IPv6 Security Concerns
Introduction to Integralis

Garry Sidaway

SVP Security Strategy

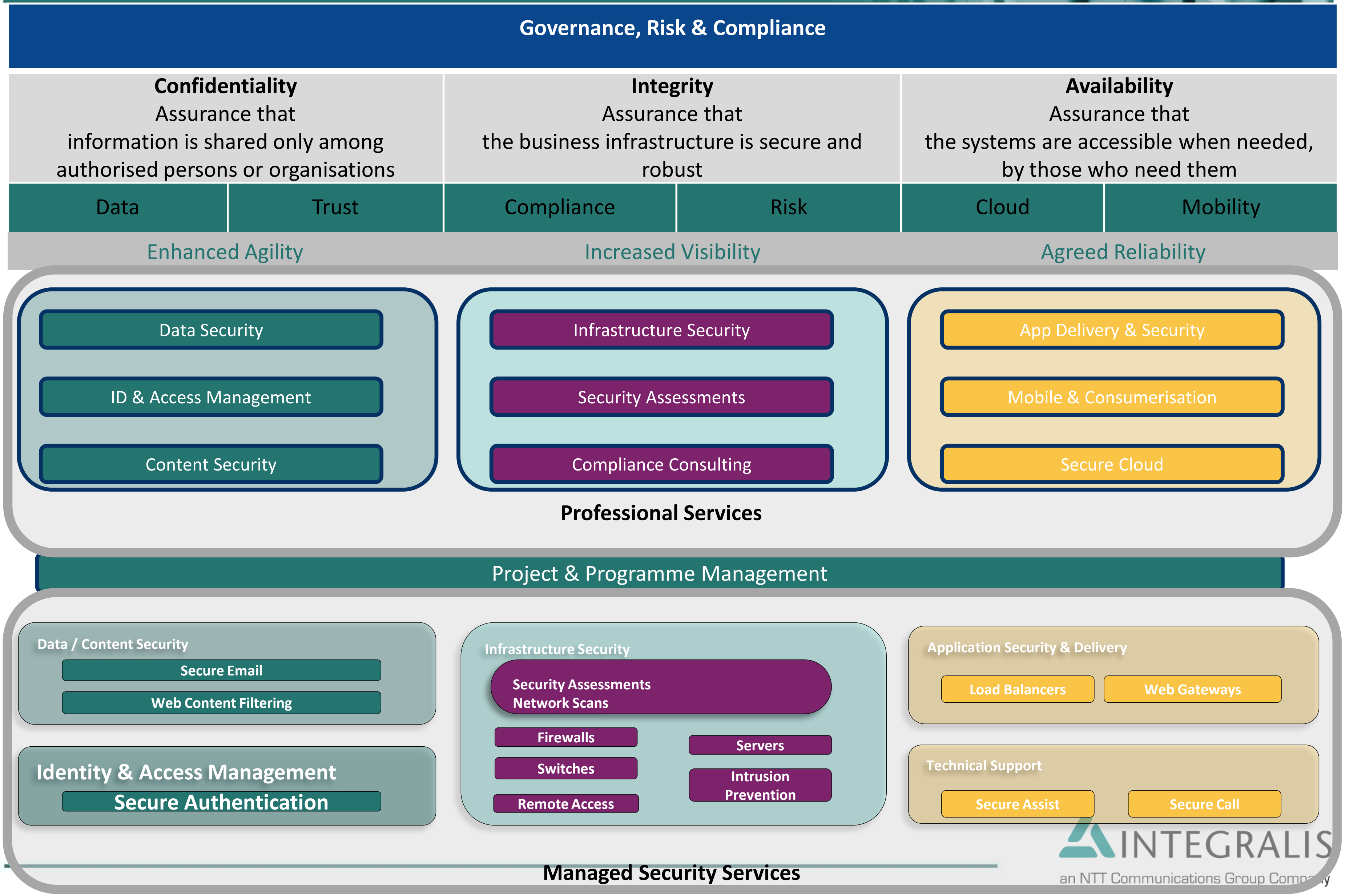
INTEGRALIS

an NTT Communications Group Company

Agenda

- Introduction to Integralis
- IPv6 Security Concerns
- Questions

Continuous Secure Service Delivery



Governance, Risk & Compliance

Confidentiality
Assurance that
information is shared only among
authorised persons or organisations

