dimension data

accelerate
your ambition

# Network Barometer Report 2016

*A gauge of global networks' readiness to accelerate business*

## *Contents*

### Copyright notice and disclaimer

The data and information contained in the Network Barometer Report are for information purposes only. While the commentary and hypotheses in this Report are based on rigorous data analysis and market experience, the Report also contains opinion. Furthermore, while reasonable steps are taken to ensure the accuracy and integrity of the data and information provided, Dimension Data accepts no liability or responsibility whatsoever if such data or information is incorrect or inaccurate, for whatsoever reason. Dimension Data does not accept liability for any claims, loss, or damages of any nature arising as a result of the reliance on, or use of, such data or information by any individual or organisation.

# Introduction

The annual 2016 Dimension Data *Network Barometer Report* gauges the readiness of today's networks to support and accelerate business.

The Report uses real factual data from two sources:

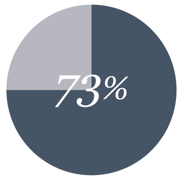
- 320 Technology Lifecycle Management Assessments (TLMAs) we carried out over 2015 for clients, covering *97,000 network devices* in *28 countries* and across multiple industry sectors
- data on the networks we monitor for our clients during 2015, gathered from four of our Global Service Centres, and covering *300,000 incidents* on more than *1.5 million assets in 105 countries*

This makes the report *more reliable* than reports compiled from opinion surveys. In the commentary, we apply insight from our client activity to shed light on the significance of the data.

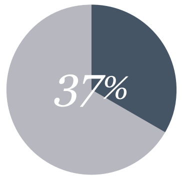
dimensiondata.com/networkbarometer

## Key findings summary

**For the first time in five years, *networks are getting younger*. 58% of devices are now current, an 11-percentage point increase from last year. Companies are starting to *refresh equipment earlier in its lifecycle*. Digitisation strategies are top of mind, *including workspace mobility and collaboration*, the Internet of Things, and automation.**



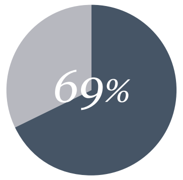
Close to three quarters of service incidents fall outside standard break-fix support contracts



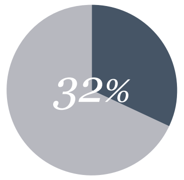
with over a third due to configuration or other human error and could be avoided with proper monitoring, configuration management, and automation.

**Ageing devices, especially branch office routers and obsolete aggregation routers, are more *likely to suffer failure*.**

***ITIL process times*** **are far shorter on networks that we manage**



Incident response is 69% faster



and repair is 32% faster on networks monitored and managed by Dimension Data.

**Add *service desk integration* and *incident response time* is reduced by a further 55%, and *incident resolution* by a further 36%.**

**Despite the *higher refresh rate*, networks are getting *less secure*, primarily due to *neglected patching*. 76% of network devices have at least one known *security vulnerability*, the highest figure in five years, and up from 60% last year.**

**Adoption of IPv6-ready equipment *has risen from 21% to 41% in the last year*. While there is market *interest in software-defined networks*, it's *early in the adoption cycle* and today, *few organisational networks* are capable of supporting a software-defined approach.**

## Recommendations

*Your network is the platform for your digital business.*
It needs to be ubiquitous, highly flexible, robust, and secure to adapt easily to business change, while increasing the maturity of your operational support environment.
*In light of this year's key findings*, we recommend:

1

Network automation is one of the key building blocks to provide the foundation for a digital strategy. Organisations executing digital strategies should refresh *networks with equipment capable of supporting automation using software-defined approaches*.

2

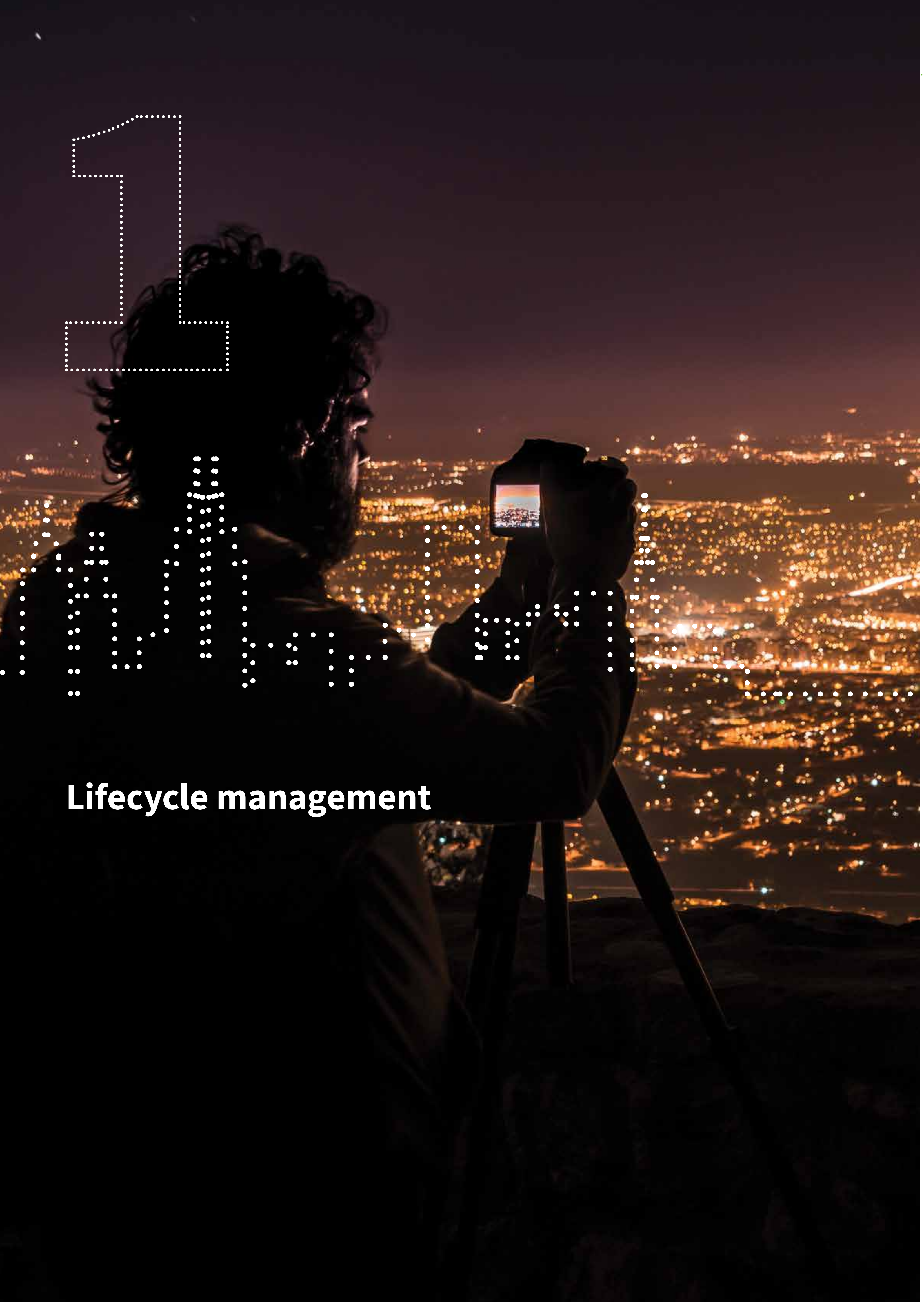
*Standardise the types of technologies used in the network and their configurations as much as possible*. This will increase network agility by allowing for faster change management processes, shorten the time to repair, and reduce support costs when devices fail.

3

Since new devices take longer to repair, organisations should architect networks for service availability. Simple break-fix support contracts on single devices are no longer enough. *Consider end-to-end service monitoring, automated troubleshooting, and automation contracts*.

4

Strategic network transformation should not neglect day-to-day security patching: *prioritise patching on business-critical edge and data centre switches*, but don't neglect aggregation and access switches.

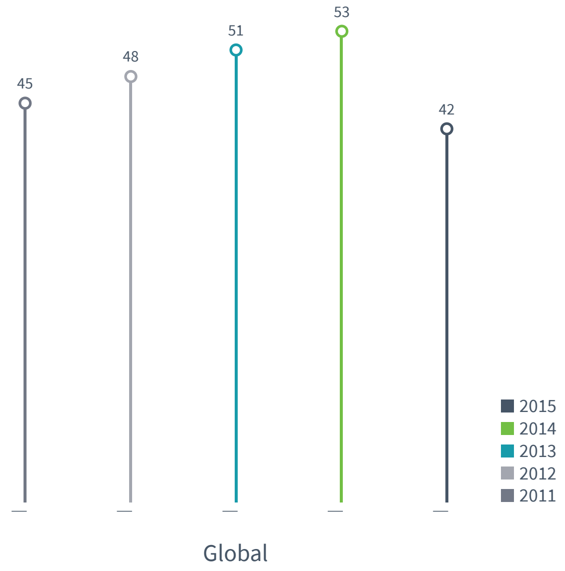


# 1

# Lifecycle management

## For the first time in five years, networks are getting younger

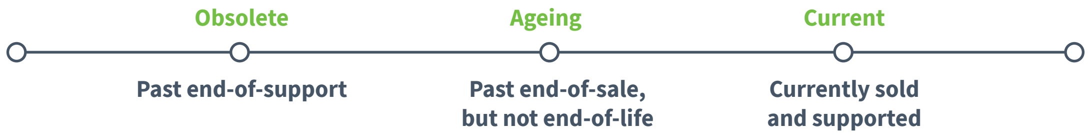
**Figure 1: Percentage of ageing and obsolete devices, global average**



In 2016, the percentage of ageing and obsolete devices in networks **fell from 53% last year to 42%**. Since 2010, networks had been ageing; this year's report illustrates that the trend has reversed.

