Level(3)® COMMUNICATIONS

Connecting and Protecting the Networked World℠

OWN IT

Security Matters
Navigating the Hybrid World

John Ayers, Sr. Director of Product Management

Managing Risk In Today's Networking Environment

The perimeter is evolving, increasing complexity and risk.

Employees are the new perimeter.

The costs of security is growing exponentially.

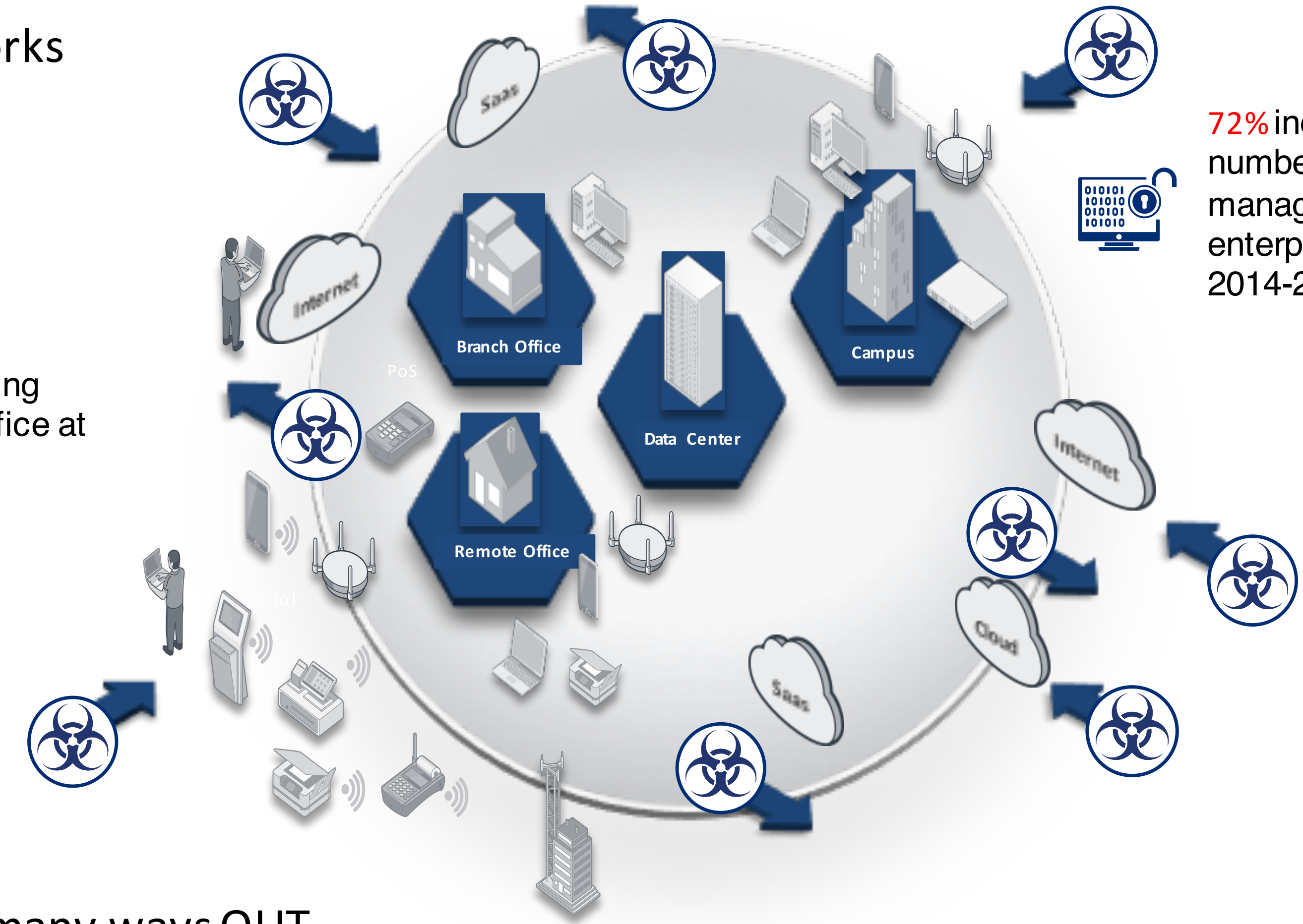
Network efficient hybrid WANs and cloud service deployments increase risk.

