Future Connectivity Guidance Smart Network Management v1.1

Document management

Revision History

Version	Date	Summary of Changes	Author
1.00	08/10/2024	Published document	Farrpoint Ltd.
1.01	22/10/2024	Cover sheet and document management added	NHS England

Future Connectivity Guidance

The Future Connectivity Programme's Connectivity Hub produces, sources and shares expert technical knowledge to support the NHS to plan and implement the right connectivity for local needs.

To target and prioritise the right blend of system knowledge and expert independent advice, we engage with health and care organisations, directly and through surveys, to understand their connectivity challenges and procure and publish externally independent commissioned reports into priority topics.

This report was produced following the selection of a supplier via an open tender procurement process run according to PCR2015 during 2024. Under the terms of the contract between NHS England and the supplier in question, the Intellectual Property Rights (IPR) of the report and any associated material sits solely with NHS England who reserve the right to adapt and amend the published version of the report.

Any enquiries on the content of the report should be directed to the NHS England Future Connectivity Programme nhsdigital.future.connectivity@nhs.net

Smart Network Management Report

This document is an independent report into Smart Network Management in the NHS, commissioned by the Future Connectivity programme and produced in collaboration with Farrpoint Ltd.

The content is intended to be supplier and vendor agnostic, which means NHS England do not endorse any specific companies, innovations, or approaches. Any mention of, or link to, a specific supplier or product does not constitute an endorsement from NHS England.

For clarity any recommendations made in this report are those of the report authors and do not represent any mandatory policy, or requirement from NHS England.

NHS England: Future Connectivity

Smart Network Management

June 2024

FarrPoint

Contents

1.	Introduction	3
1.1	Background	3
1.2	Purpose of this Report	3
2.	What is Smart Network Management?	5
2.1	Definition	5
2.2	What do Manufacturers Call Smart Network Management?	7
3.	Why Use Smart Network Management?	9
3.1	The Challenge	9
3.2	How Smart Network Management Can Help	11
4.	Case Studies	21
4.1	Calderdale & Huddersfield NHS Foundation Trust	21
4.2	Milton Keynes University Hospital NHS Foundation Trust	22
4.3	West Suffolk NHS Foundation Trust	23
4.4	Loughborough University	24
5.	Market Overview	26
5.1	HPE (Aruba & Juniper)	26
5.2	Cisco	29
5.4	Extreme Networks	31
5.5	Future Developments	32
6.	Smart Network Management Deployment	34
6.1	Technology Considerations	34
6.2	Other Deployment Considerations	35
6.3	Key Questions for Suppliers	36
Glossary		38

1. Introduction

1. Introduction

1.1 Background

Health organisations are increasingly reliant on digital services and data to support healthcare delivery, building and facilities management, administration, patient services, research, and a range of other applications. These services are delivered to a wide range of users on a variety of client devices.

Wired and wireless networks are used to deliver all these digital services and are seeing increasing levels of demand and need to be reliable and secure. Historically, the response to increased demand on a network was to provide more speed and capacity; however, increasingly, there is a need for networks to differentiate between applications, client devices, users and locations and to use this information to offer an appropriate level of service and access.

The increased complexity of networks, the applications and devices that rely on them, and cyber security threats mean that traditional manual network and device provisioning and management are likely to become unsustainable. Resource is not available to manage and monitor the associated range of configurations, service levels, and security risks. Smart Network Management offers a range of functionality that helps address these issues, using management and visualisation tools, automation and, increasingly, artificial intelligence, to deliver, monitor and manage network services in an increasingly complex and demanding environment.

1.2 Purpose of this Report

This report has been commissioned by NHS England Future Connectivity Programme[1]. It is aimed at Integrated Care System (ICS) and NHS Trust Chief Information Officers and their Network Managers & Service Managers.

The report defines Smart Network Management and describes how it can help health organisations ensure their networks continue to offer high levels of service and availability despite increasing demand and complexity. It also demonstrates the operational and cost efficiencies Smart Network Management can deliver, with suppliers quoting operational savings of 20 – 50% by using network infrastructure and support resource more effectively.

This report is intended to provide an initial introduction to Smart Network Management and an overview of its application and benefits in a health environment.

The detail in this report has been obtained using a review of documentation and interviews with equipment manufacturers and health organisations. We are grateful for the support these manufacturers and organisations provided.

Where this report references a specific manufacturer's product or service, this should not be interpreted as a recommendation. All such references are for indicative purposes only.

[1] https://digital.nhs.uk/services/future-connectivity

2. What is Smart Network Management?

2. What is Smart Network Management?

2.1 Definition

The term Smart Network Management does not describe a specific network technology or product. Instead, it describes a range of features and functionality delivered using visualisation tools, automation and artificial intelligence that simplify and automate the delivery, monitoring and management of network services in an increasingly complex and demanding environment.

From a network user/client perspective, Smart Network Management ensures they are provided with an appropriate level of network service and access based on user type, application, client device and location.

