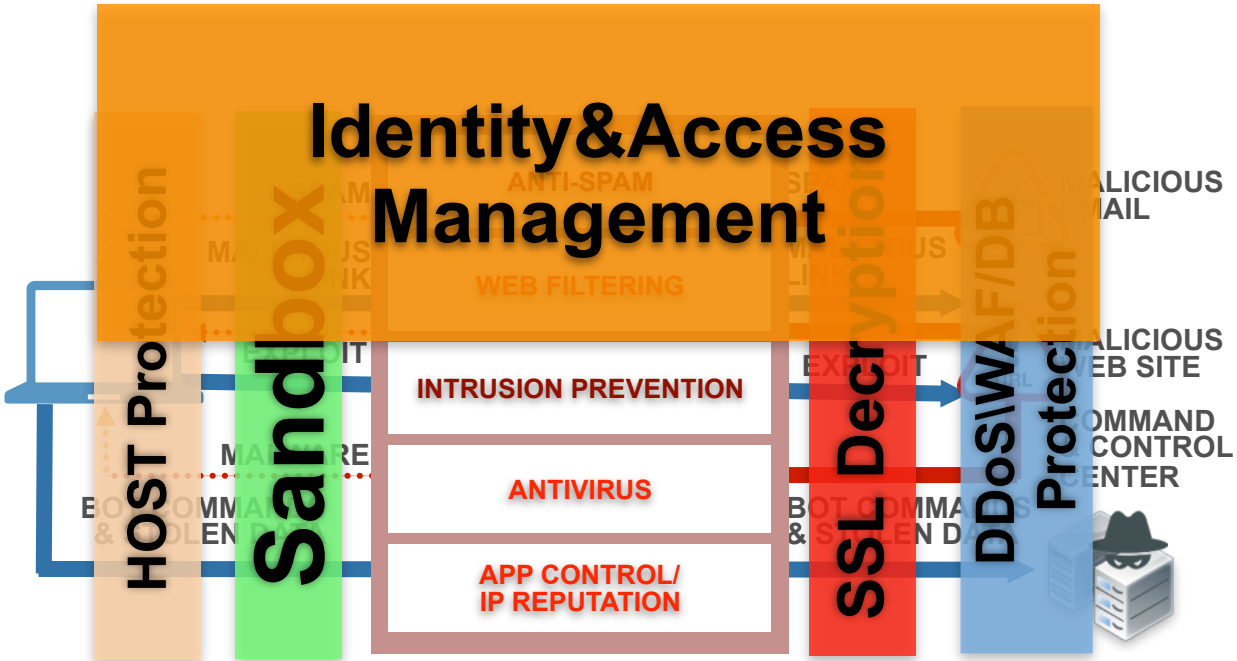




COMMAND AND CONTROL

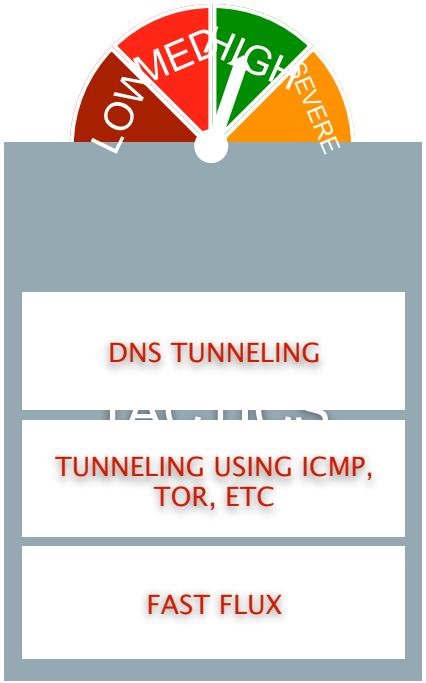
Goal: Communicate undetected back to malicious infrastructure to and download other tools.