Scarcity of in-house security expertise compounds challenges.

New World & New Perimeter.

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

Borderless Networks



72% increase in the number of devices managed in the enterprise from 2014-2015

61% of workers reporting working outside the office at least part time

Many ways IN many ways OUT

Security Market Drivers

- IT resources are strained
  - Staffs are too small, lack the expertise and/or are overburdened
- Increase in the volume, variety, and complexity of threats of all types
  - Attacks now using 5+ vectors

- Security product sprawl
  - Many companies report 15+ vendors in their network!
- Distribution of workforce and proliferation of devices
  - Workers connect as many as 5 device to the corporate LAN

**HIS 2016*

Organizations are Losing Ground

It is hard to get a handle on security…

Spending is up

Staffing challenges

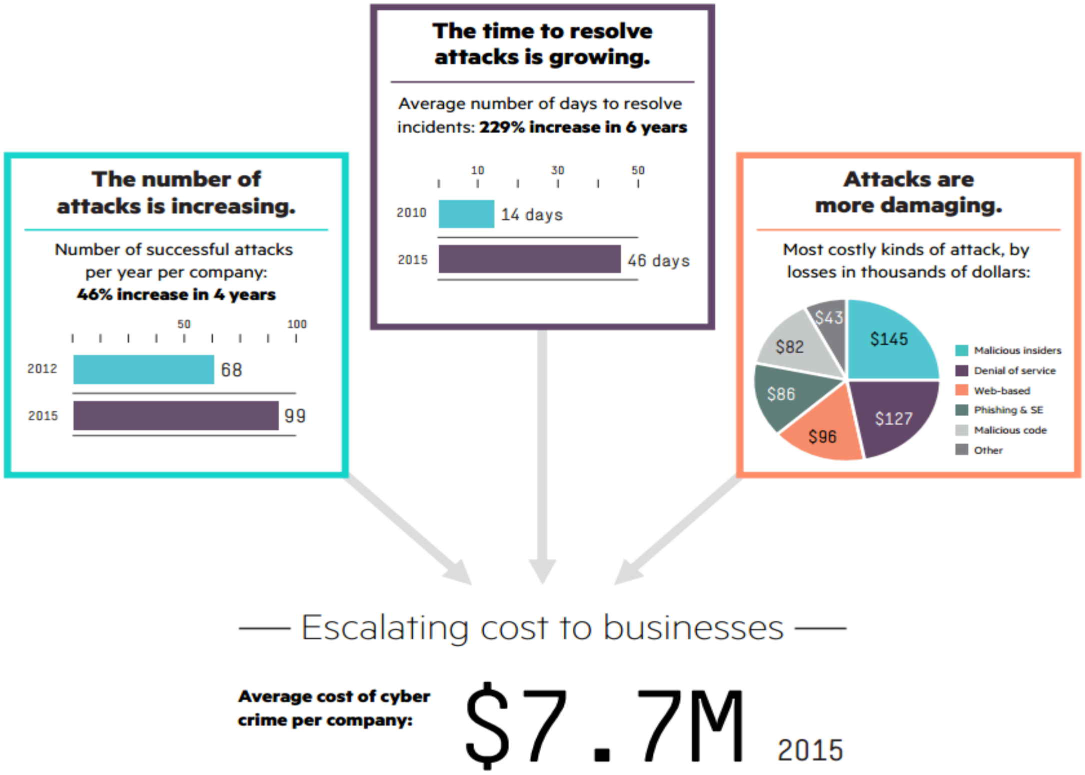
The struggle is keeping up; it's difficult to get ahead

Growing Cost of Cyber Crime

Level(3) COMMUNICATIONS

Connecting and Protecting the Networked World℠

Financial impact has increased by nearly 40 percent in a three year period



The time to resolve attacks is growing.

Average number of days to resolve incidents: **229% increase in 6 years**

The number of attacks is increasing.

Number of successful attacks per year per company: **46% increase in 4 years**

Attacks are more damaging.

Most costly kinds of attack, by losses in thousands of dollars:

— Escalating cost to businesses —

Average cost of cyber crime per company: $7.7M 2015

- Denial of service (DoS) attacks accounted for nearly half of all security incidents in the technology sector.
- Web app attacks were responsible for over half of all breaches where data was stolen.