Integrity
Assurance that
the business infrastructure is secure and
robust

Availability
Assurance that
the systems are accessible when needed,
by those who need them

Data | Trust | Compliance | Risk | Cloud | Mobility

Enhanced Agility

Increased Visibility

Agreed Reliability

Data Security

ID & Access Management

Content Security

Infrastructure Security

Security Assessments

Compliance Consulting

App Delivery & Security

Mobile & Consumerisation

Secure Cloud

Professional Services

Project & Programme Management

Data / Content Security

Secure Email

Web Content Filtering

Identity & Access Management

Secure Authentication

Infrastructure Security

Security Assessments
Network Scans

Firewalls

Switches

Remote Access

Servers

Intrusion
Prevention

Application Security & Delivery

Load Balancers

Web Gateways

Technical Support

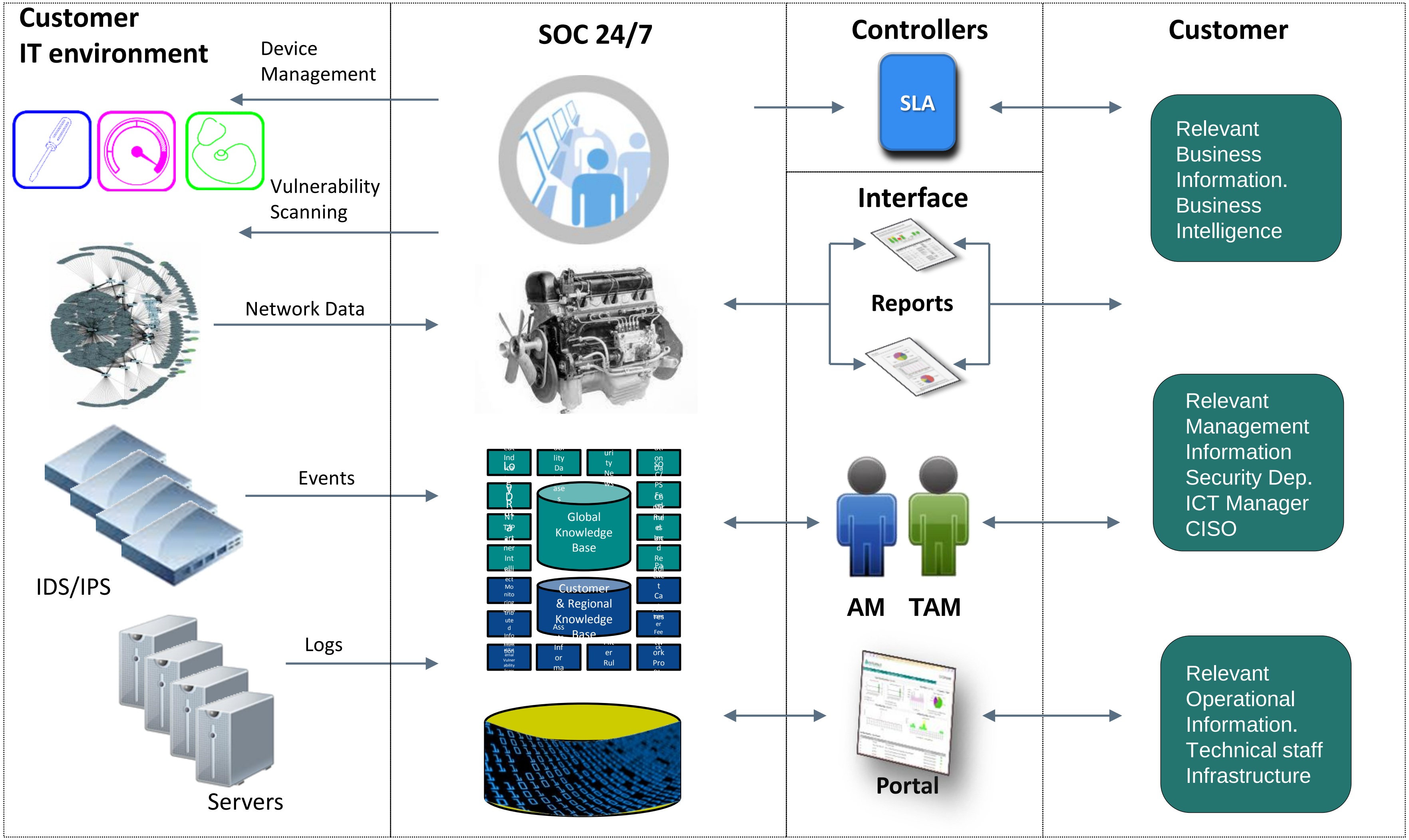