This can be attributed to companies replacing ageing and obsolete equipment with the new generation of programmable infrastructure, particularly in data centre networks.

### Lifecycle stage definitions

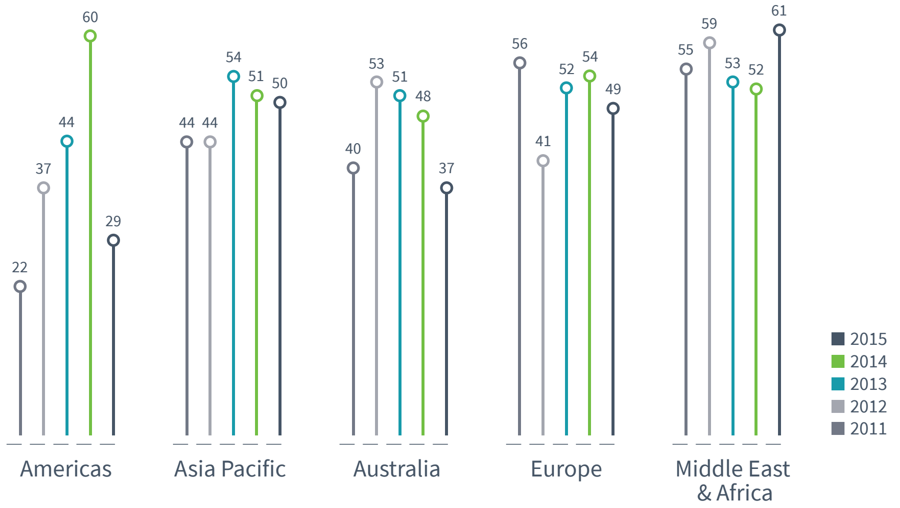

Obsolete
Past end-of-support
Ageing
Past end-of-sale, but not end-of-life
Current
Currently sold and supported

### Old isn't necessarily bad

Ageing networks are not necessarily a bad thing, you just need **to understand the implications**. They require a **different support construct**, with gradually increasing support costs. It does however mean you can delay refresh costs. Ageing networks are less likely to support initiatives such as **software-defined networks and automation**, or **handle traffic volumes** necessary for collaboration or cloud, so organisations need to approach this with care.

# There’s considerable regional variation in the age of networks

Figure 2: Percentage of ageing and obsolete devices by region



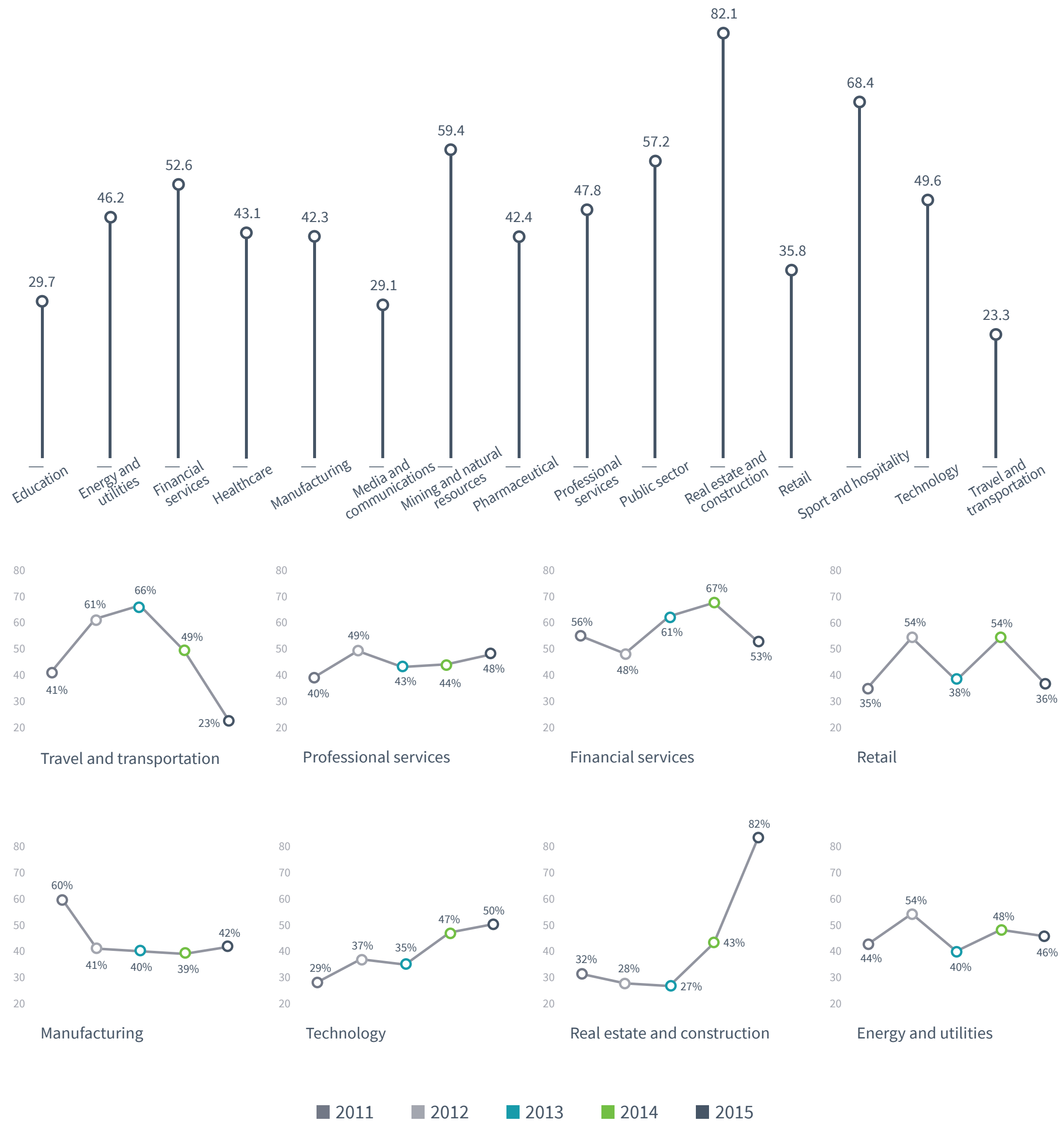
In Europe, Asia-Pacific, and Australia, network age has reduced broadly in line with the global average (42%). However, in the Americas there’s been a very marked (31 percentage point) **reduction in ageing and obsolete devices from 60% in 2015 to 29% this year**.

We believe this to be a release of pent-up spend following four years of financial constraint. Clients appear to be refreshing networks with the new generation of programmable infrastructure. In Asia-Pacific and Australia, we’ve noticed equipment refresh occurring as part of data centre network redesigns.

In Middle East & Africa, contrary to the global trend, network age has increased, which we believe to be the result of economic uncertainty, particularly in South Africa.

# Network age also varies by industry

Figure 3: Percentage of ageing and obsolete devices, by industry



There’s been a sharp decline in the age of networks in the travel and transportation sector over the last two years. And a slight decline in financial services and retail this year, as the spend on network refresh picked up.

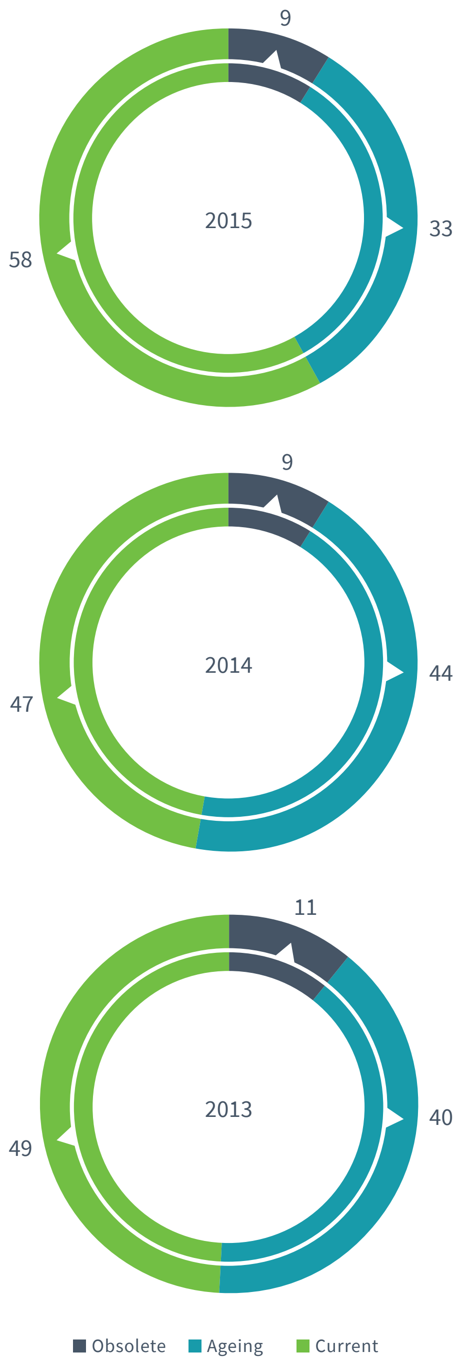
The age of networks in manufacturing, as well as energy and utilities, hasn’t changed much. And there’s been a steady increase in network age in technology and professional services over the last few years.