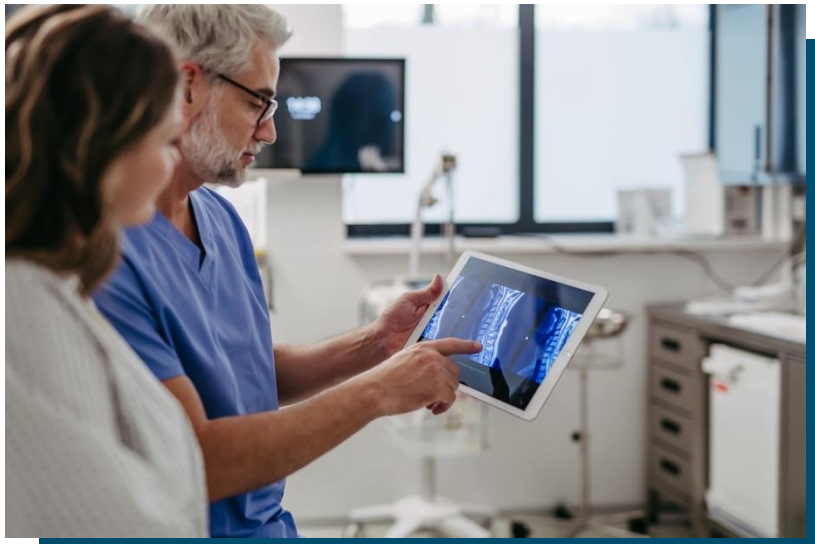
From a network team perspective, Smart Network Management improves visibility and efficiency, providing network teams with tools and information to connect and configure client devices, monitor and manage network and application performance, identify and resolve network issues, and keep the network secure.

Increasingly, applications and data are hosted in the cloud, meaning several networks, services and suppliers are involved in ensuring a reliable user experience. Smart Network Management can help monitor and manage these, providing end-to-end visibility of both on-premise applications and cloud services. Smart Network Management solutions are usually (though not exclusively) provided as a cloud-based service.

Smart Network Management does not replace existing technologies or functionality, such as Software Defined Networking (SDN), Intrusion Detection (IDS), Secure Access Service Edge (SASE), 802.1x, or Zero Trust Network Access. Equally, use of all these technologies is not a prerequisite of implementing Smart Network Management. Instead, Smart Network Management describes a set of tools and functionality that can be used to monitor and manage a network that often uses one or several of these kinds of technologies.

Smart Network Management does not necessarily require new network infrastructure, in many cases Health Organisations will be able to use the elements of functionality it offers to better manage their existing infrastructure.

Figure 1 summarises some of the headline Smart Network Management features and functionality. The next section of this report provides further detail on this functionality and the challenges it can help to address.



Guarantee network and application service	• Differentiated level of service based on application, user, device, location. • End-to-end monitoring of application and network performance. • Automated detection of issues - improve network and application availability.
Reduce network management and administration overhead	• A complete view of network and application performance, network use, application use – wired, wireless, third party networks and cloud-based services. • Automatic detection and alerting of network or application performance issues, including location-based issues. • Device fingerprinting. • Suggested remediation of network and application issues. • Automatic raising of support tickets.
Reduce network installation and configuration overhead	• Automatic provisioning of client devices and network configuration. • Automatic configuration of network devices. • Network modelling.
Strengthen cyber security and data protection	• Real-time threat identification and network response. • Role, device, location based access to applications and services. • Detection and isolation of rogue clients and network devices. • Real-time updates on threats.
Sustainability and Net Zero	• Automatic switch to low power configurations. • Zero touch set up – minimise travel time for staff support, installation and associated carbon footprint. • Network design tools to enable low power connectivity for IoT devices.
Commercial	• Maximising existing infrastructure and digital investment. • Reduction in power costs. • Minimising equipment required. • More efficient use of network team resource.

Figure 1: Examples of Smart Network Management Features and Functionality

2.2 What do Manufacturers Call Smart Network Management?

As mentioned above, this report uses the term Smart Network Management to describe a range of features and functionality. This is used as a manufacturer-agnostic term. Manufacturers themselves use a range of names to refer to this functionality. These can include 'next-generation networking', 'AI Networking', Artificial Intelligence for IT Operations (AIOps)', 'Software Defined Access' or 'Advanced Networks'.

Not all manufacturers will offer all of the functionality detailed in this report. In addition, manufacturers' Smart Network Management offerings continue to develop, meaning new and enhanced functionality is being regularly released. An example of this is the incorporation of artificial intelligence and machine learning. Some capability is already offered by manufacturers, however, this is likely to increase in the near future given the opportunities the technology offers to process the vast amounts of data available to provide insights into network usage, performance issues and resolution, and to improve cyber security.

Section 5 contains details of the Smart Network Management offering from a number of network equipment providers. This includes details of the product and feature naming used by these manufacturers.

3. Why Use Smart Network Management?

3. Why Use Smart Network Management?

3.1 The Challenge

3.1.1. Increasing Demand and Complexity

Health organisations are increasingly reliant on digital services and data to support healthcare delivery, building and facilities management, administration, patient services, research, and a range of other applications (Fig. 2 provides some examples of common digital services supported by health networks).

These digital services support a complex range of users, client devices, and use cases. The network cannot treat all connections equally. Instead, it must ensure that each device and application receive an appropriate level of service and that access to services and data is controlled to manage increasing cyber security and data protection threats.