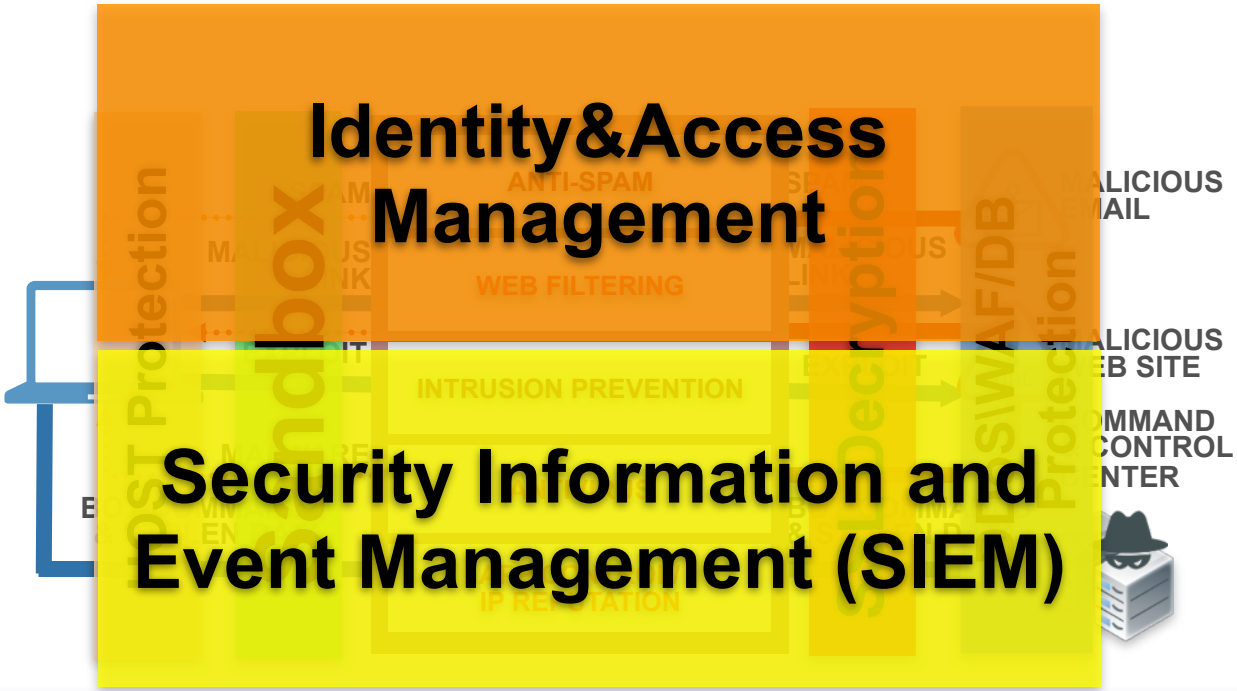




COMMAND AND CONTROL

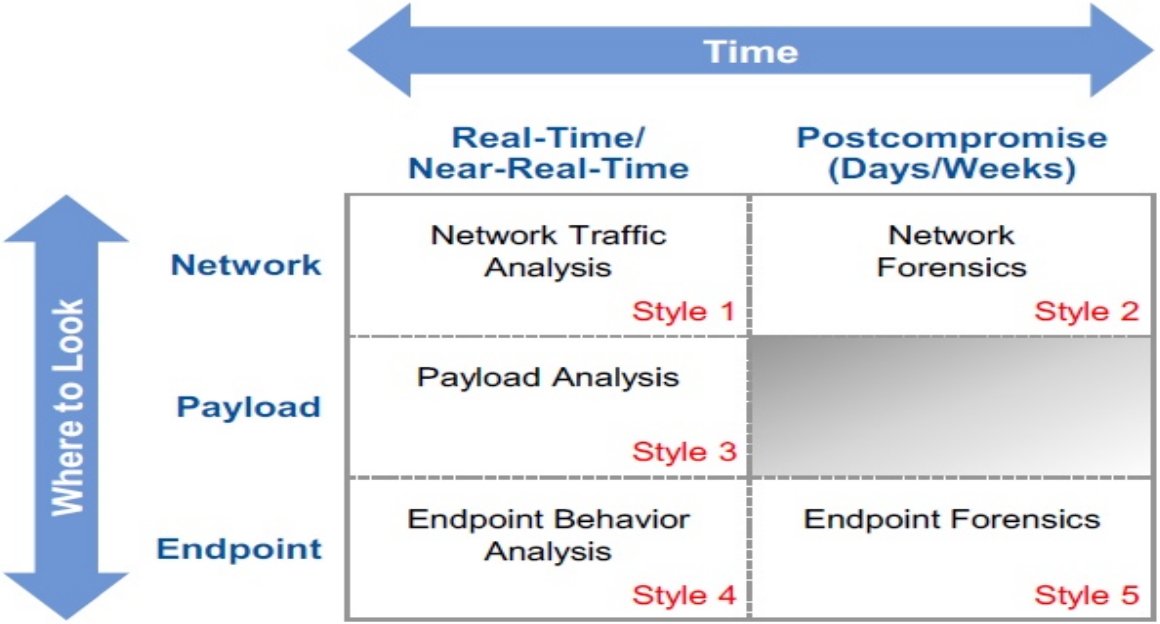
Goal: Communicate undetected back to malicious infrastructure to and download other tools.