In the real estate and construction sectors, we’ve seen a sharp increase in network age over the last three years, which we believe is due to the impact of the economic downturn in those sectors.

# Organisations are starting to refresh more strategically

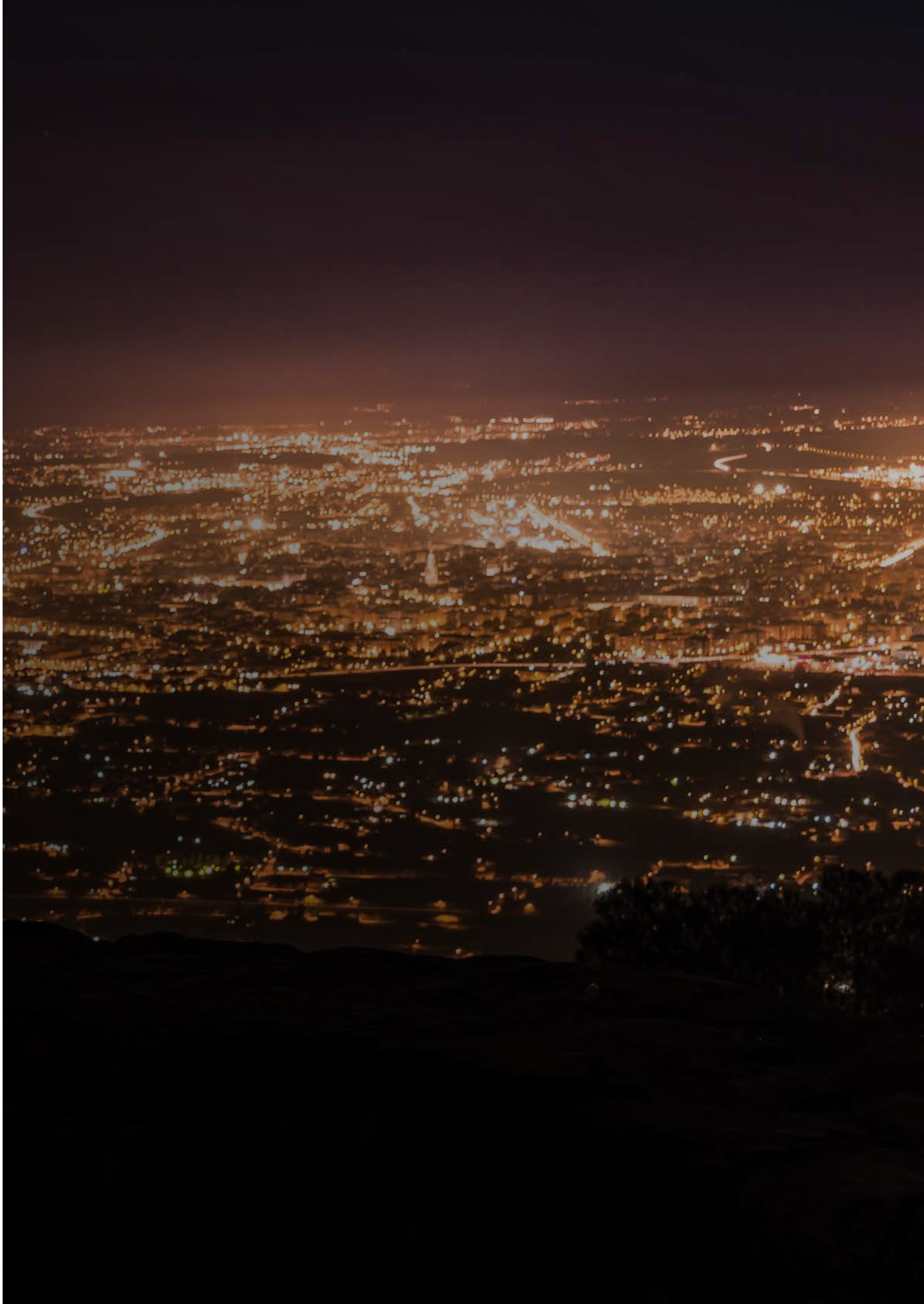
Historically, companies tended to wait until devices were obsolete before refreshing. We're now seeing more strategic approaches to refresh, with an architectural vision in mind.

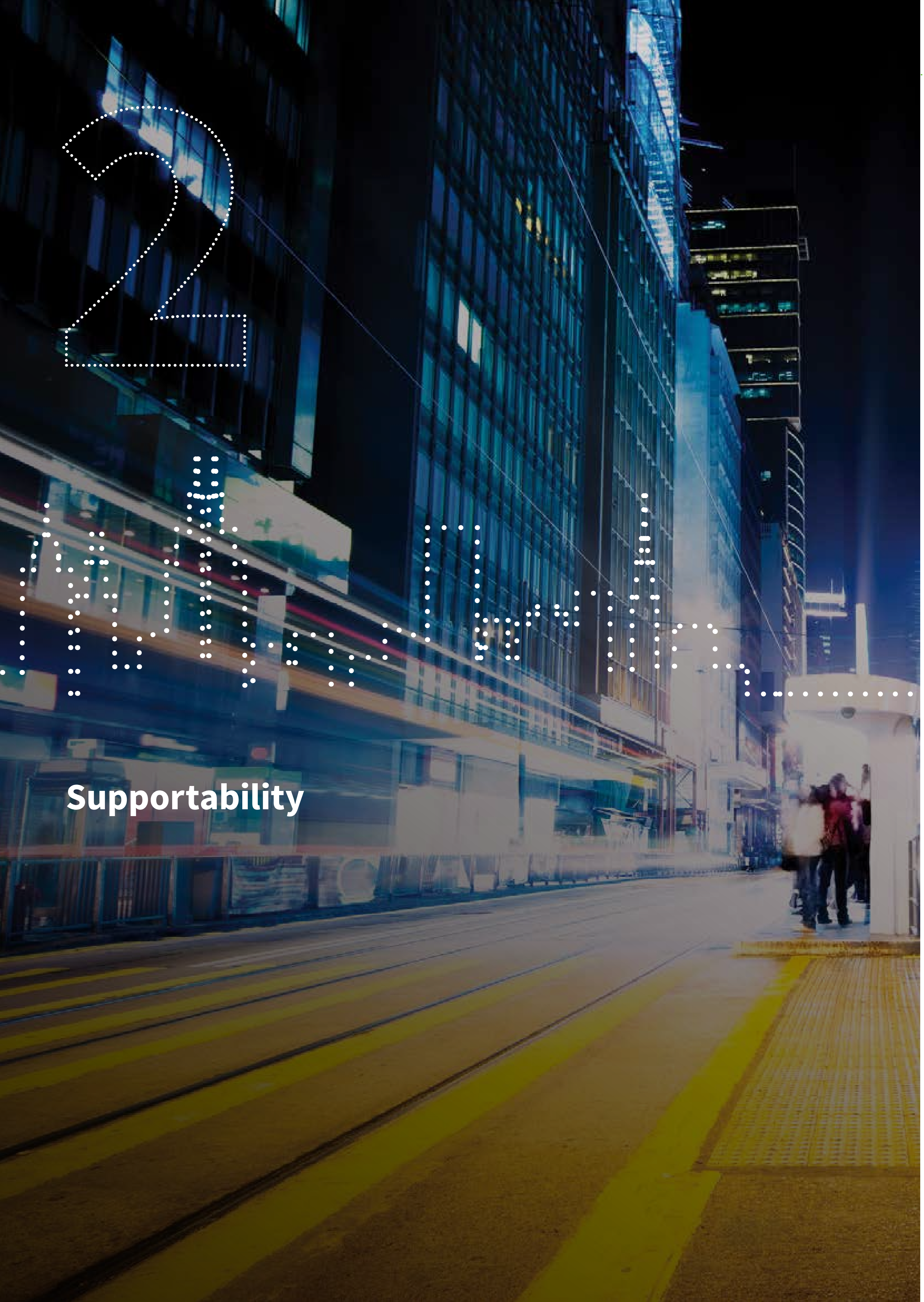
Figure 4: Percentage of devices by lifecycle stage



Over the last year, the percentage of obsolete devices in networks has remained the same, while the **percentage of ageing devices has fallen significantly from 44% to 33%**. At the same time, the **percentage of current devices has risen significantly from 47% to 58%**.

This means companies are no longer tactically replacing obsolete devices with like-for-likes, but they're replacing fully functional and supported ageing devices. We believe the reason is that they're pursuing architectural strategies to move towards the new generation of wireless and programmable devices, with the added advantage of lower support costs.