Secure Assist

Secure Call

Managed Security Services

INTEGRALIS
an NTT Communications Group Company

Integralis – More than Technology
Blend of Managed & Professional Services



Customer
IT environment

Device
Management

Vulnerability
Scanning

Network Data

Events

IDS/IPS

Logs

Servers

SOC 24/7

Global
Knowledge
Base

Customer
& Regional
Knowledge
Base

Controllers

SLA

Interface

Reports

AM TAM

Portal

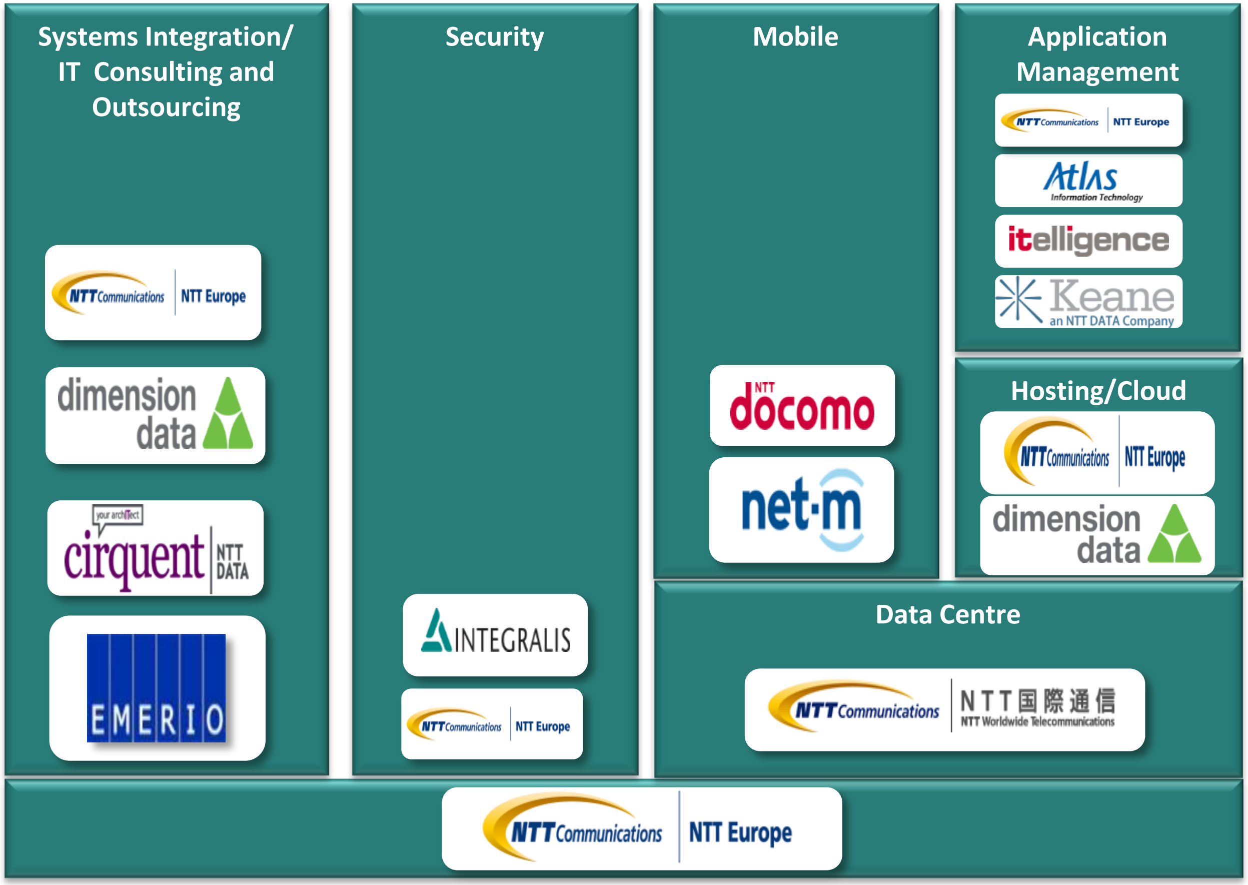
Customer

Relevant
Business
Information.
Business
Intelligence

Relevant
Management
Information
Security Dep.
ICT Manager
CISO

Relevant
Operational
Information.
Technical staff
Infrastructure

Integralis Security Fabric - NTT Group Continuous Secure Service Delivery



Systems Integration/ IT Consulting and Outsourcing

NTT Communications | NTT Europe

dimension data

your archiTect cirquent NTT DATA

EMERIO

Security

INTEGRALIS