POSTCOMPROMISE

Figure 1. Five Styles of Advanced Threat Defense

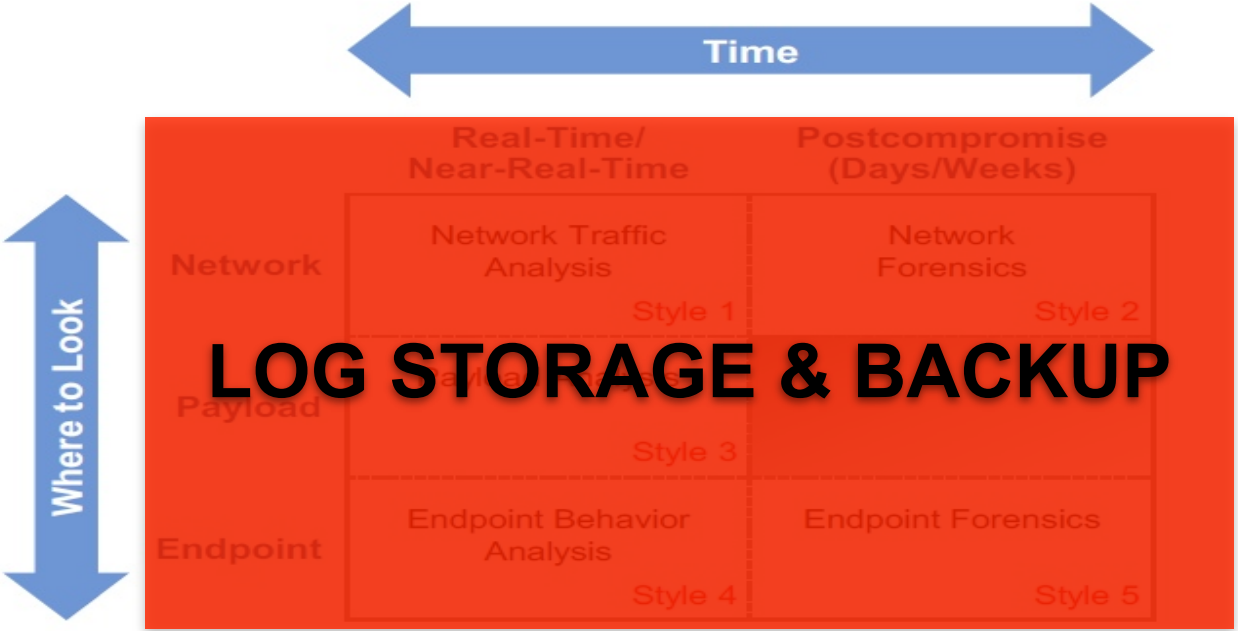


Source: Gartner (August 2013)

http://www.networkworld.com/news/2013/103013-gartner-defense-attacks-275438.html?page=2

POSTCOMPROMISE

Figure 1. Five Styles of Advanced Threat Defense



Source: Gartner (August 2013)

http://www.networkworld.com/news/2013/103013-gartner-defense-attacks-275438.html?page=2

A GLOBAL LEADER IN NETWORK SECURITY

Global presence and customer base

- Customers: **210,000+**
- Units shipped: **2+ Millions**
- Offices: **80+** worldwide, Prague Technical Assistance Center

Platform Advantage built on key innovations

- FortiGuard: industry-leading threat **research**
- FortiASIC: **custom** ASIC-based architecture – first reach of 1Tb
- Market-leading technology: 210 **patents**, 156 pending