Common Digital Services Supported by Health Networks (Examples)

- Patient Management Systems / Electronic Patient Record System
- Support for smart / connected medical devices and scanners
- Unified Messaging and collaboration applications, e.g. Microsoft Teams, videoconferencing, IP Telephony, Microsoft365.
- Picture Archiving and Communication System (PACS)
- Building management system controls and sensors
- Internet of Things devices – e.g. refrigeration monitors, pharmacy tracking
- Asset / device location tracking
- Patient and visitor Internet access
- Network / Internet access for partner organisations

Figure 2: Examples of Digital Services Commonly Supported by Health Networks

Network use cases vary significantly and have the potential to conflict. High priority, life-critical applications, need guaranteed network availability and to ensure that performance is not degraded by lower priority (and potentially high bandwidth) applications such as patients accessing streaming media. Some applications, such as Picture Archiving and Communication System (PACS), consume very large amounts of bandwidth, while other applications, such as asset tracking, can have a very large number of connected devices with each generating very little data.

Users can access digital services using multiple devices. They are increasingly seeking mobility, meaning these devices are laptops, tablet devices, and smartphones, including personal devices. The network needs to determine the type of device being used and potentially its location and apply appropriate network and application access controls.

Multiple users may access a single device, such as devices located in wards and other shared areas. Again, appropriate network and application access needs to be applied based on who is using a device.

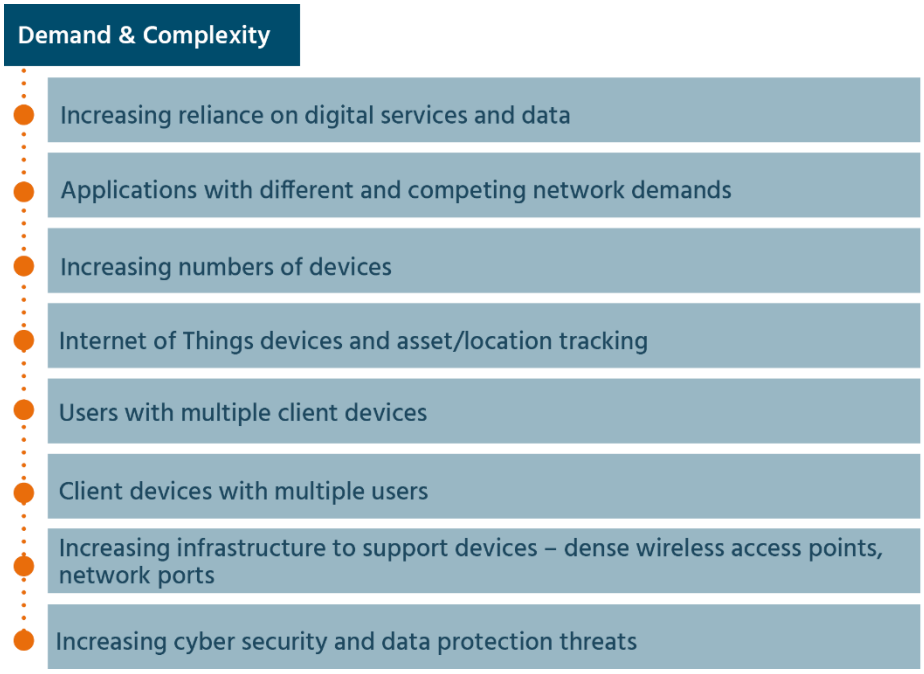


Figure 3: Examples of Demand and Complexity Impacting the Management of Health Networks

3.1.2. The Challenge Is Not New

These challenges are not new. Historically, increasing network demand has been addressed by providing more capacity: increasing network ports and wireless access points, and increasing access and core bandwidth. Quality of Service, VLANs, 802.1x and other controls have been used for many years to identify users and offer differentiated levels of network service and access.

In the past, these upgrades and controls have been completed manually by network teams. These teams are then also responsible for monitoring and managing the network and for responding to network incidents. However, the large and increasing number and the variety of network connected devices and the range of applications and services they access make this traditional manual approach to network provisioning, monitoring and management increasingly time-consuming and complex (Fig. 3). Budget pressures mean that seeking additional network team resources to address this increasing manual workload is usually not an option.

Smart Network Management functionality uses a range of visualisation tools, automation and artificial intelligence to help reduce this burden, simplify network management, keep networks available and secure, and ensure network users get the access and level of service they require. A later section of this report provides case studies of health organisations already using this functionality to manage complex IT infrastructures.

Figure 4 provides a high-level view of the development of network management functionality. Historically, management used manual processes and offered limited insights into network use and performance. Developments introduced a range of tools providing management and insight over elements of the network, and application level monitoring provided visibility of the end-user experience. However, these tools were often standalone, and so provided a siloed view. Smart network management is the third step shown in Figure 4, bringing together the management tools to provide more complete visibility and control over network

and application performance. Although automation is also included, at this point, the use of, and trust in, AI and machine learning is still developing and so is shown as the basis of the next development of Smart Network Management functionality.