NTT Communications | NTT Europe

Mobile

NTT docomo

net·m

Application Management

NTT Communications | NTT Europe

Atlas Information Technology

itelligence

Keane an NTT DATA Company

Hosting/Cloud

NTT Communications | NTT Europe

dimension data

Data Centre

NTT Communications | NTT国際通信 NTT Worldwide Telecommunications

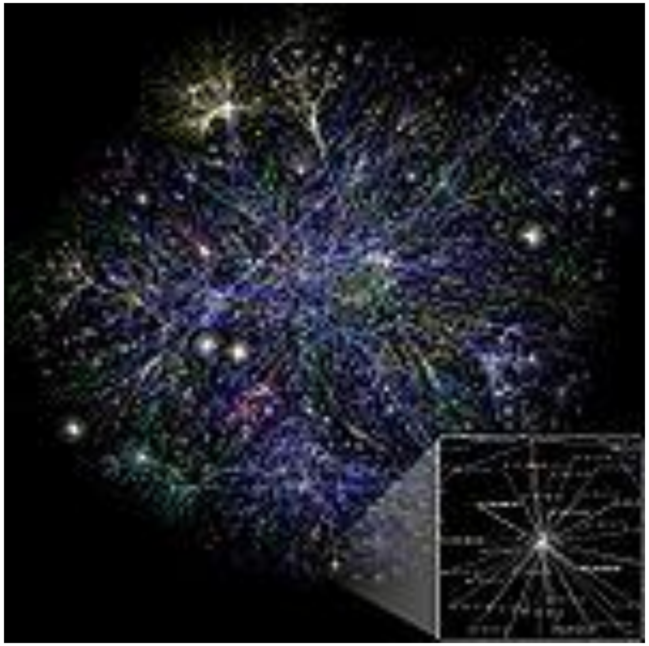
NTT Communications | NTT Europe

- NTT Communications **$10 billion revenue** and **10,000 people globally**
- Global networks and IT **in over 150 countries** providing ITC & IT Security solutions
- **Global Tier 1 IP Backbone**
- Managing more than **$12.5 billion** of network infrastructure assets globally
- Access to more than **12,500** specialists
- **Global reach, dedicated service support and management, local touch**

Agenda

- Introduction to Integralis
- IPv6 Security Concerns
- Questions

Too BIG to attack?