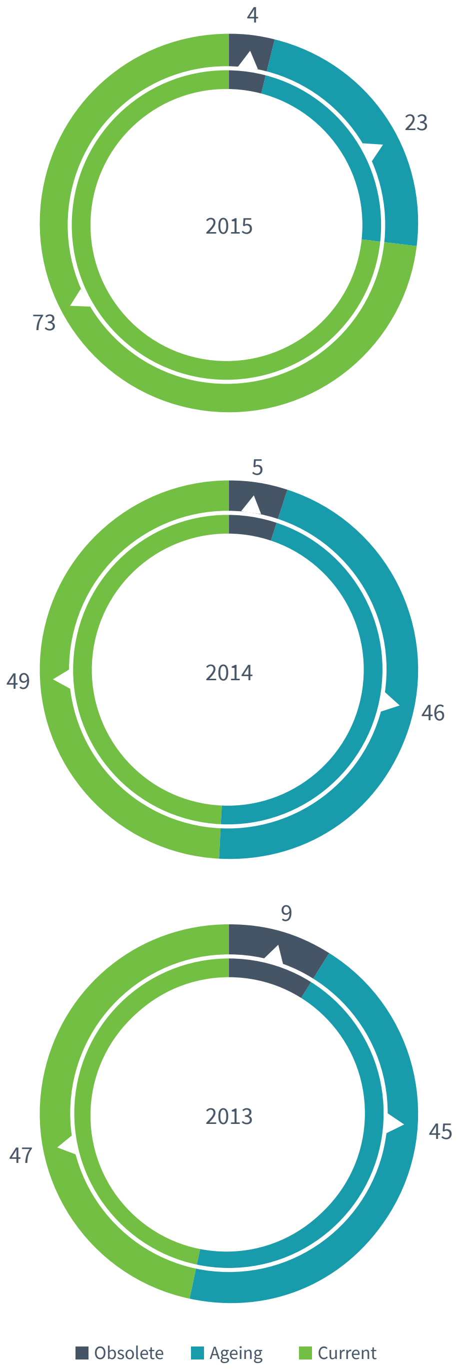




# 2 Supportability

## Supported networks are younger and more strategic

Figure 5: Lifecycle stage of devices under monitoring

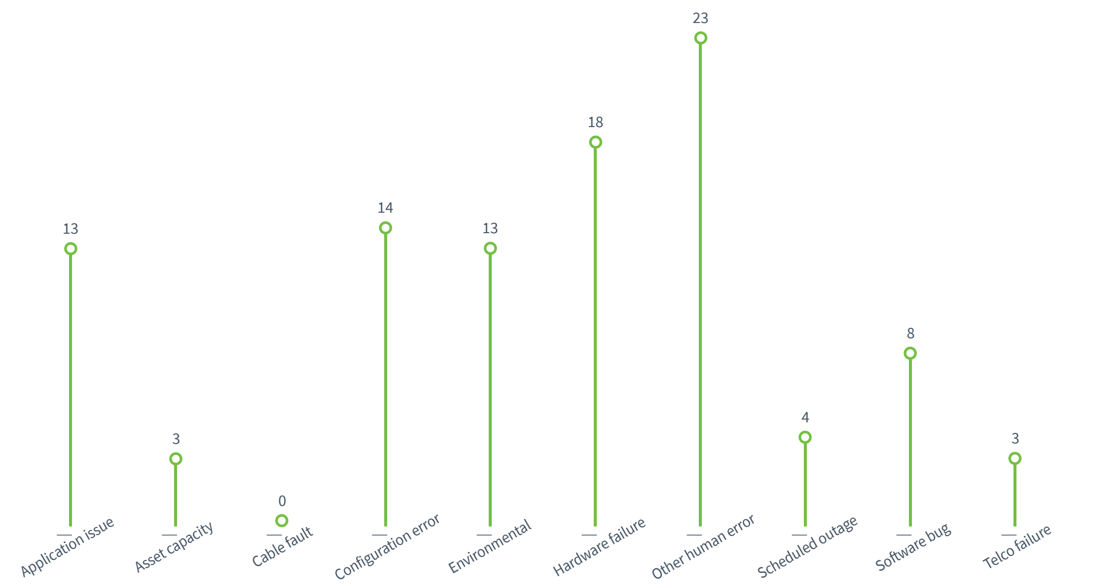


The reversal of the last five years' ageing trend is even more distinct in networks that are monitored. The **percentage of current devices on networks monitored by Dimension Data rose from 49% last year to 73%.** Most of the devices replaced were merely ageing, as opposed to obsolete.

This reflects the fact that we encourage our clients to strategically transform towards software-defined networks, with automated service, and consumption-based commercial models.

## Most incidents fall outside standard break-fix

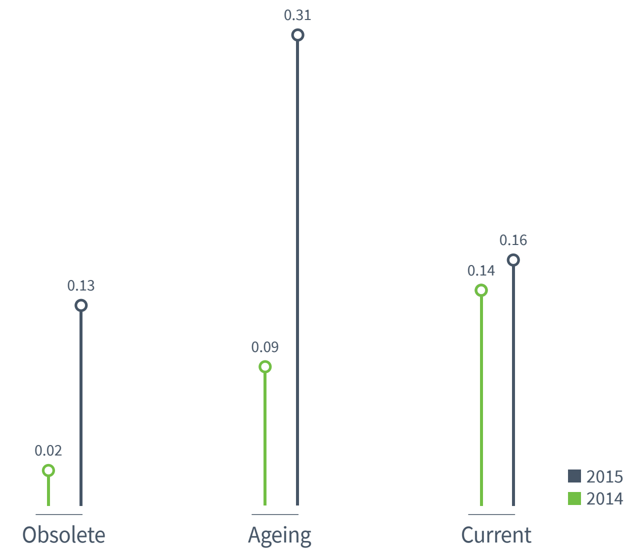
**Figure 6: Percentage of incidents by root cause**



**Only 26% of incidents fall under standard network support contracts** covering network hardware and software; the rest are due to telco failure, power outages, cable faults, configuration errors, or application issues. As 14% of incidents are caused by configuration error, and 23% to other human error, over one-third of incidents could be avoided with proper monitoring, configuration management, and automation.

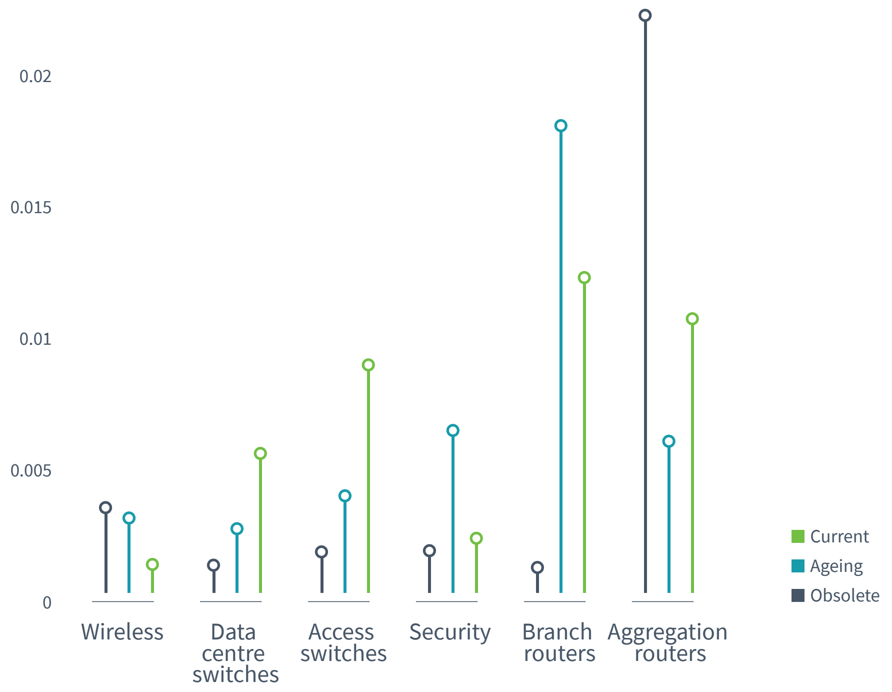
## Ageing devices are more likely to fail

**Figure 7: Percentage of failure rate by lifecycle stage**



This year we've seen an **increase in the number of incidents across the board**, and a pronounced **increase in the number of incidents on ageing devices**.

**Figure 8: Percentage of failure rate by device category**

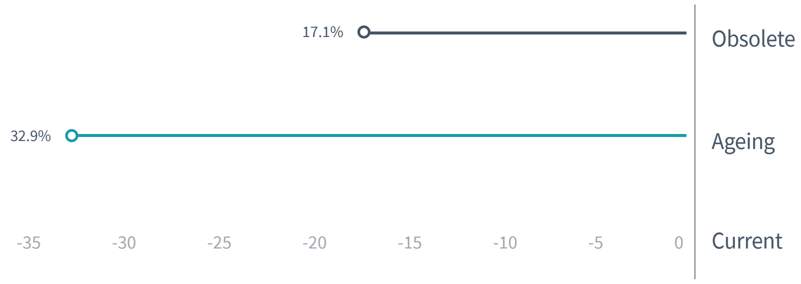


Ageing devices, especially branch office routers and obsolete aggregation routers are more likely to suffer failure.

Also, we have noticed a trend towards an increase in repair time for newer software-defined devices. This trend will need to be confirmed over time as a more relevant sample size becomes available.