Source: HP Ponemon Study t" Feb. 2015; Verizon 2016 Breach Report

Scarcity of Security Expertise Compounds these Challenges

Level(3) COMMUNICATIONS
Connecting and Protecting
the Networked World℠

Insights from CISOs

"Protecting the enterprise is harder and more complex."

"Management wants me to reduce budget and provide predictable operating expense."

"I can't find or keep good security people."

"Meanwhile, I'm just trying to keep us safe."

> 70 security vendors in my IT environment

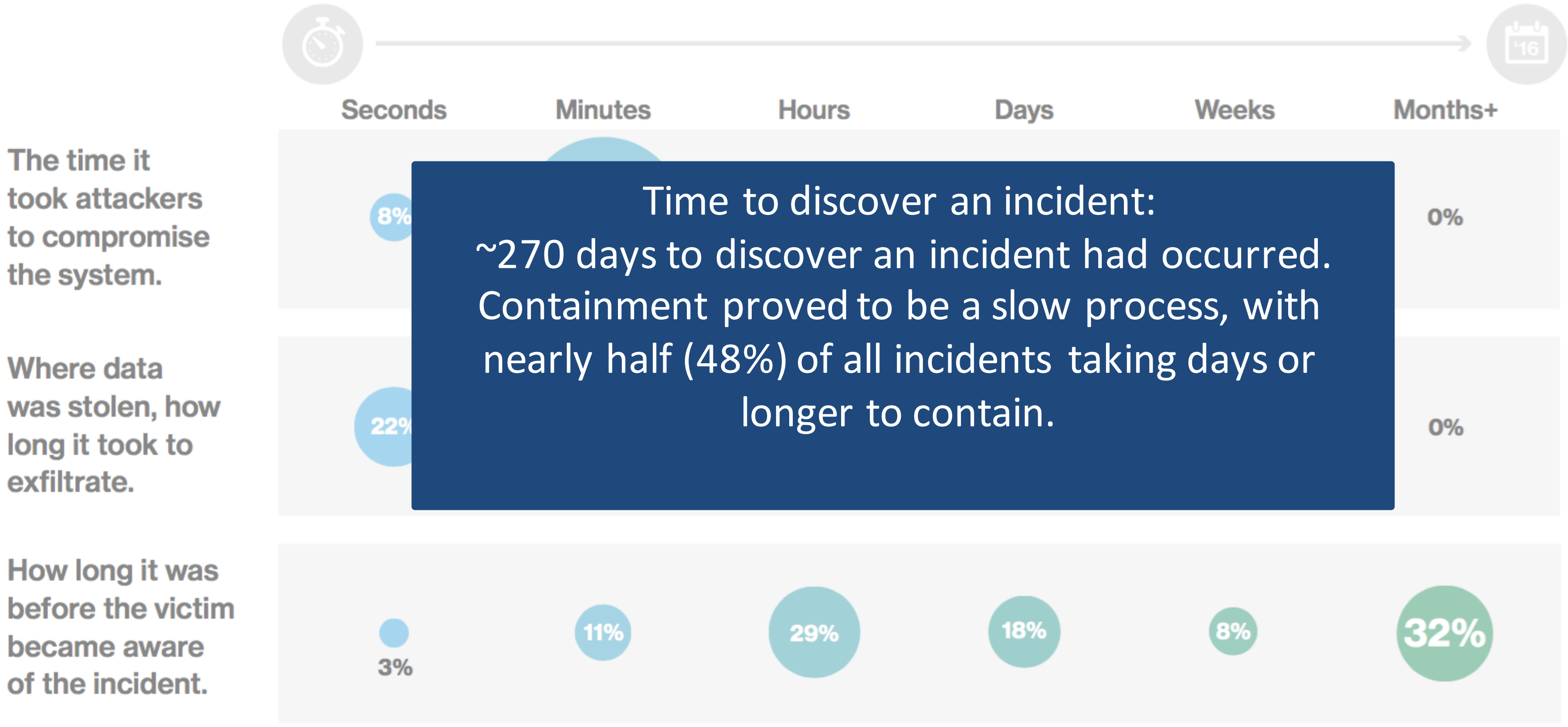
Should I consider MSS?