Routing paths through a portion of the Internet
as visualized by the Opte Project

IPv6 Address space is huge

IPv6 Address 128 bits

128 bits: 1x10^12/sec =107,828,975,246 Centuries

Smart Networks

Your network maybe IPv4, but what are your devices?

many devices may be communicating over IPv6, within your network already

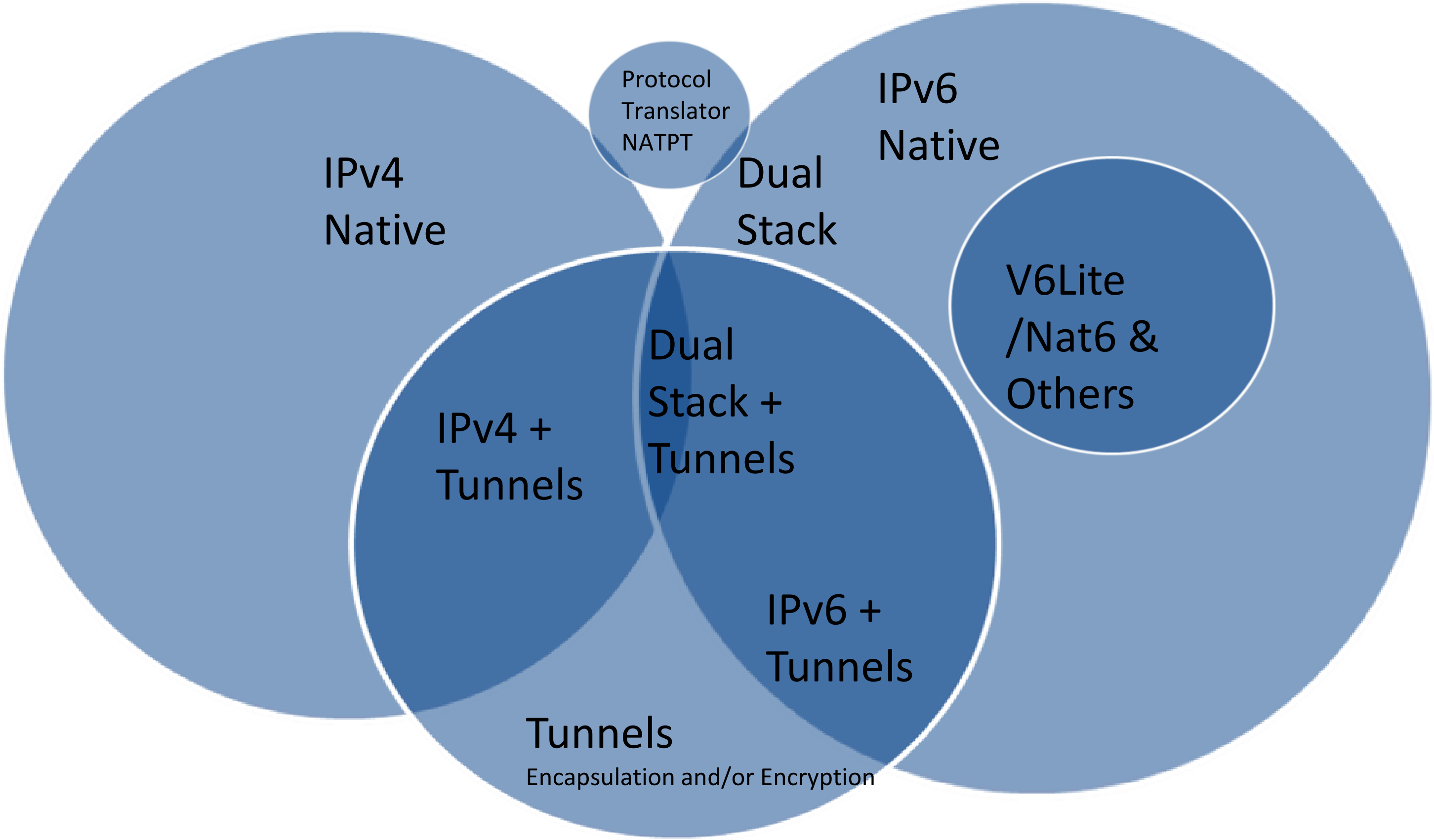
Address Space

- One Interface may simultaneously have various addresses
  - Link local , site local, global unicast
  - The administrator may enable global unicast addresses only for devices that must access the internet.

- Extension Headers in IPv6 may be used to bypass the security policy
  - E.g. routing headers have to be accepted at specific devices (IPv6 endpoints)

- In IPv6 some ICMP and (link-local) Multicast messages are required for the correct operation of the protocol
  - The firewalls should be appropriately configured only to allow the right messages of these types
  - The IPv4 ICMP security policy must be appropriately adapted for ICMPv6 messages

Attack Surfaces



Teredo: IPv6 Tunneling Protocol

ISATAP: Windows v6 Transition Tool

6in4

6over4

Freenet6

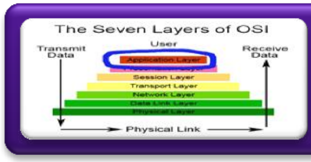
And many more

Visibility is Security

Ref Joe Klein # Command Info

EXTRA: The Same

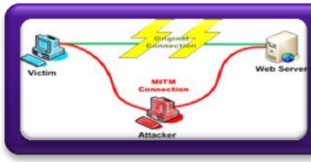
- There are some security issues that IPv6 has little effect on:



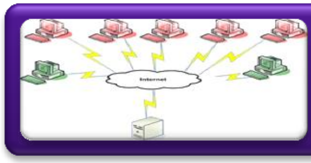