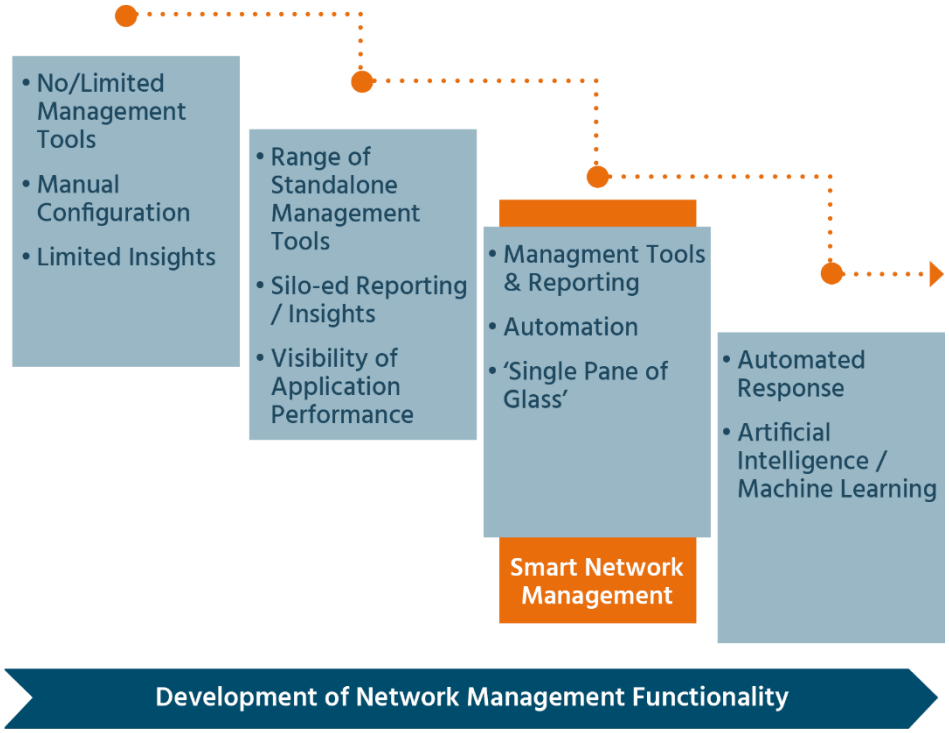


Figure 4: Development of Network Management

3.2 How Smart Network Management Can Help

3.2.1. Delivering Differentiated Network Access and Performance

Smart Network Management functionality can help identify and deliver the appropriate level of network service and access a connected client should receive. These client devices are increasingly mobile, with reliable and high-quality wireless coverage being required throughout buildings.

Policy for network access and level of service can be defined based on factors such as role, device type, posture, user group, and location. This allows, for example, high-priority applications, such as Electronic Patient Records, to be prioritised over patients' streaming media.

Device access can be restricted, for example, with IoT devices only being able to connect to their associated application or guest/patient access restricted to Internet access and with limited bandwidth.

Again, these controls are not new. However, Smart Network Management tools reduce the overhead associated with applying the controls, allowing policy to be defined once and be applied automatically as devices connect to the network, rather than requiring manual configuration of the client or network.

Machine learning is used by some manufacturers to support this functionality, using characteristics such as MAC address, application access, and traffic patterns to identify and classify devices and apply appropriate policies. Services[2] are available that apply this machine learning to data lakes obtained from a large customer base and across a range of locations, offering near real-time information on device identification, classification, as well as any associated threats.

[2] Example: https://cylera.com/solutions/use-cases/threat-response/

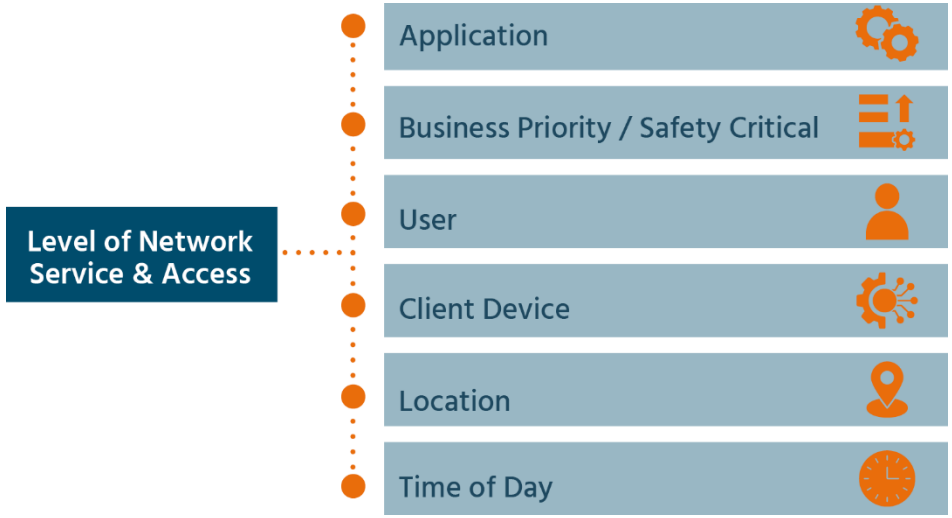


Figure 5: Examples of factors determining the level of Network Service and Access Offered to a Device

The level of network service and access offered to clients can be granular, based on a combination of factors (Fig. 5). This access often uses a zero-trust security approach (examined further in a later section), only providing access to the data and services required by a client:

- **Application**: Client access can be restricted to defined applications and services;
- **Business Priority / Safety Critical**: High-priority or safety-critical applications and services can be prioritised to ensure a high level of application performance and availability;
- **User**: Authenticated users, partner organisations, guests, patients, and untrusted devices can be provided with different levels of access;
- **Client Device**: Different access can be provided for NHS provided clients, connected devices such as MRI scanners, IoT devices, staff personal devices, and untrusted devices;
- **Location**: Different access can be provided to devices in different buildings or within different parts of a building;
- **Time of Day**: Access and level of service can be varied throughout the day, for example, allowing greater bandwidth to patient streaming when clinical demand reduces, such as after outpatient clinic operating hours.