0% Unemployment

The adversary is winning

IDC, Market Analysis Perspective: Worldwide Security Services, 2015 — Breach Is a Foregone Conclusion, Doc #259239, Sep 2015

The bad guys are getting better AND faster



Time to discover an incident:
~270 days to discover an incident had occurred. Containment proved to be a slow process, with nearly half (48%) of all incidents taking days or longer to contain.

Figure 2: Incident timeline for the technology sector

Source: Verizon 2016 Data Breach Investigations Report

Risk Based Security

- Technical and administrative controls that are selected once an organization has identified the true risk to their business.
  - NGFW - Blocks access to and from suspect IP addresses.
  - Web Filtering – Denies access to malicious or blocked websites.
  - Application Control – Specific controls based on features of applications. Blocks attacks that are designed to exploit holes intentionally allowed through a corporate firewall.
  - Authentication - enables controlled network access and applies authentication to users of security policies and VPN clients.

Who is Attacking & Why?

- 89% of breaches had a financial or espionage motive.
- 63% of confirmed breaches involved leveraging weak, default or stolen passwords.
- 30% of phishing messages were opened in 2015; and 12% of targets clicked on the malicious attachment or link.

Source: Verizon 2016 Data Breach Investigations Report

How are they doing it

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

- **35% of breaches - Malware**
  - 84% of malware was direct install
  - 95% of malware evaded Anti-virus

- **12% email attachments**
  - Downloaded through malicious email
  - Phishing attacks, Ransomware

http://www.computerhope.com

- **63% brute force attacks**
  - Confirmed breaches involved leveraging weak, default or stolen passwords.
  - DoS