Application-layer attacks

Sniffing

Rogue Devices



Man-in-the-Middle Attacks



Flooding/DoS Attacks

Unfamiliarity Causes Misconfigurations

Many network administrators and IT practitioners are still relatively unfamiliar with all IPV6's “ins and outs”

Common issues:

- Not realizing IPv6 is already in their network
- Ignorance of Tunneling Mechanisms
- Lack of ACL policy for IPv6 multi-homing
- Unawareness of potential privacy issues
- Over permissiveness, just to get it to work

IPv6 Security Controls Lagging Hacking Arsenal/Tools

- Attacker already have many IPv6 capable tools:

- THC-IPv6 Attack Suite
- Nmap
- Wireshark
- Multi-Generator (MGEN)
- IPv6 Security Scanner (vscan6)
- Halfscan6
- Strobe
- Netcat6
- TCPDump
- COLD
- Spak6
- Isic6 Hyenae
- SendIP
- Packit
- 4to6ddos
- 6tunneldos
- Imps6-tools
- Relay6
- 6tunnel
- NT6tunnel
- VoodooNet
- Scapy6
- Metasploit (etc.)
- Web Browsers (XSS & SQLi)

Fake_MIPv6

Is IPv6 More Secure

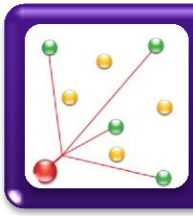
- IPv6 is a bigger toolkit for defence and attack
- Powerful tool for defence
  - IPSec (Authentication & Encryption
  - Secure Neighbour Discovery (SEND)
  - Crypto-generated address (CGA)
  - Unique Local Addresses (ULAs)

- New Attack Vectors
  - Automated Tunneling
  - Neighbourhood Discovery and auto-configuration
  - End-to-End (E2E) model
  - Complexity
  - Lack of education

Firewalls (and Admins) Must Learn New Tricks

How to filter ICMPv6?