# New devices take longer to repair

Figure 9: Mean-time-to-repair by lifecycle stage, percentage compared to current

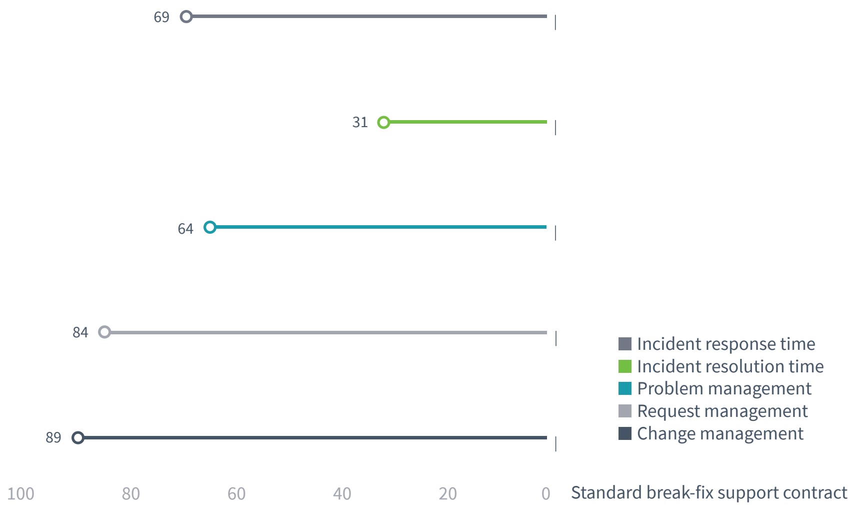


**Compared to current devices, obsolete and ageing devices take respectively 17.1% and 32.9% less time to repair.** Issues on new devices tend to be software-related. Because they're new, bugs need to be fixed by the vendor, and a new version of the software issued. This process pushes up the average time to fix on current devices.

Supporting obsolete devices is more labour-intensive. Often no like-for-like replacement is available for failed parts, and alternatives require careful manual installation and testing.

# ITIL process times are quicker on networks we manage

Figure 10: ITIL process time reduction on networks managed by Dimension Data



Change management is **89% faster** on **networks managed by Dimension Data versus non-managed**. Requests are handled **84% faster**. Problem management is **64% faster**. Incident response is **69% faster on networks monitored by Dimension Data** versus non-monitored.

Overall, **faults on networks monitored by Dimension Data** are repaired around **32% faster** than those on non-monitored ones, the same as last year.

### Why are changes 89% faster on managed networks?

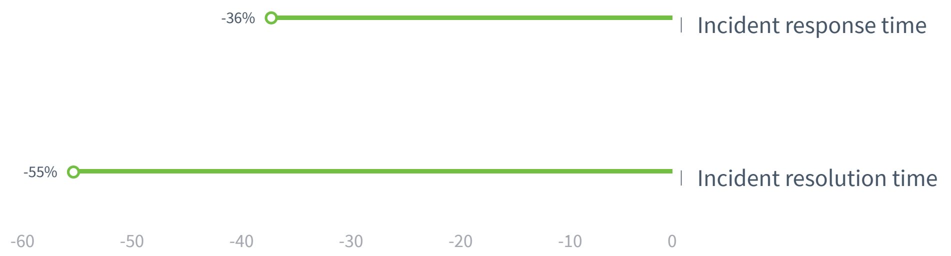
On **non-managed networks**, Dimension Data is likely to have a support contract on a particular device, but we aren't responsible for the surrounding environment. So the speed with which we can perform a change on the device is not within our control – we're dependent on the client, vendors, telcos, and other third parties.

When the network is under a **managed contract**, we **control the whole environment** in which the change is being made, so we can **co-ordinate all aspects** of the change within a defined time window, carry it out efficiently, and it's more likely to work the first time.

This is important to organisations, as changes are the second most common ITIL process after incidents, and make up a large proportion of their operating expenditure.

# Incident management is much faster with service desk integration

**Figure 11: Reduction in incident response and resolution times, with service desk integration**



Looking at networks monitored by Dimension Data, on networks with service desk integration, **incident response time is 55% faster**, and **incident fix time is 36% faster**, compared to networks with no service desk integration.

### What is service desk integration?

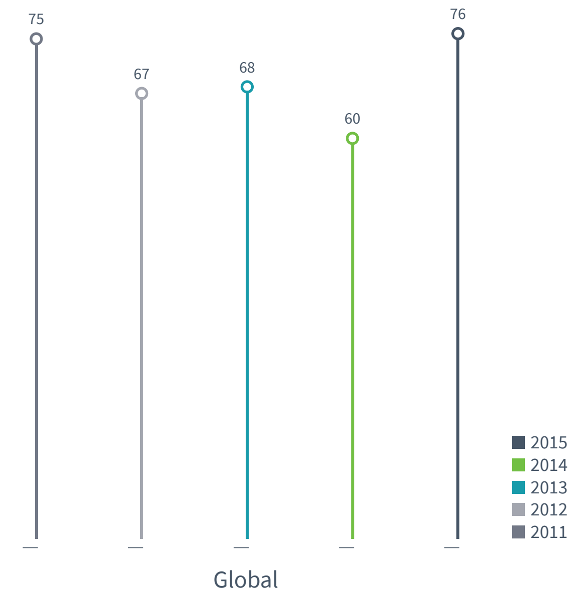
Service desk integration is our **joined-up platform for managing all support processes**, on **all networking technologies**, from all vendors, featuring:

- **remote monitoring**
- **automatic identification, diagnosis, and repair of faults**
- **automatic real-time exchange of ticket information with client and vendor systems**
- **root cause trend analysis for proactive problem avoidance**

# 3 Security

## Networks are less secure this year

Figure 12: Percentage of network devices with at least one security advisory, globally



This year, **76% of network devices have at least one known security advisory**, the highest figure in five years, and up from 60% in last year's Report.

**What's a security advisory?**

A notice issued by a manufacturer that they're **aware of a security vulnerability** on one of their products.

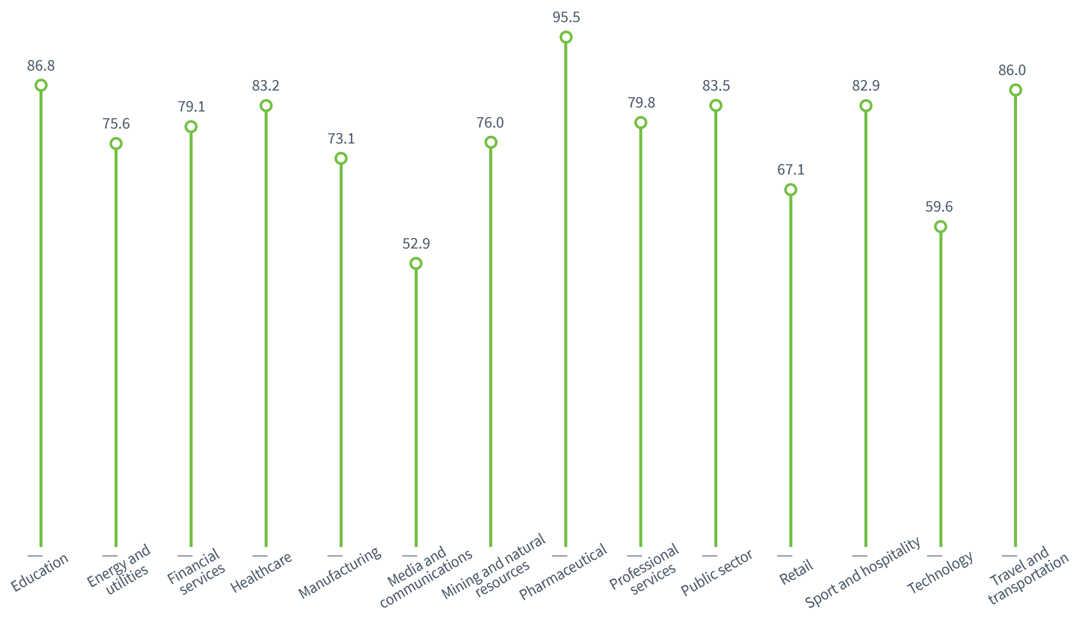
## Top 5 security advisories

Figure 13: Top 5 security advisories

| Title | Penetration rate | Severity | CVE | Published date | Last year's ranking |
|---|---|---|---|---|---|
| **TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products – IOS & IOS-XE – 109444** | 25.62% | High | CVE-2008-4609 | 8-Sep-2008 | 4 |
| **Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability – 108558** | 24.94% | High | CVE-2009-0631 | 25-Mar-2009 | 6 |
| **Multiple Vulnerabilities in OpenSSL Affecting Cisco Products – IOS** | 22.91% | Critical | CVE-2010-5298<br>CVE-2014-0076<br>CVE-2014-0195<br>CVE-2014-0198<br>CVE-2014-0221<br>CVE-2014-0224<br>CVE-2014-3470 | 5-Jun-2014 | – |
| **Cisco IOS Software Network Address Translation Vulnerabilities** | 22.91% | High | CVE-2014-2109<br>CVE-2014-2111 | 26-Mar-2014 | 5 |
| **Cisco IOS Software DHCP Denial of Service Vulnerability** | 21.01% | High | CVE-2013-5475 | 25-Sep-2013 | – |

# Some industries are getting more secure, others more vulnerable

**Figure 14: Percentage of devices with at least one security advisory, by industry**



### Retail networks are getting more secure

According to NTT's Global Threat Intelligence Report 2016, the retail sector topped the list of all cybersecurity attacks on all industries. That's because the retail sector processes large volumes of personal information and credit card data making it attractive to hackers. The sector now appears to be responding.

This year's Network Barometer Report reveals that the percentage of network equipment with security vulnerabilities in the retail sector has fallen to 67% (from 81% last year).