Organizations Must Evolve

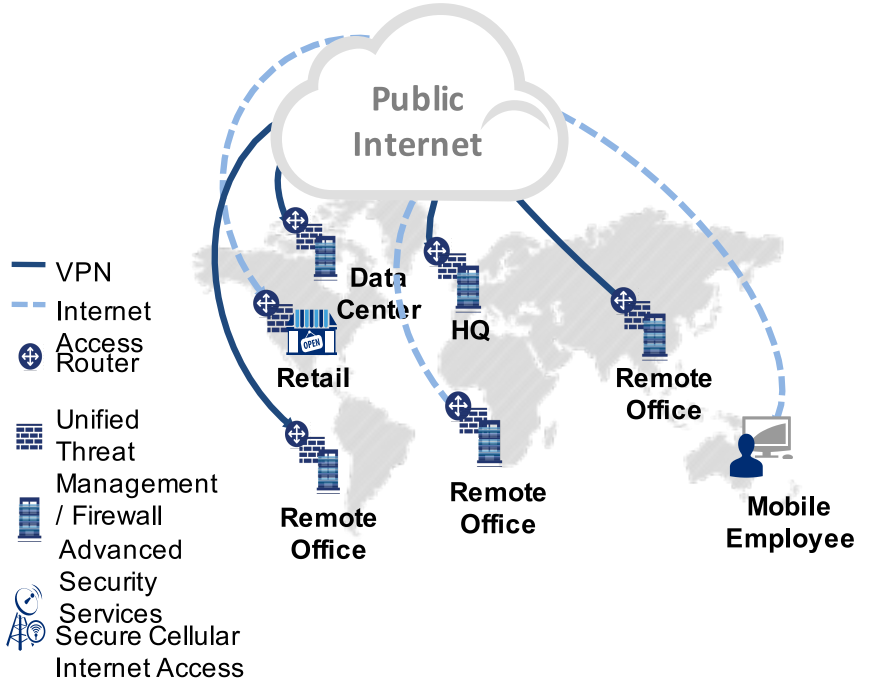
To Efficiently Manage Today's Threats

Level(3) COMMUNICATIONS

Connecting and Protecting the Networked World℠

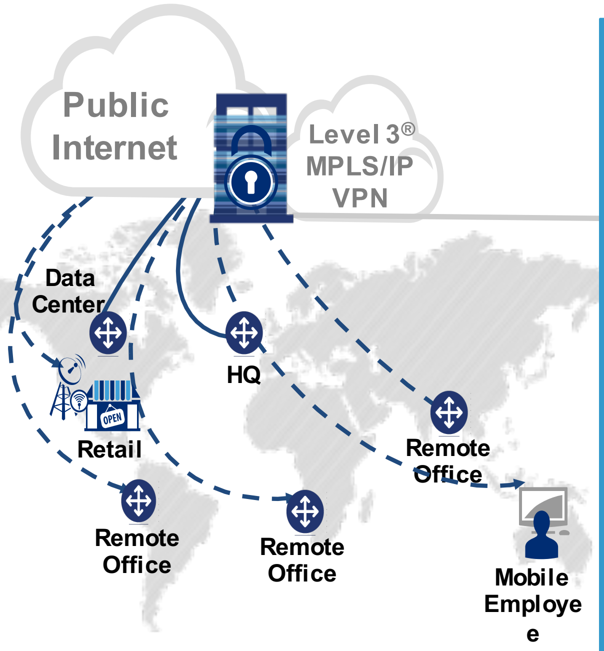
PREMISES-BASED SECURITY CHALLENGES

Environment



NETWORK-BASED SECURITY SOLUTIONS

Future Customer Environment



Security Gateway

- Next-generation firewall
- Intrusion detection
- AV/AS
- Web content /URL filtering
- Application awareness and control
- Malware sandboxing

Concept of a Clean Pipe

The Fresh Water Analogy

Definition: examining and filtering network traffic before that traffic ever reaches the customers premises.

—Frost and Sullivan; “Secure Pipes: Changing The Expectation Of Your Internet Service Providers,” Frank Dickson, Jan. 2015