3.2.2. Monitoring Application and Network Performance

Smart Network Management tools can monitor application and network performance to ensure that the defined level of network access and service is being provided.

Network management systems and application performance monitoring tools can currently be used to manage the user experience. Smart Network Management brings this functionality into a monitoring and management solution, providing a 'single pane of glass' view of live and historical performance and service levels.

End-to-end user experience can be monitored by examining network traffic, using software agents on client devices, or hardware sensors (example in Fig. 6) that generate synthetic user traffic

Figure 6. HPE Aruba User Experience Insight Sensor. Source: Aruba Networks[3]

Application performance issues and opportunities to optimise performance can be quickly identified and notified to the appropriate support team. As detail of application performance and issues is presented in a summarised and user-friendly manner, it is not necessary to have IT skills and knowledge to use the system. This means access can be provided to teams responsible for applications, such as the Patient Management System, allowing them to view performance, and potentially identify and resolve issues without the need to involve IT, for example where the solution highlights poor performance is due to issues with a cloud provider. The Milton Keynes case study detailed later provides an example of a Trust using this approach.

The Smart Network Management functionality can also provide the support team with suggested steps to address the issue, allowing faster remediation (See Fig. 7). This reduces the time taken to identify and resolve issues, improving network and application availability. Again, AI can play a role in identifying issues and suggested remediation, with vendors applying machine learning to data lakes containing network control and performance data from across their customer base.

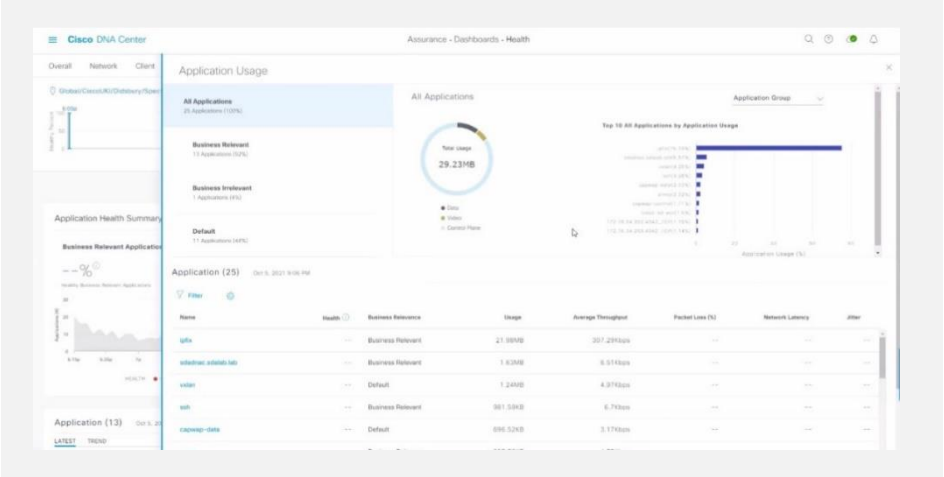


Figure 7. Cisco Catalyst Centre, Application Usage. Source: Cisco

[3] Example hardware sensor: https://www.arubanetworks.com/en-gb/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/

At present, many Smart Network Management tools offer the capability to suggest remediation steps, with network teams being required to review and accept these changes before they are applied to the network. There is potential for Smart Network Management to go further, using artificial intelligence to identify issues and automatically apply steps to address them. However, there is understandable hesitation to offer or use this functionality as it requires a significant level of trust in the decisions and changes being made using AI. There is potential for significant risk to health service delivery if inappropriate network changes are applied in an uncontrolled or unsupervised manner.

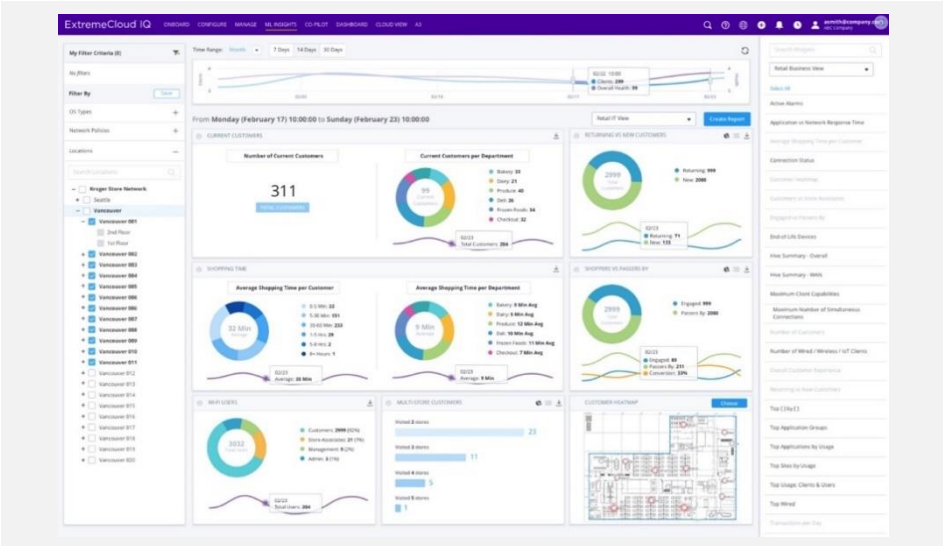


Figure 8. ExtremeCloud IQ Network Management Platform. Source: Netagen[4]

Smart Network Management tools present monitoring data to network teams as a 'single pane of glass' view of network and application use and performance (examples in Fig. 8 and Fig. 9). The capability of this monitoring varies between vendors but typically offers data on utilisation of the network, including wired, wireless, third-party networks, and increasingly, extending to cloud infrastructure and services. Network traffic can be further examined, drilling down to obtain data on the applications being used and associated client devices and users.