Founded **2000,** 1st product shipped **2002,** IPO **2009**

HQ: Sunnyvale, California

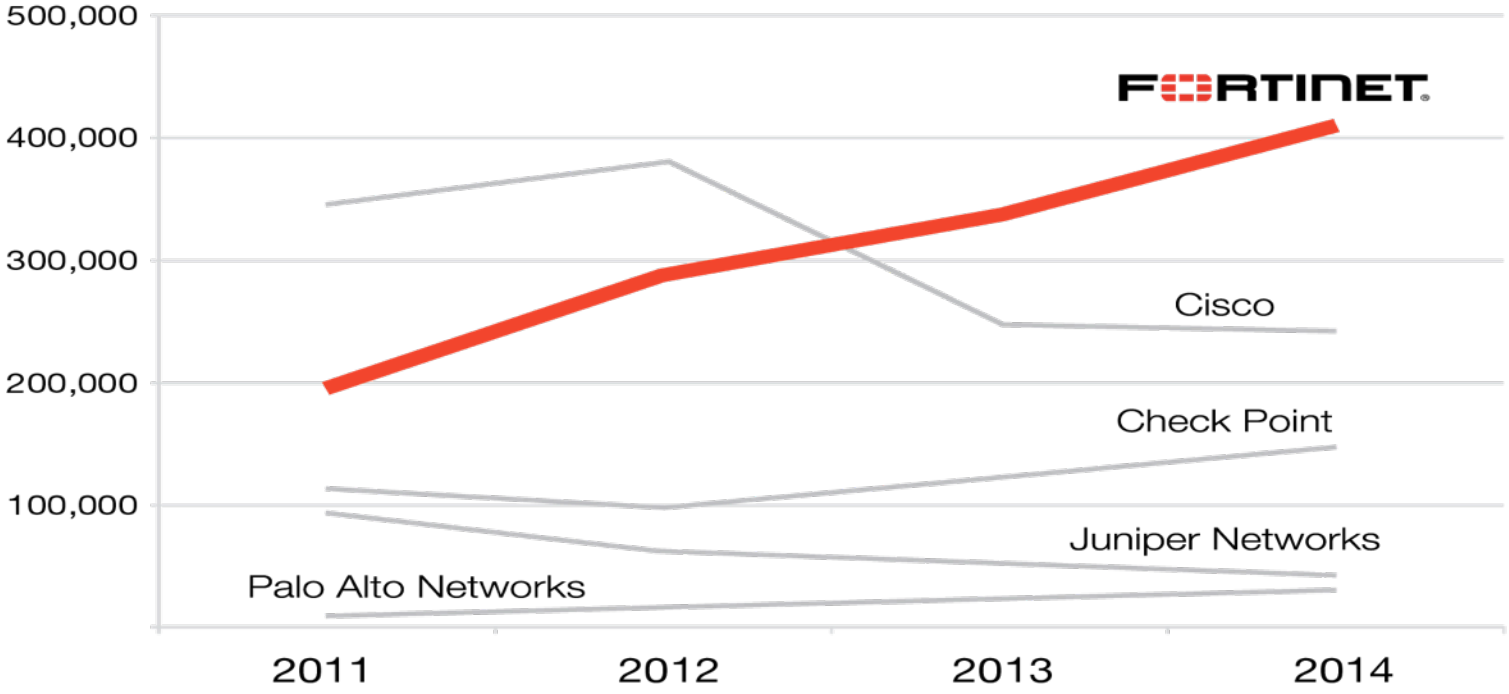
Employees: **2800+** worldwide

Consistent growth, **gaining** market share

Strong positive cash flow, **profitable**

#1 IN NETWORK SECURITY APPLIANCES