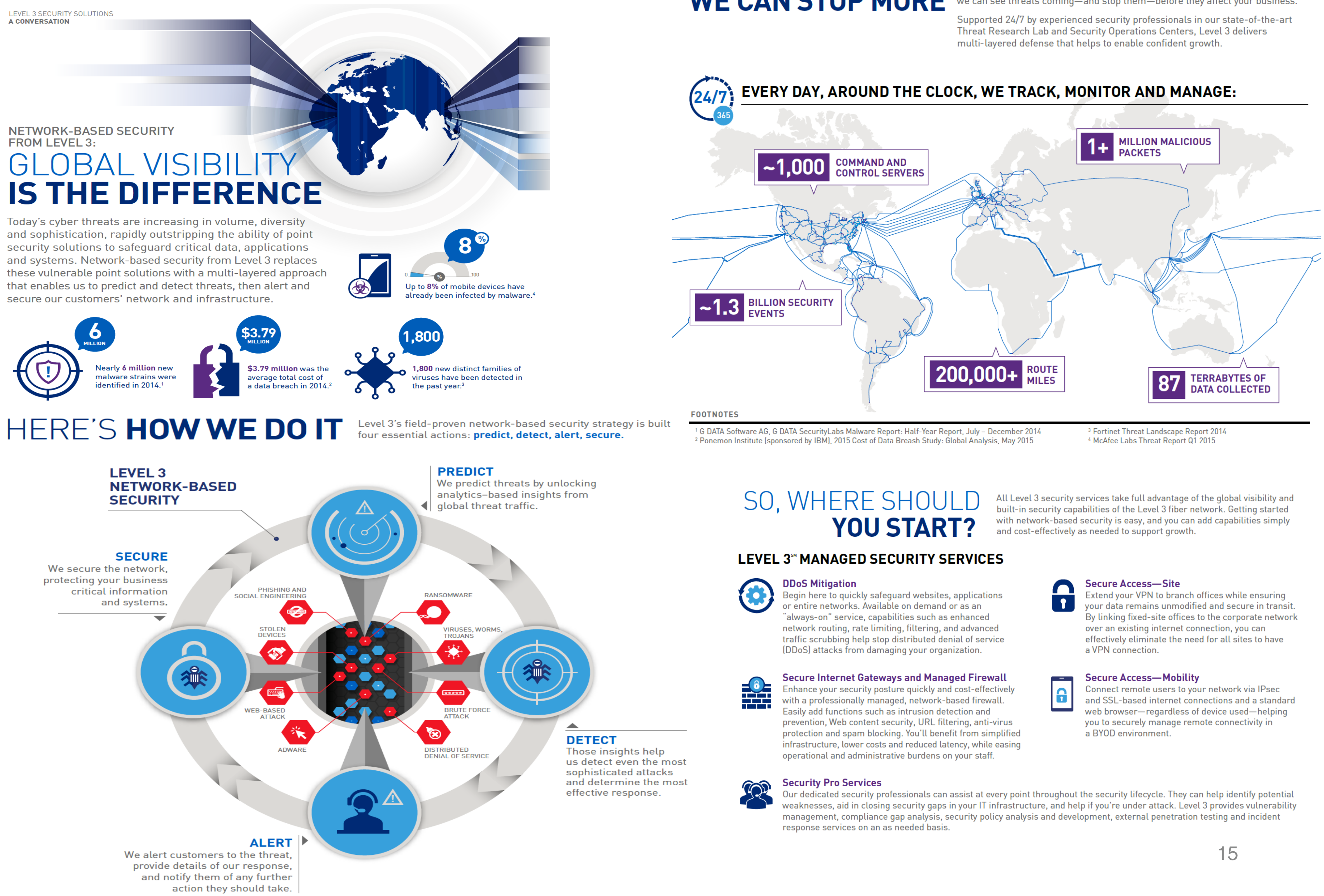
Level(3) COMMUNICATIONS

Connecting and Protecting
the Networked World℠

OWN IT

Level 3 Enterprise Security Gateway – What is it?

Who is Level 3?



LEVEL 3 SECURITY SOLUTIONS
A CONVERSATION

NETWORK-BASED SECURITY
FROM LEVEL 3:

GLOBAL VISIBILITY IS THE DIFFERENCE

Today's cyber threats are increasing in volume, diversity and sophistication, rapidly outstripping the ability of point security solutions to safeguard critical data, applications and systems. Network-based security from Level 3 replaces these vulnerable point solutions with a multi-layered approach that enables us to predict and detect threats, then alert and secure our customers' network and infrastructure.

Up to **8%** of mobile devices have already been infected by malware.[4]

Nearly **6 million** new malware strains were identified in 2014.[1]

$3.79 million was the average total cost of a data breach in 2014.[2]

1,800 new distinct families of viruses have been detected in the past year.[3]

HERE'S **HOW WE DO IT**

Level 3's field-proven network-based security strategy is built four essential actions: **predict, detect, alert, secure.**

LEVEL 3 NETWORK-BASED SECURITY

PREDICT
We predict threats by unlocking analytics–based insights from global threat traffic.

SECURE
We secure the network, protecting your business critical information and systems.

DETECT
Those insights help us detect even the most sophisticated attacks and determine the most effective response.

ALERT
We alert customers to the threat, provide details of our response, and notify them of any further action they should take.

WE SEE MORE, SO **WE CAN STOP MORE**

What's needed now is network-based security from Level 3. We build and operate a vast global fiber network, providing us with a comprehensive vision of what's happening across the threat landscape. That vantage point means that we can see threats coming—and stop them—before they affect your business.

Supported 24/7 by experienced security professionals in our state-of-the-art Threat Research Lab and Security Operations Centers, Level 3 delivers multi-layered defense that helps to enable confident growth.

EVERY DAY, AROUND THE CLOCK, WE TRACK, MONITOR AND MANAGE:

~1,000 COMMAND AND CONTROL SERVERS

1+ MILLION MALICIOUS PACKETS

~1.3 BILLION SECURITY EVENTS

200,000+ ROUTE MILES

87 TERRABYTES OF DATA COLLECTED

FOOTNOTES

[1] G DATA Software AG, G DATA SecurityLabs Malware Report: Half-Year Report, July – December 2014
[2] Ponemon Institute (sponsored by IBM), 2015 Cost of Data Breash Study: Global Analysis, May 2015
[3] Fortinet Threat Landscape Report 2014
[4] McAfee Labs Threat Report Q1 2015

SO, WHERE SHOULD **YOU START?**

All Level 3 security services take full advantage of the global visibility and built-in security capabilities of the Level 3 fiber network. Getting started with network-based security is easy, and you can add capabilities simply and cost-effectively as needed to support growth.

LEVEL 3℠ MANAGED SECURITY SERVICES

DDoS Mitigation
Begin here to quickly safeguard websites, applications or entire networks. Available on demand or as an "always-on" service, capabilities such as enhanced network routing, rate limiting, filtering, and advanced traffic scrubbing help stop distributed denial of service (DDoS) attacks from damaging your organization.