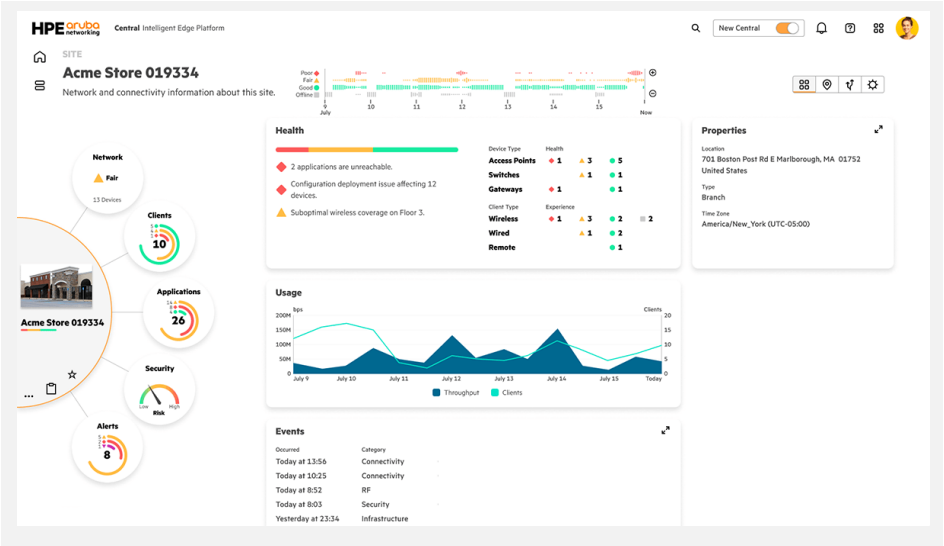


Figure 9. HPE Aruba Networking Central. Source: Aruba Networks[5]

[4] https://netagen.com/solutions/cloud/extremecloud-iq/

[5] https://blogs.arubanetworks.com/corporate/introducing-the-next-generation-of-hpe-aruba-networking-central/

3.2.3. Reducing Network Management and Administration Overhead

Smart Network Management tools can reduce the time and effort network teams spend on network management and administration, with some vendors quoting operational savings of between 20 – 50%[6].

As detailed above, Smart Network Management tools can identify client devices as they connect to the network and automatically apply appropriate policy, this can include the use of machine learning to automatically identify devices based on fingerprinting using MAC address, application use, or traffic patterns. This can reduce or eliminate effort associated with connecting a client device and can use dynamic network controls in place of previous manual configuration of VLANs, QoS, etc. This automation, in addition to reducing network team workload, also helps reduce the risk of incorrect manual provisioning of devices and associated performance and security risks.

Network traffic can be monitored, with new application traffic flows being identified and highlighted to network staff. Applications can be automatically classified, with the Smart Network Management solution providing suggested Quality of Service classifications and uploading the necessary configuration changes to switches.

The monitoring of network and application performance across all connected devices and networks simplifies network management. Faults and performance issues are notified to network teams, providing details of the users, devices and applications impacted. In some cases, issues can be automatically raised as a support ticket in the Service Management platform[7]. Smart Network Management tools can highlight the network element(s), services, or applications causing the issue and suggest steps to remediate it, reducing the time and effort required to triage the issue and identify a suitable fix.

The simplified view Smart Network Management tools provide of application performance and network issues means that they can be used without the need for specialist IT skills and knowledge. As detailed previously, this means that teams responsible for applications can be provided with access to allow them to monitor performance and respond to issues without the involvement of IT resource.

Smart Network Management tools can provide details of network issues with a location context. For example, highlighting if performance issues are being experienced in certain buildings or areas, or in the handoff between specific APs, allowing potential wireless performance or capacity issues to be identified and addressed.

3.2.4. Reduce Network Installation and Configuration Overhead

Smart Network Management can also reduce the time and effort network teams need to spend on network installation and configuration. Zero-touch installation is available, with automatic configuration of new network devices. Network device upgrades can also be completed remotely and with zero downtime.

Applications such as asset tracking and support for wireless telephone handsets (VoIP or IP Telephony) are increasingly being used in health settings. A high density of wireless access points is required to support these applications. There is a degree of network support effort and complexity associated with the installation of these APs to ensure they offer the required level of service. Smart Network Management tools can help address this, automatically configuring radio channels, monitoring the level of service provided to the applications, highlighting locations

[6] Source: Futuriom report for Extreme Networks: One Network, One Cloud, One Extreme: A unique architecture. https://www.futuriom.com/articles/news/one-network-one-cloud-one-extreme-a-unique-architecture/2023/11

[7] Example: https://www.extremenetworks.com/resources/solution-brief/xiq-se-integration-with-servicenow-solution-brief

with issues, including issues with the handoff between APs, and suggesting suitable remediation.