UNIT SHARE

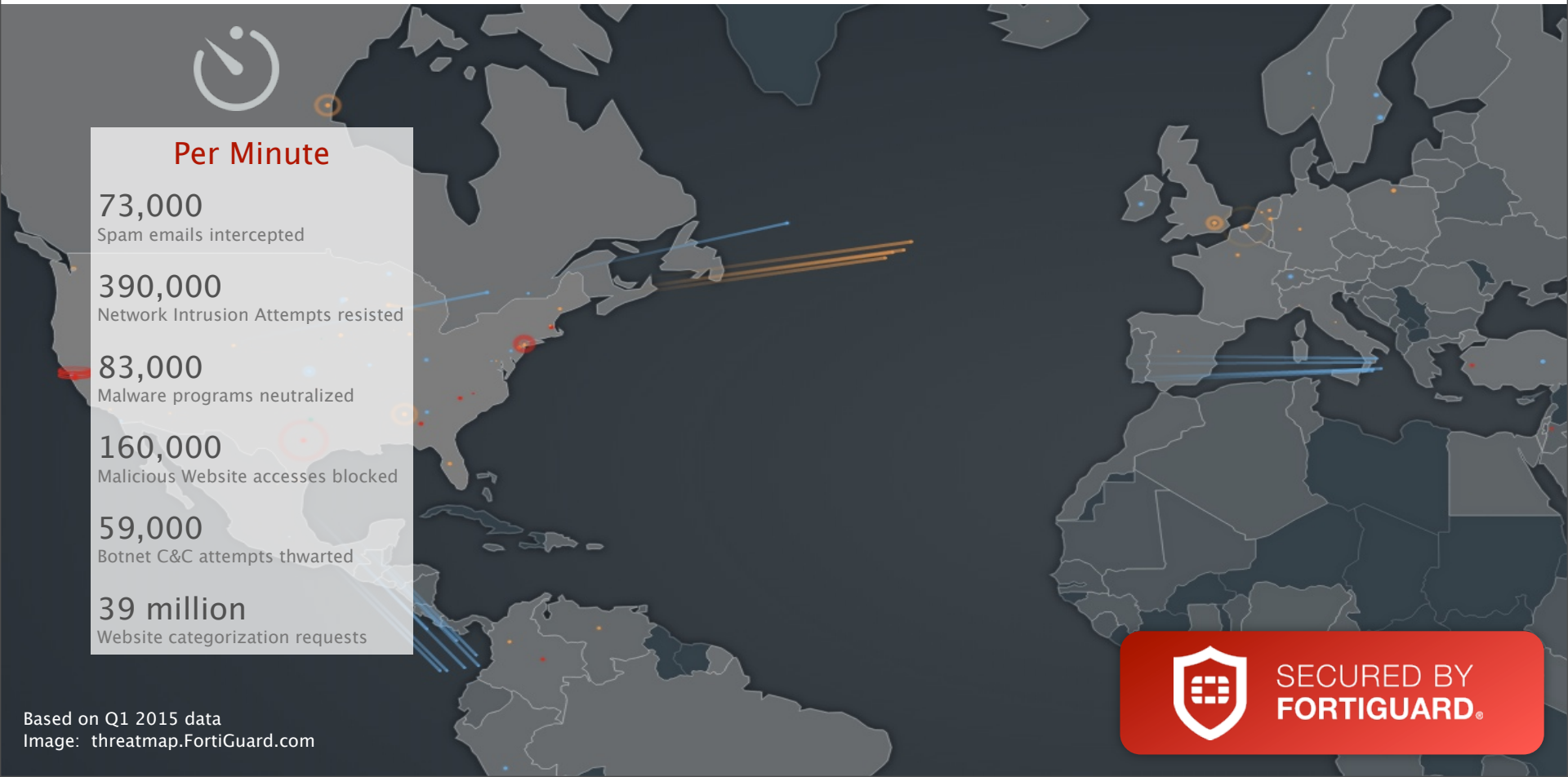


Source: IDC Worldwide Security Appliances Tracker, March 2015 (based on annual unit shipments)

SECURE: IN A FORTIGUARD MINUTE

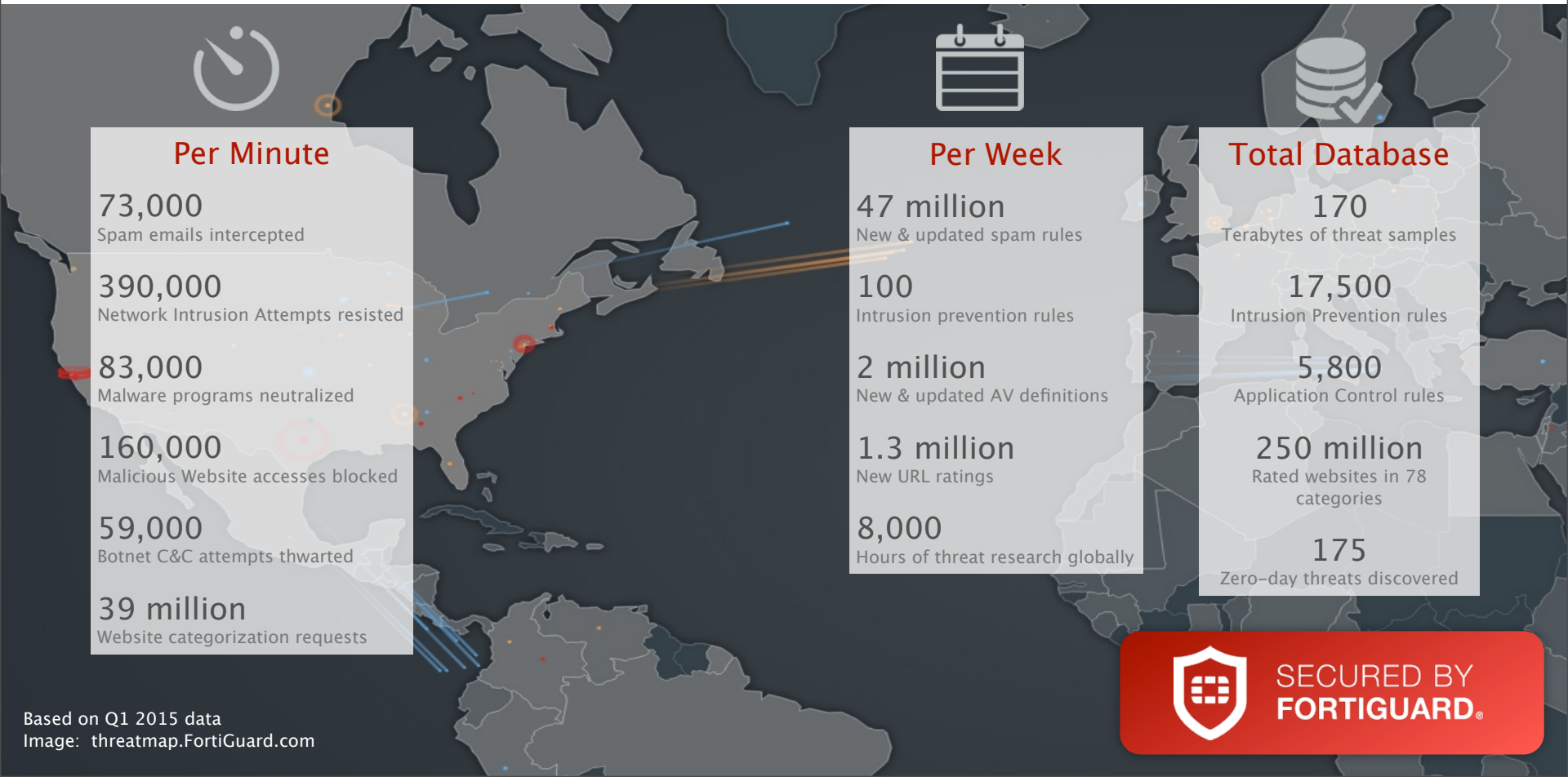
Based on Q1 2015 data
Image: threatmap.FortiGuard.com