Handling new extension headers



Filtering Multicast and Anycast

Hosts w/multiple addresses

- Automatic configuration security mechanisms that mask the MAC address may also be used to conceal and attacker.
- Assign global addresses only to systmes that require Internet connectivity
- Non-trivial addresses for critical systems
- Filter non necessary services at the firewall
- Selective ICMPv6 filtering
- Keep the systems and application security level current by deploying patches
- Careful selection of the cases when Extension Headers should be allowed

Typical IPv6 Devices Have Multiple Addresses

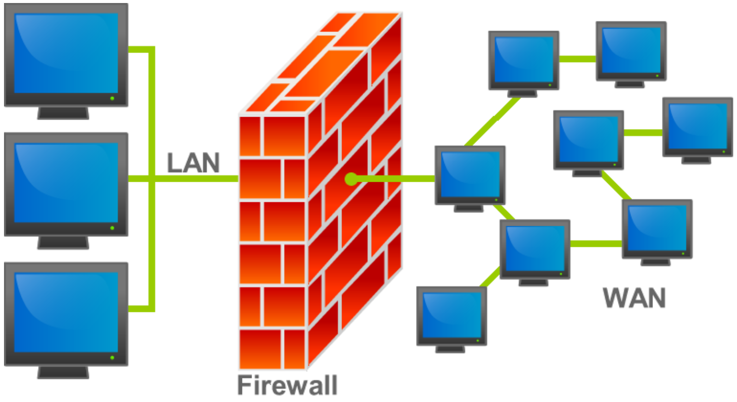
At least a *Link-Local Address* (FE80::/10)

Likely a *Unique Global Address* (2000::/3)

Possibly a *Site-Local Address* (FC00::/7)

You will probably need MULTIPLE Firewall or ACL policies for these extra networks within your organization

Preferably, static tunnel configuration. Only authorized systems should be allowed as tunnel end-points



- The firewall should have the ability to check fragmented packets
- Filter packets with wrong source addresses
- Traceback procedures at levels 2 and 3 should be available to show concealed attackers
  - The big number of available addresses may be used to hide the attackers.
- Disallow packets with multicast source addresses
- It’s better to avoid “translation” mechanisms between IPv4 and IPv6 and use dual stack instead

So Long NAT! Hello, End-2-End Addressing

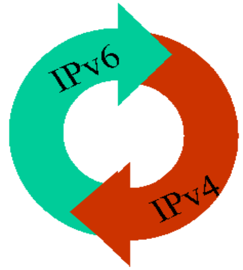
NAT does NOT provide security!

End-2-End (public) addressing increases accountability

So… Does/Will IPv6 Provide More Security?

- **Probably Not.** Few will adopt/use the IPv6 related security additions early on. Furthermore, the protocol’s “newness” and administrator’s unfamiliarity may result in more vulnerabilities at first. *That said, IPv6 security is NOT worse than IPv4.*