Where network upgrades are required, Smart Network Management tools can assist, offering network models and Digital Twins (see glossary for definition) to design and test upgrades. This can include radio planning (Fig. 10), which can use building plans to simulate the impact of introducing new access points. This potentially reduces the time and effort associated with physical Wi-Fi coverage surveys, with coverage being checked only in the areas where modelling results highlight potential problems.

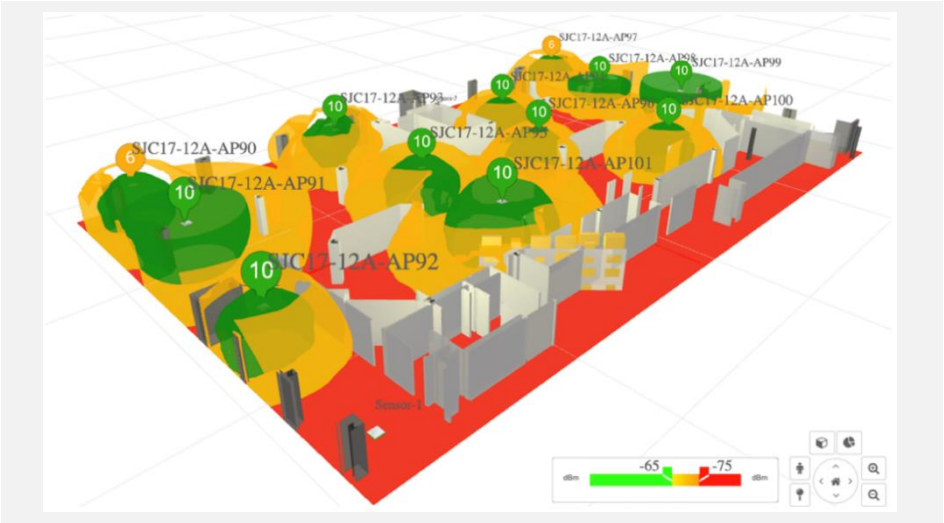


Figure 10. Cisco AP Virtual Reality Planning Tool. Source: Cisco[8]

3.2.5. Strengthen Cyber Security & Data Protection

Network Access Control functionality has been available for many years. Smart Network Management extends this capability, using a unified approach and automation and AI to apply granular and dynamic control of network access.

Smart Network Management tools can apply role-based network and application access controls based on a range of factors, as detailed in previous sections.

Devices are only provided with access to the required network services, applications and data. This allows the network to securely connect trusted NHS devices, staff BYOD, users from partner organisations, guests, patients and IoT applications, such as building management and asset tracking devices.

This network segmentation reduces the risk associated with cyber attacks, limiting the access available to a compromised device, minimising malware propagation, and detecting, identifying and isolating compromised clients. A lessons-learned report produced by NHS England[9] following the WannaCry attack highlighted how Trusts were seeking to implement network segmentation to improve cyber security.

This network access control often uses a zero-trust security approach, treating all client devices as untrustworthy by default. Clients and users are authenticated and potentially posture checked prior to providing access to the network. Network access can be restricted only to the required applications and services.

Devices can be automatically identified, and appropriate access policy applied, reducing the need for manual configuration and the associated risk of errors.

Controls can include location-based access to restrict certain devices, users, or application access to defined locations (example of live client tracking in Fig. 11). For

[8] https://blogs.cisco.com/networking/cisco-wireless-3d-analyzer

[9] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

example, only allowing access to sensitive data or applications to users in specific buildings, or barring access when in public areas.

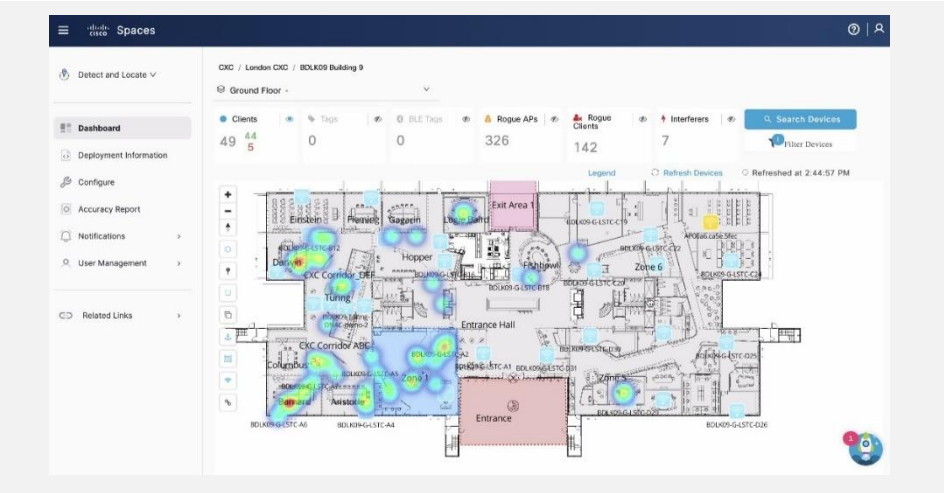


Figure 11. Cisco Spaces. Real Time Tracking of Client Devices & Space Utilisation. Source: Cisco

Smart Network Management tools can use AI to monitor network and application traffic to identify and isolate cyber threats. This can include identifying, locating, and isolating rogue client or network devices, such as access points, switches, or connections to other networks. This functionality can also be used to highlight unauthorised or 'shadow IT' applications to IT support and cyber security staff.