### Manufacturing networks are getting less secure

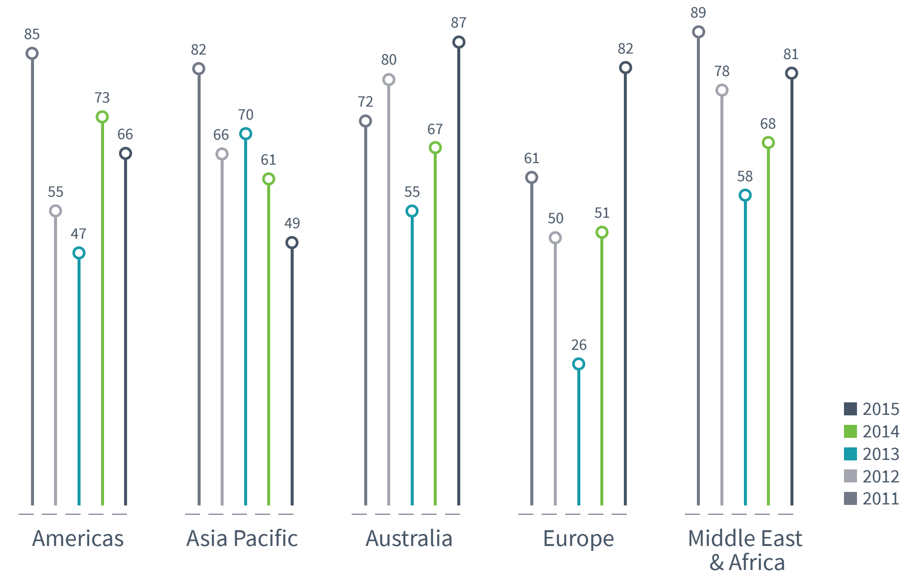
The percentage of devices with vulnerabilities in manufacturing networks has risen dramatically from 47% last year to 73% this year. The NTT Global Threat Intelligence Report 2016 ranks the sector as the fifth most likely to be victim of a cyberattack. We see a potential risk that, unless the sector strengthens its security posture (patching), it could suffer a rise in security breaches, especially as the industrial Internet of Things becomes more pervasive.

**NTT's Global Threat Intelligence Report provides *insights on the latest security threats* and *offers recommendations* for protecting organisations from cybersecurity incidents.**

download the executive's guide

# Network security depends on both refresh and patching

**Figure 15: Percentage of devices with at least one vulnerability, by region**



In Europe, **network vulnerability has increased significantly** over the last three years, **from 26% in 2014, to 51% in 2015, to 82% this year**. Network vulnerability has **also risen in the Middle East & Africa** over the last three years. In **Australia, 87% of network devices** have at least one known vulnerability. In **Asia Pacific and the Americas**, networks are respectively a **little less vulnerable**, and less vulnerable than last year.

Network security depends on both refresh and patching. New devices have fewer vulnerabilities, so just by refreshing, you make your network more secure. For example, in the Americas we've seen an increase in device refreshes, and a corresponding fall in security advisories.

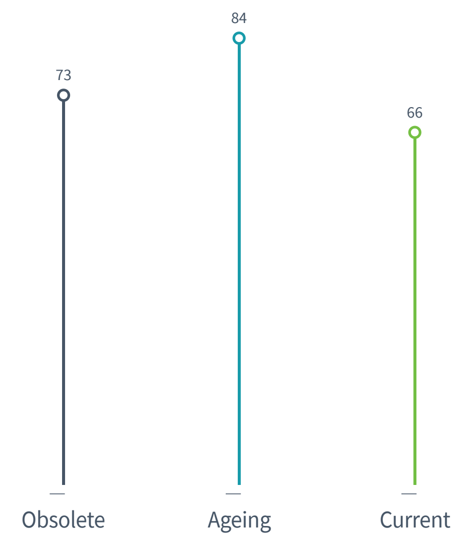
Network device security also depends on patching. In Asia Pacific the marked decrease in vulnerability outstrips the refresh rate, which is also due to diligent patching. By contrast, in Europe and Australia, network equipment is being refreshed, but vulnerabilities have nonetheless increased. This is attributable to less diligent patching.

### How can refreshed networks be less secure?

Because a device and its software are new, there'll be an **initial 'settling-in time'**, in which **vulnerabilities will be discovered**, and the patching requirements will be more frequent and intense. We see a number of clients, particularly in Europe, putting **more of their investment into strategic refresh of network equipment**, and less into day-to-day operational maintenance. By failing to keep up to date with software patches on their new equipment, they **risk making their new networks less secure**.

## Ageing devices are less secure only because they're not being patched

Figure 16: Devices with at least one vulnerability, by lifecycle stage



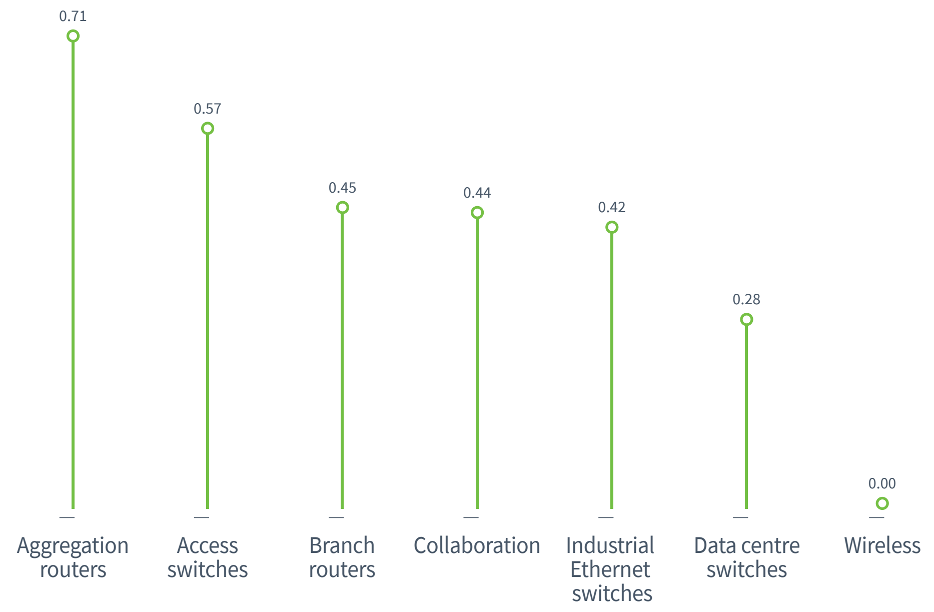
**Current devices have the lowest level of vulnerabilities**, at 66%. What's **surprising is that ageing devices have the highest, at 84%**.

We'd expect to see fewer vulnerabilities on ageing devices compared to current ones, if they were being patched. The fact that ageing devices have more vulnerabilities than current ones is because companies are not installing the security patches that vendors are issuing.

The high number of obsolete devices with vulnerabilities (73%) is to be expected. Since they're past end-of-support, the software vendors are no longer releasing security patches for them.

## Vulnerabilities are more prevalent in some parts of the network than in others

Figure 17: Average number of vulnerabilities per device, by device category



This chart shows which types of network device are most vulnerable. It shows, for example, that aggregation routers have an average of 0.71 vulnerabilities per device, which is another way of saying that any given aggregation router is 71% likely to have a vulnerability.

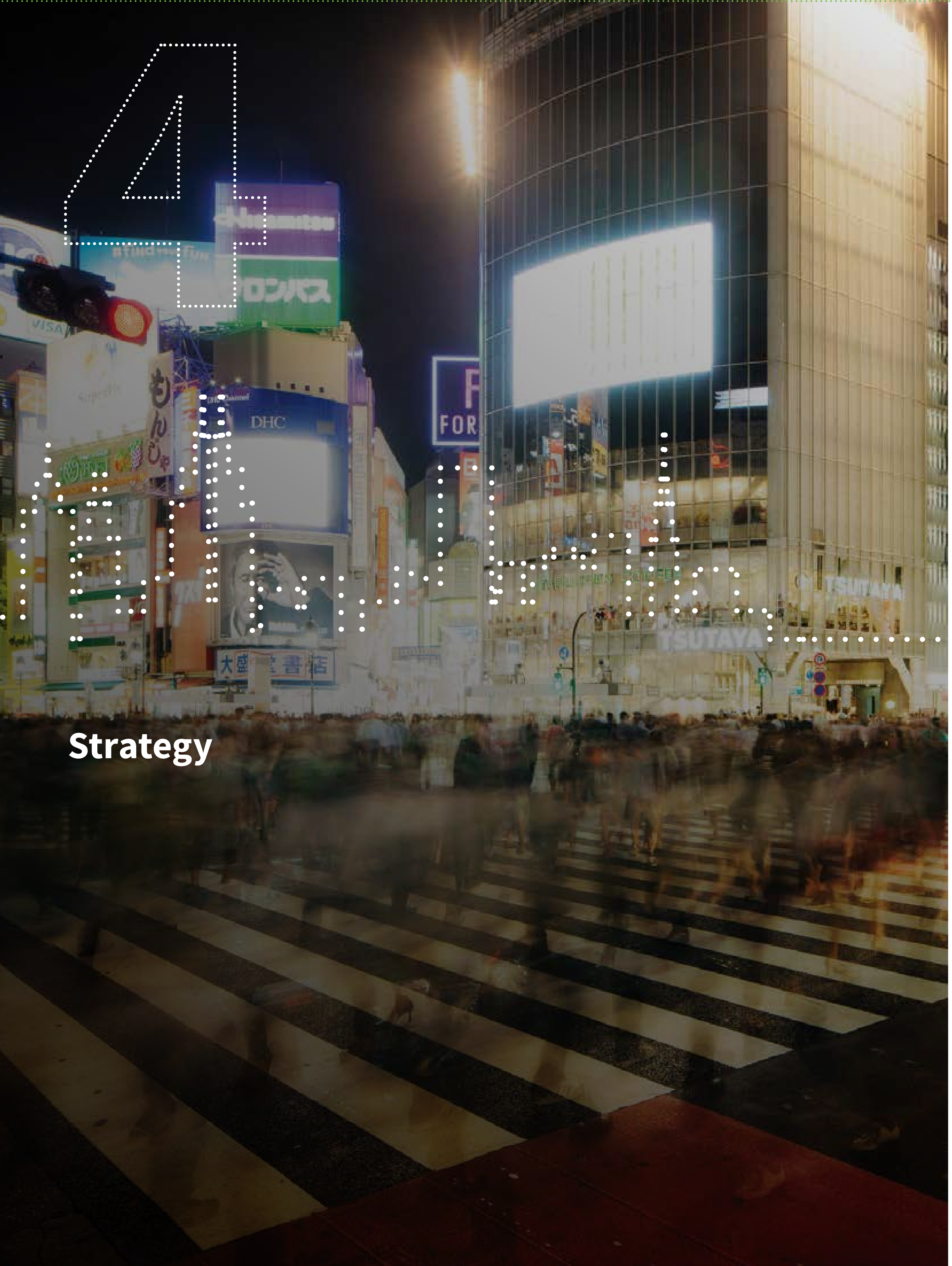
Aggregation routers and access switches are the most vulnerable device categories.