Secure Internet Gateways and Managed Firewall
Enhance your security posture quickly and cost-effectively with a professionally managed, network-based firewall. Easily add functions such as intrusion detection and prevention, Web content security, URL filtering, anti-virus protection and spam blocking. You'll benefit from simplified infrastructure, lower costs and reduced latency, while easing operational and administrative burdens on your staff.

Secure Access—Site
Extend your VPN to branch offices while ensuring your data remains unmodified and secure in transit. By linking fixed-site offices to the corporate network over an existing internet connection, you can effectively eliminate the need for all sites to have a VPN connection.

Secure Access—Mobility
Connect remote users to your network via IPsec and SSL-based internet connections and a standard web browser—regardless of device used—helping you to securely manage remote connectivity in a BYOD environment.

Security Pro Services
Our dedicated security professionals can assist at every point throughout the security lifecycle. They can help identify potential weaknesses, aid in closing security gaps in your IT infrastructure, and help if you're under attack. Level 3 provides vulnerability management, compliance gap analysis, security policy analysis and development, external penetration testing and incident response services on an as needed basis.

Level 3 Enterprise Security Gateway

Our Solution:

The new Level 3 Enterprise Security Gateway (ESG) is a network-based layer of protection against an increasingly complicated threat landscape delivered in the cloud. ESG combines a wide range of next-generation security technologies that help organizations stay ahead of threats.

Level 3 Value:

Built on the proven foundation of network-based security, Level 3's Enterprise Security Gateway delivers cost-effective, flexible and reliable protection wherever business happens — without sacrificing performance.

The Level 3 network acts as a sensor, you have the visibility and control you need to monitor, block and report attempts to break into your network.

Level 3 ® Enterprise Security Gateway Service

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

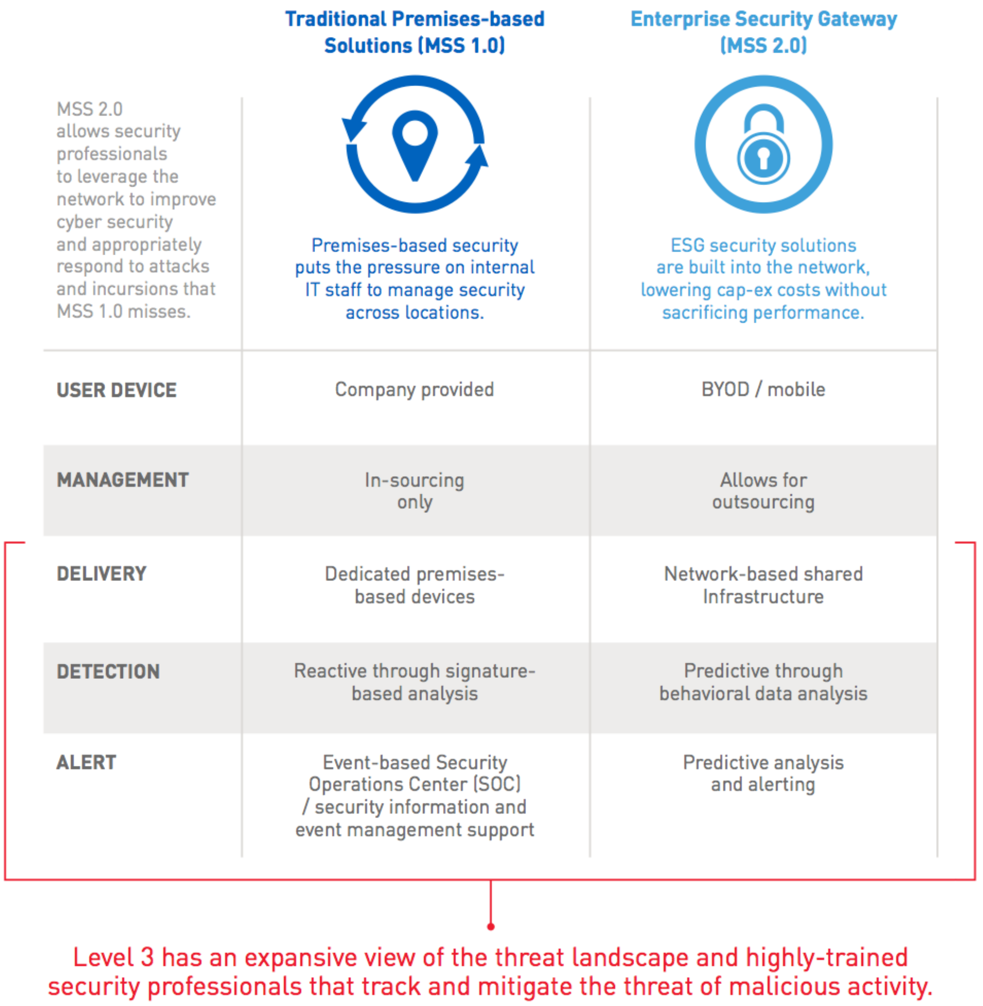
A flexible, secure gateway for your protected network