SECURE: IN A FORTIGUARD MINUTE



Based on Q1 2015 data
Image: threatmap.FortiGuard.com

SECURE: IN A FORTIGUARD MINUTE



Per Minute

73,000
Spam emails intercepted

390,000
Network Intrusion Attempts resisted

83,000
Malware programs neutralized

160,000
Malicious Website accesses blocked

59,000
Botnet C&C attempts thwarted

39 million
Website categorization requests

Per Week

47 million
New & updated spam rules

100
Intrusion prevention rules

2 million
New & updated AV definitions

1.3 million
New URL ratings

8,000
Hours of threat research globally

Total Database

170
Terabytes of threat samples

17,500
Intrusion Prevention rules

5,800
Application Control rules

250 million
Rated websites in 78 categories

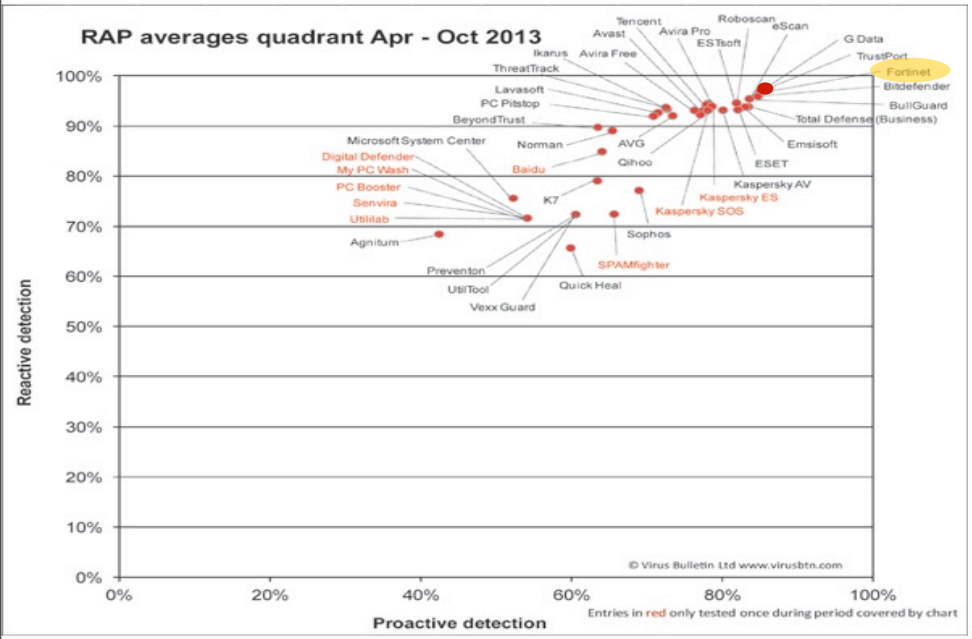
175
Zero-day threats discovered

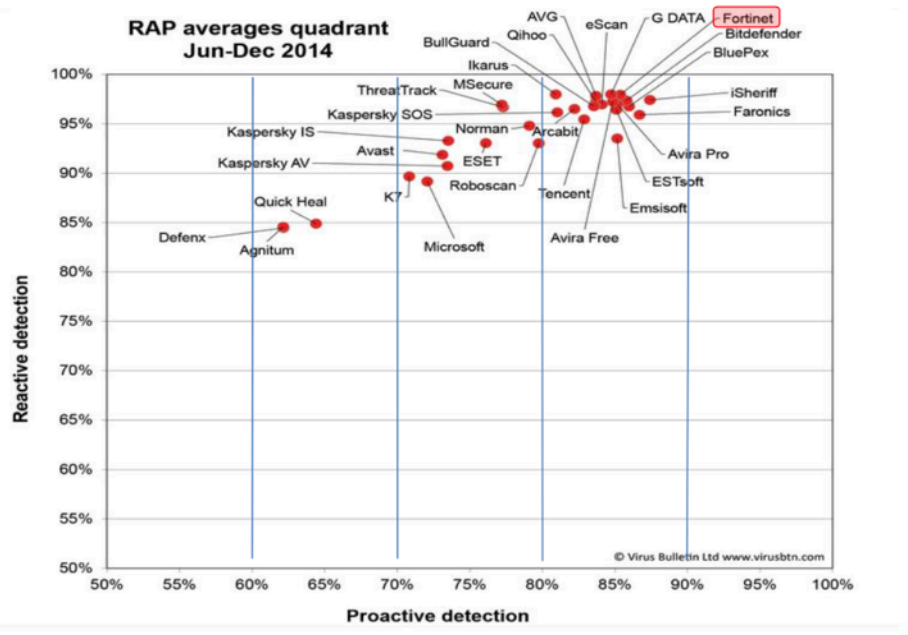
SECURED BY FORTIGUARD®

Based on Q1 2015 data
Image: threatmap.FortiGuard.com

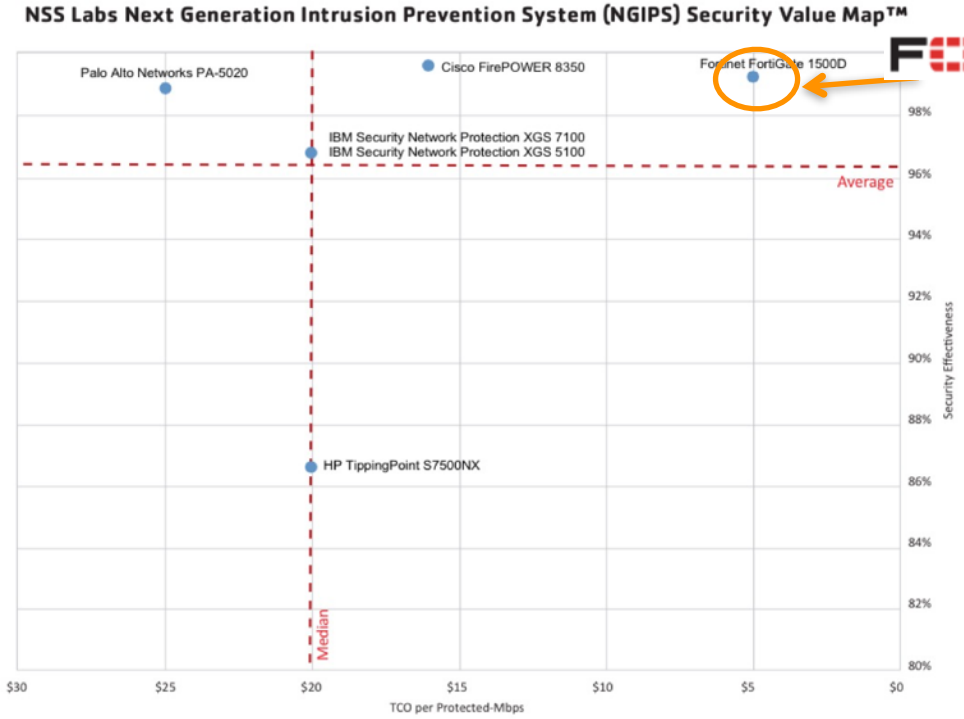
APT: PROACTIVE MALWARE DETECTION

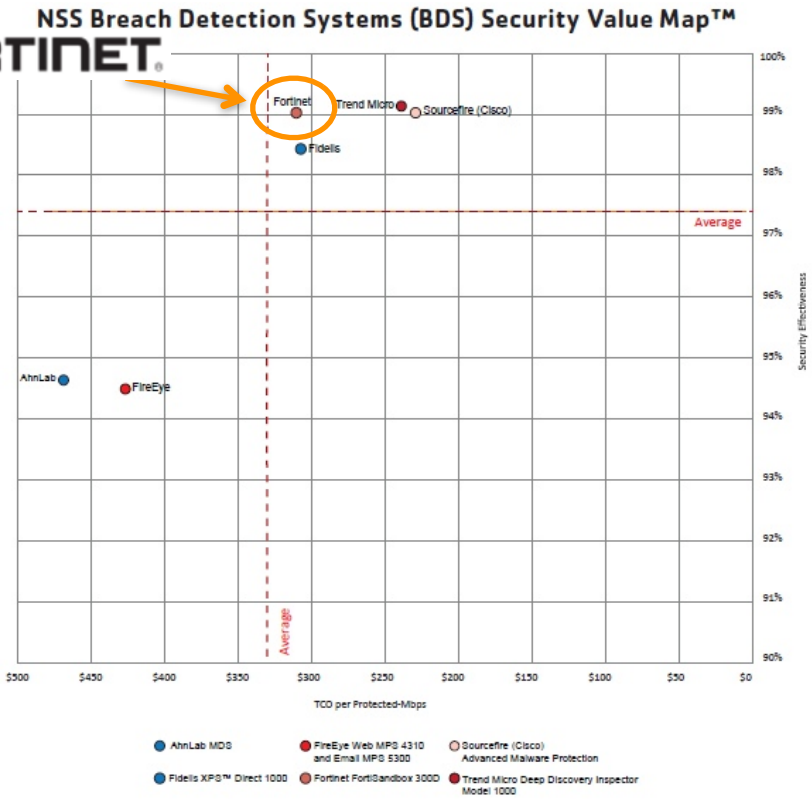
Proactive APT Defense





TOP RATED NGIPS AND SANDBOX





NSS Labs Group Test Results

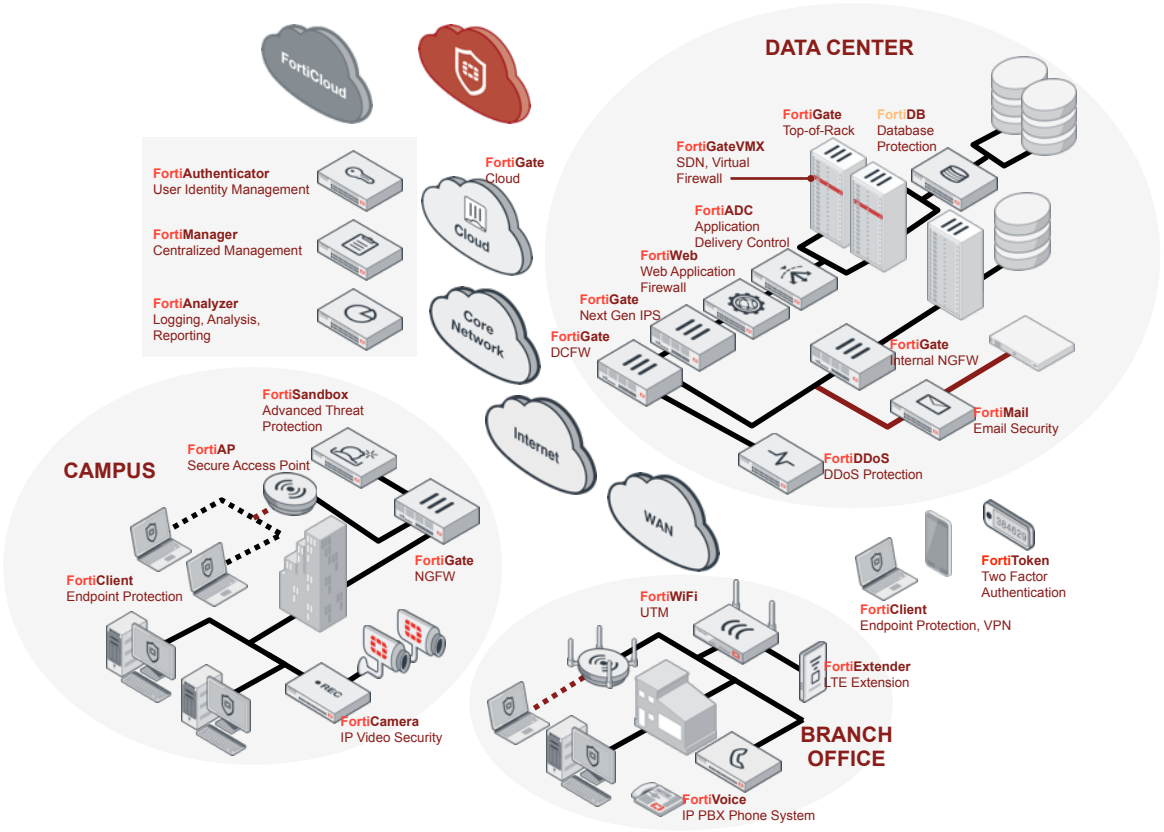
Product	Years and NSS Test Rating				
NGFW/Firewall	2011 Neutral	2012 Neutral	2013 Recommended	2014 Recommended	
NGIPS/IPS		2012 Recommended	2013 Neutral		2015 Recommended
WAF				2014 Recommended	
EPP					2015 Recommended
Breach Detection				2014 Recommended	2015 Recommended

Five years of historical data provided where available. Cell color indicates NSS rating (■ Recommended, ■ Neutral, ■ Caution)

THE FORTINET SECURED NETWORK

Product List

FortiADC	Application Delivery Controller
FortiAnalyzer	Log Analysis
FortiAP	Secure Wireless
FortiAuthenticator	Authentication
FortiCamera	IP Video Security
FortiClient	Endpoint Security
FortiCloud	Cloud Logging and Provisioning
FortiDB	Database Security
FortiDDoS	DDoS Protection
FortiExtender	Cellular LTE Extension
FortiGate	Core Firewall Platform
FortiMail	Email Security
FortiManager	Centralized Management
FortiSandbox	Advanced Threat Protection
FortiToken	2FA Token
FortiVoice	IP PBX Phone Systems
FortiWeb	Web Application Firewall
FortiWiFi	UTM with Wireless Access



Thank you

csr_sales@fortinet.com