The high number of vulnerable industrial Ethernet switches is also significant. These switches are typically used in manufacturing and industrial environments where a compromise could have an adverse impact on the safety of employees or the continuity of production.

We've seen a welcome reduction in the number of vulnerable data centre switches and wireless devices since last year, due to patching a refresh cycles.

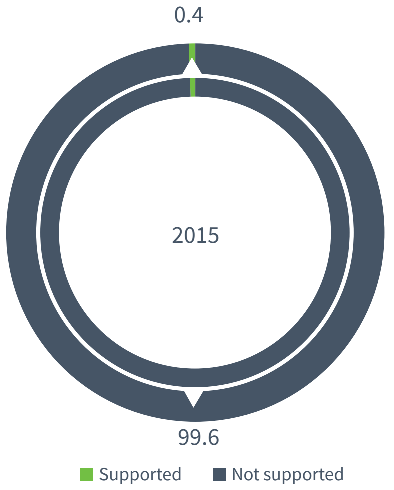
### How should you prioritise patching resource?

Determine the **business criticality of the applications** and **business functions supported** by each device category and **apply patching resource** according to the areas with **most business impact**.



## Software-defined networking is coming soon, but not just yet

Figure 18: Software-defined WAN readiness



In 2015 less than half a percent (0.4%) of devices could support software-defined networking (SDN) (this figure is mainly Cisco iWAN products, but also those of other major manufacturers like Riverbed and Viptela, and various start-ups and niche players).

We see intense market interest and testing, and expect widespread adoption of software-defined WAN technologies which will lead to a migration of data centre aggregation routers and branch/edge routers in the coming year.

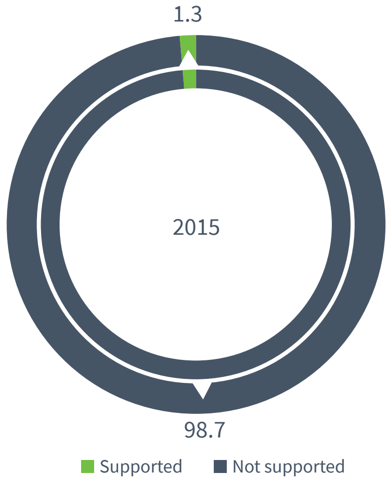
### What are software-defined WANs?

This approach to wide area networking **helps manage the new traffic patterns in cloud architectures**. Before cloud, data basically travelled back and forth between the user and their data centre. With cloud, the application could be anywhere. So the **priority becomes offloading cloud traffic from the corporate WAN** as close as possible to the user **to give a good user experience**. Software-defined networks make it easy to do this. They also give **more visibility of bandwidth utilisation** and **carrier spend**.

### What's holding back adoption?

Traditionally, telcos bundled edge routers with carriage, but software-defined WANs decouple the router from the telco. We suspect companies are **simply waiting until the end of their present telco contracts before refreshing equipment**. There's also a sense of 'wait and see' in the market. The technology is new, and companies seem to be holding off investing until wrinkles are ironed out and opex savings proven.

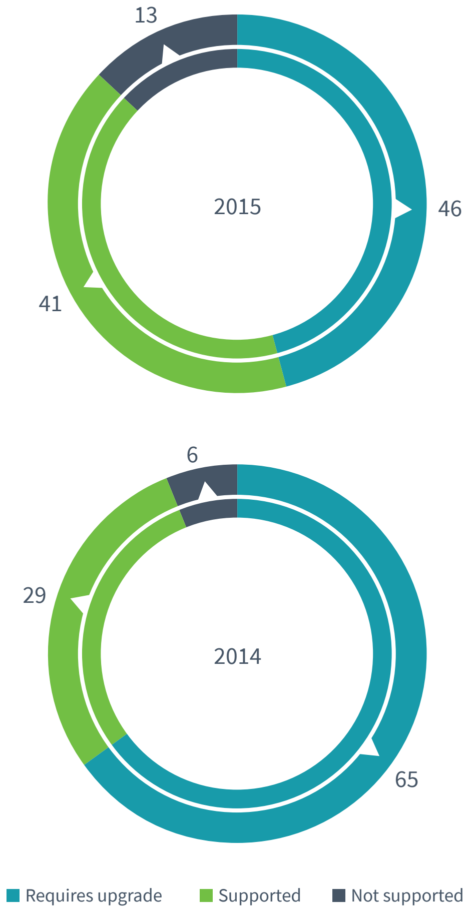
**Figure 19: Data centre network automation readiness**



Software-defined data centre networks are also still embryonic, with only 1.3% of data centre switches currently SDN-ready. We're starting to see companies purchasing SDN-ready data centre equipment, with software-defined networking in mind (and partly because it's cost-effective), but they're not yet widely adopting automation software.

## There's been a big rise in devices supporting IPv6

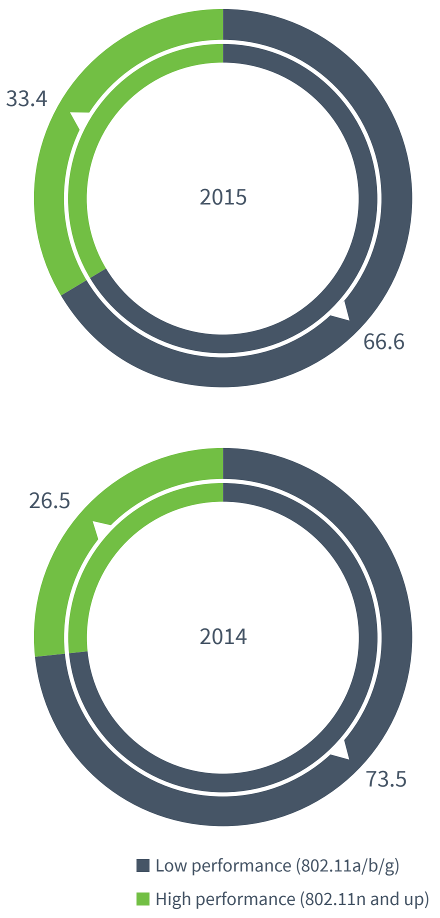
**Figure 20: Percentage of devices supporting IPv6**



The **percentage of devices supporting IPv6 has risen from 21% last year to 41% this year**, due to the increase in current devices in networks. This allows organisations with newer networks to support their digitisation strategies by enabling connectivity for the Internet of Things, big data, analytics, and containerisation.

## Organisations are adopting newer wireless standards

Figure 21: Percentage of access points supporting newer wireless standards (wireless capabilities)

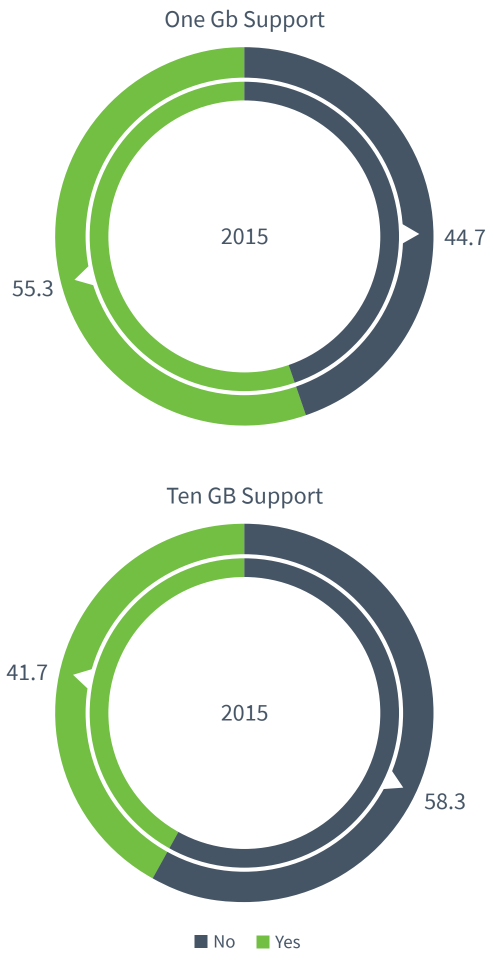


The percentage of access points supporting wireless protocol 802.11n and up **rose from 26.5% in 2015's Report to 33.4%** this year. Companies need these access points to handle the higher throughput required by workplace mobility and collaboration strategies.