Network-based security solution offering next-generation firewall protection delivered in the cloud

- Broad security coverage across today's distributed hybrid networks, data centers, cloud deployments, branches, remote offices and mobile workers

- Cost-effective, flexible and reliable protection wherever business happens — without sacrificing performance

- Optimize infrastructure with flexible, bandwidth- IP agnostic access methods: IPsec and GRE



	Traditional Premises-based Solutions (MSS 1.0)	Enterprise Security Gateway (MSS 2.0)
MSS 2.0 allows security professionals to leverage the network to improve cyber security and appropriately respond to attacks and incursions that MSS 1.0 misses.	Premises-based security puts the pressure on internal IT staff to manage security across locations.	ESG security solutions are built into the network, lowering cap-ex costs without sacrificing performance.
USER DEVICE	Company provided	BYOD / mobile
MANAGEMENT	In-sourcing only	Allows for outsourcing
DELIVERY	Dedicated premises-based devices	Network-based shared Infrastructure
DETECTION	Reactive through signature-based analysis	Predictive through behavioral data analysis
ALERT	Event-based Security Operations Center (SOC) / security information and event management support	Predictive analysis and alerting

Level 3 has an expansive view of the threat landscape and highly-trained security professionals that track and mitigate the threat of malicious activity.

Summary

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

- The threat landscape is evolving rapidly due to nation-state, organized crime, and cyber terrorism
- Customers are building a network with multiple perimeters “Hybrid”
- Hybrid World is here to stay adopt a robust Data encryption approach
- Organizations must assume the “new normal” -- at least some parts of their networks have been compromised
- Personal Information are an asset -- understand its value, location, and movement
- Perform regular security evaluations, risk assessments, and awareness training for employees
- Determine core competencies, perform functions that you do well, outsource others to trusted, skilled firms
- Some security functions must be done in partnership with your service provider(s)

Cloud Security Services Checklist

Are you reaping the benefits of managed security?

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

Actionable Alerts:

Do you get accurate alerts with few false positives?
Are your alerts customized to your network and business?
Do your notifications describe the significance of alerts and how to react?

Threat Detection:

Does your service provider often detect critical security threats that you were completely unaware of?
Has your service provider modeled the APTs kill chain to more accurately detect Indicators of Attack and Compromise?
Does your service provider utilize global threat intelligence for correlation and threat discovery?
Does your provider incorporate advanced tools like Next-Generation SIEM, Use Case Analytics, behavior analysis, business context, and pattern discovery to detect and prioritize threats?

High-Touch SOC Services:

Are your Security Analysts responsive and available whenever you need them?
Does your provider's Security Operations Center (SOC) team proactively investigate suspicious events and not overly rely on system-generated alerts?
Does your SOC team truly understand your landscape and act as an added member of your security team?
Are you regularly consulted on new threats, alert trends and how to benefit your security posture?

Customized to Your Needs:

Does your service provider maintain a Run-book customized to your unique environment, processes, and rules?
Does your service provider create custom use cases, rules, and content to benefit your specific technologies, and environment?
Does your service provider create dashboards and reports customized to the needs of different users?

Auto Response:

Does your service provider allow for automating the response to high-risk events for breach prevention to ensure threats are addressed in real-time, 24x7?

Visibility :

Do you have full visablity to your security events and the ability to analyze and investigate each event?
Does your service provider provide easy-to-use dashboards, log search, and reports to visualize your security posture?

Flexible Deployment:

Does your service provider offer the choice of a cloud-based firewall services, managed on-premise firewall services, or hybrid deployment models?