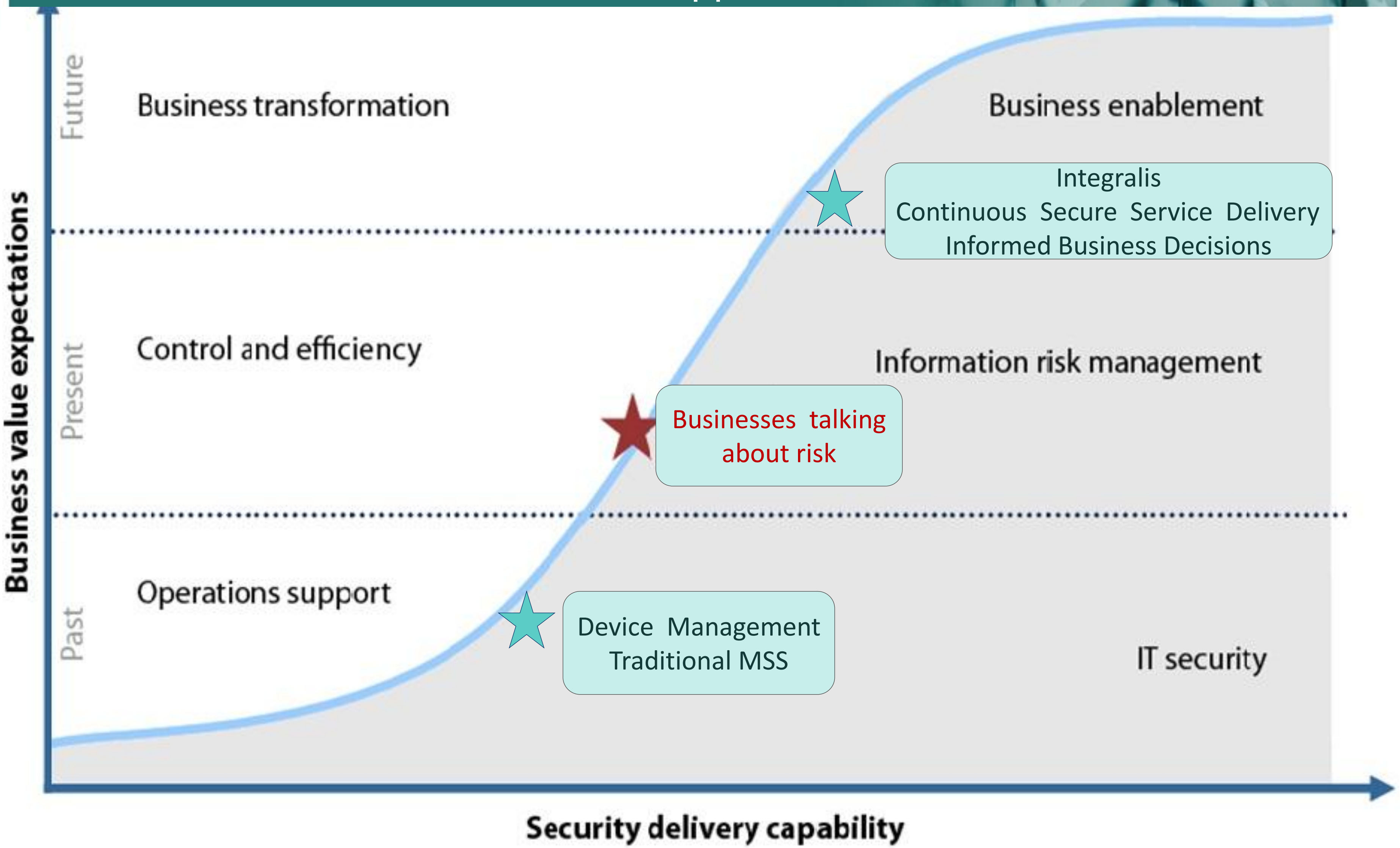
Short Term



- **Yes**. If leveraged, some IPv6 additions can increase our overall network security. As we become more familiar with it, and more network services begin to leverage advanced options, *IPv6 should prove slightly more security than IPv4.*

Long Term

Integralis – Risk Management – Business Decision Support


Business value expectations
Future
Present
Past
Business transformation
Business enablement
Integralis
Continuous Secure Service Delivery
Informed Business Decisions
Control and efficiency
Information risk management
Businesses talking about risk
Operations support
Device Management
Traditional MSS
IT security
Security delivery capability

INTEGRALIS
an NTT Communications Group Company

End to End Security Services

What next

Questions

Discussion

References

References and acknowledgements

- Ref Joe Klein # Command Info
- http://tools.ietf.org/html/rfc3964
- Test domain for ipv6 support
- www.mrp.net/cgi-bin/ipv6-status.cgi
- Whatismyv6.com or ip6.me