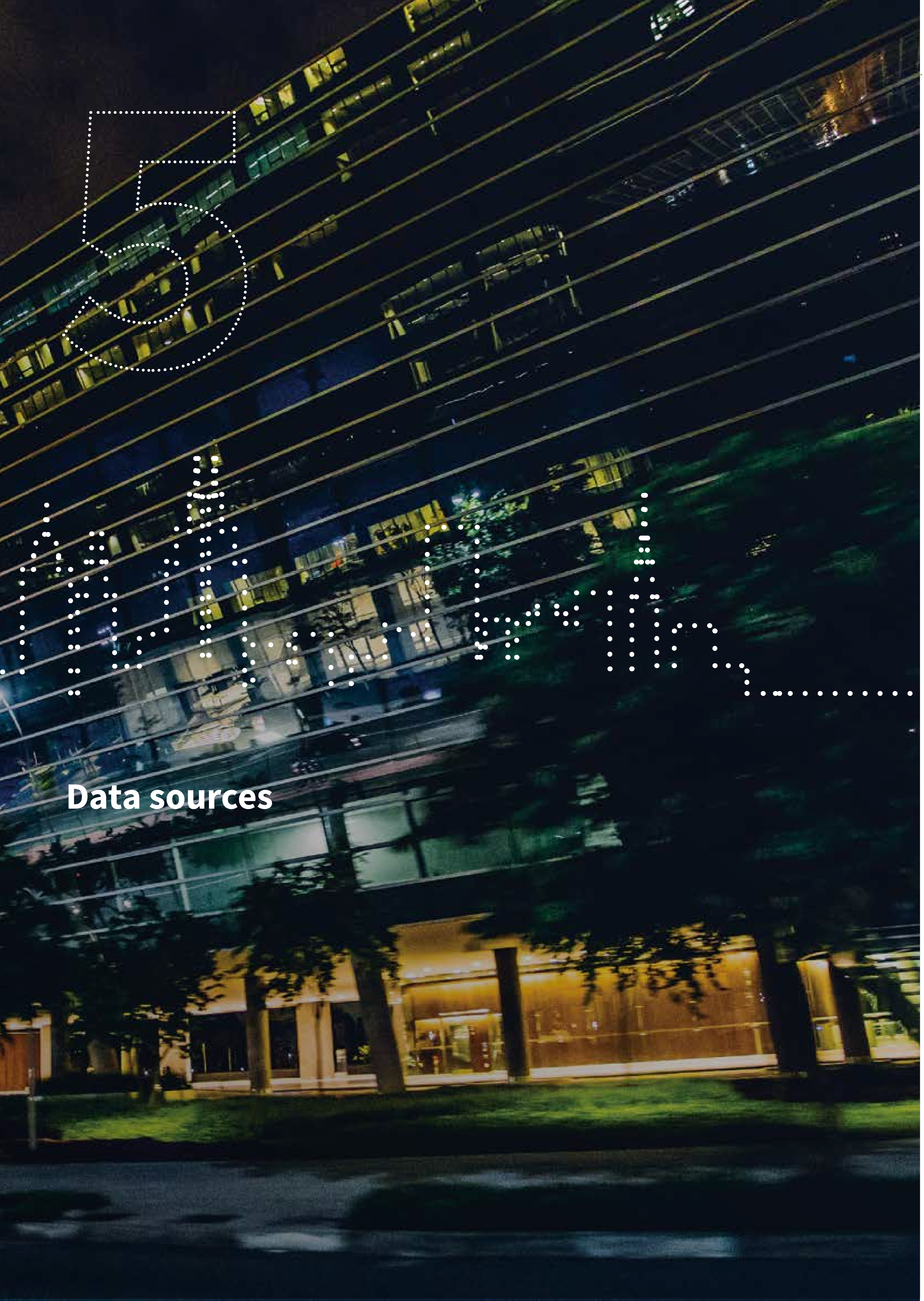
We expected this to be higher given the rise of workplace mobility and believe many companies are incorrectly assuming their existing wireless infrastructure will be able to support the large increase in wireless traffic required in the modern workplace.

## They're also buying plenty of capacity

Figure 22: Percentage of access switches by bandwidth



In the past 12 months, there's been an **18-percentage point increase in switches** with **10Gb uplinks**, and a **similar increase in switches** with **1Gb-capable access points.** This is to accommodate the higher throughput requirements of the collaboration applications used in modern workplaces.



# 5 Data sources

## About Dimension Data

Dimension Data uses the power of technology to help organisations achieve great things in the digital era. As a member of the NTT Group, we accelerate our clients' ambitions through digital infrastructure, hybrid cloud, workspaces for tomorrow, and cybersecurity. With a turnover of USD 7.5 billion, offices in 57 countries, and 31,000 employees, we deliver wherever our clients are, at every stage of their technology journey. We're proud to be the Official Technology Partner of Amaury Sport Organisation, which owns the Tour de France, and the title partner of the cycling team, Team Dimension Data for Qhubeka. Visit us at dimensiondata.com

## About our Technology Lifecycle Management Assessment

This global technology assessment discovers installed assets on the network, identifies their lifecycle status, determines maintenance coverage, and flags potential security vulnerabilities as well as configuration errors.

The assessment results help you to align your technology infrastructure with best practices for configuration, security, and patch management, thereby ensuring that you're not exposing your organisation to unnecessary risk.

The technology lifecycle data used in the Network Barometer Report is gathered from these automated assessments.

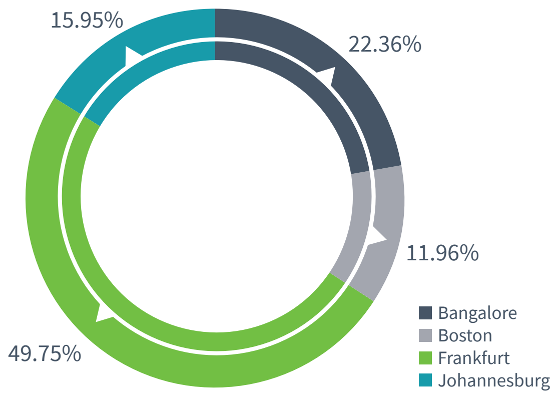
**Figure 23: Number of assessments by country**

| Country | 2015 |
|---|---|
| Algeria | 3 |
| Asia Pacific | 2 |
| Australia | 51 |
| Austria | 8 |
| Belgium | 3 |
| Botswana | 2 |
| Brazil | 16 |
| Canada | 1 |
| Chile | 2 |
| Czech Republic | 16 |
| France | 10 |
| Germany | 9 |
| Hungary | 5 |
| India | 36 |
| Italy | 5 |
| Japan | 3 |
| Kenya | 3 |
| Korea | 2 |
| Luxembourg | 1 |
| Malaysia | 4 |
| Mexico | 3 |
| Netherlands | 1 |
| New Zealand | 5 |
| Philippines | 2 |
| Poland | 2 |
| Portugal | 3 |
| Saudi Arabia | 1 |
| Singapore | 1 |
| Slovakia | 4 |
| South Africa | 59 |
| Spain | 9 |
| Switzerland | 15 |
| UAE | 2 |
| UK | 10 |
| USA | 21 |

Figure 24: Percentage of devices by country

| Country | 2015 | Country | 2015 | Country | 2015 |
|---|---|---|---|---|---|
| Algeria | 0.17% | Hungary | 0.74% | Poland | 0.28% |
| Asia Pacific | 0.07% | India | 0.85% | Portugal | 0.17% |
| Australia | 23.23% | Italy | 0.80% | Saudi Arabia | 0.06% |
| Austria | 0.60% | Japan | 3.17% | Singapore | 0.18% |
| Belgium | 1.22% | Kenya | 0.74% | Slovakia | 0.62% |
| Botswana | 0.17% | Korea | 0.48% | South Africa | 10.95% |
| Brazil | 8.38% | Luxembourg | 0.07% | Spain | 0.75% |
| Canada | 0.06% | Malaysia | 3.77% | Switzerland | 4.22% |
| Chile | 0.51% | Mexico | 0.26% | UAE | 0.29% |
| Czech Republic | 2.86% | Netherlands | 2.91% | UK | 3.44% |
| France | 2.23% | New Zealand | 1.65% | USA | 20.91% |
| Germany | 2.07% | Philippines | 1.12% | | |

Figure 25: Configuration item distribution by Global Service Centre (percentage)



## What are the implications of the Network Barometer Report for your organisation?

Is your network digital business ready? Please contact us to discuss the implications of the findings in this Report for your own organisation's network, and how your network supports your digital business ambitions.

**dimensiondata.com/networkbarometer**