Machine learning can be used to identify and share details of cyber threats between organisations and automatically apply measures to mitigate them, reducing the time to respond to emerging threats.

3.2.6. Sustainability and Net Zero

Smart Network Management can also help NHS organisations with sustainability goals and to reach net zero.

The network monitoring outlined in previous sections can be used to reduce the power consumption of the network infrastructure. This can be achieved by switching off network switches, ports, and access points, or moving them into a power saving configuration during periods of low/no network activity.

As an example (other manufacturers offer similar functionality), Cisco APs contain several radio modules. When all are operational, an AP can typically draw 30-40 Watts. Smart Network Management can be used to instruct the AP to power down most of the radios at quiet times of the day or when only a limited number of clients are connected. This can reduce power consumption to around 7 Watts[10].

An AP can be powered down completely to save further power; however, putting an AP into a low-power state rather than powering it down has a number of advantages. The AP remains active and able to support a small number of clients, for example, continuing to support IoT devices that operate 24x7, or location tracking. The AP can be configured to revert to full operation if the number of connected clients reaches a defined threshold – this process is faster than bringing an AP into operation following a full power down.

[10] Examples of the power consumption of AP models by wireless standard are shown in the tables on Pages 4-8 here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_access_point_power_control.pdf

Powering APs down completely may be suitable for locations that are not used (and do not contain equipment or systems that require monitoring) at known times. For example, this may be suitable for some Primary care locations that do not operate 24x7.

Aruba offers a similar low-power configuration. Their APs can be put into a low-power mode during defined times. The AP remains powered up, but the radios are powered down. The AP activates the radios regularly to check for clients requiring a connection. This configuration can be used in dense wireless environments, with a proportion of APs being configured for low power configuration, meaning that full coverage remains available, but capacity is reduced.

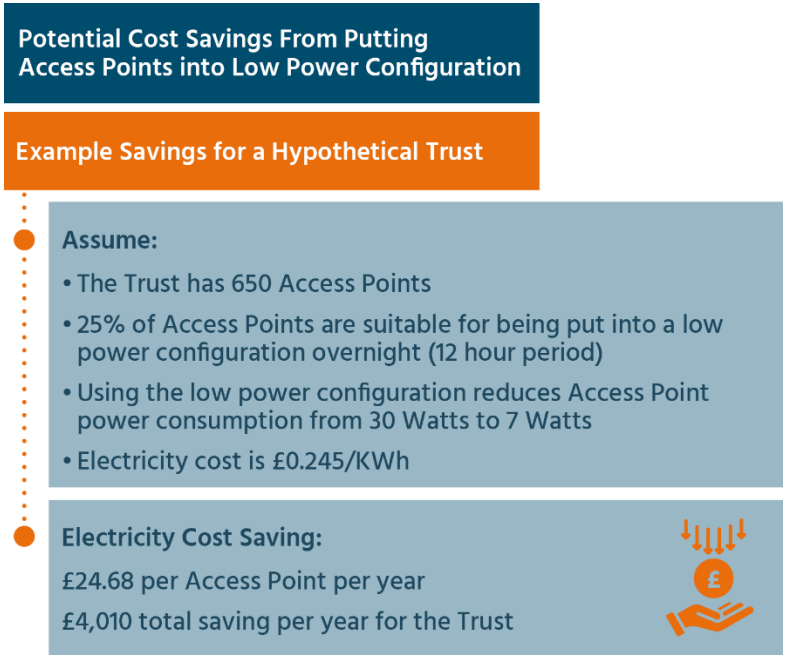


Figure 12. Example Cost Savings From Implementing AP Power Saving Arrangements For a Hypothetical Trust. Source: FarrPoint.

Increasing reliance on wireless networks means that it is unlikely that Health organisations will be able to put all their APs into a low-power mode or switch them off completely. However, high electricity costs mean that even putting a proportion of APs into a lower power mode could deliver tangible cost savings (Example scenario shown in Fig. 12).

Smart Network Management also provides zero touch setup of new network devices which can potentially help reduce the need for travel for network teams and associated carbon emissions.

Smart Network Management inventory tools mean that NHS organisations have accurate details on the infrastructure they currently operate, its operating system and support status. The ability to use models and Digital Twins to test network designs helps ensure that NHS organisations make the best use of, and obtain full value from, the equipment they have already invested in, and minimises the need for additional equipment and the associated environmental impact and power requirements.

3.2.7. Commercial Benefits

Smart Network Management can provide commercial benefits to NHS organisations.

In many cases (as described further in the implementation section), NHS organisations already have access to many Smart Network Management features as part of their existing network licenses. Feedback from equipment vendors suggests that some organisations have not fully implemented and exploited this functionality. Given this, implementing or extending the use of Smart Network Management functionality helps ensure that NHS organisations obtain full value from their existing infrastructure investments.

Smart Network Management systems simplify the operation of multiple virtual networks over a single shared infrastructure. In some cases health organisations

operate multiple networks, for example, separate networks for clinicians, patients, and building management systems. The automated network and client configuration and security provided by Smart Network Management tools makes it simpler to consolidate services onto a single infrastructure, with associated cost savings and support efficiencies.

Smart Network Management tools can also provide efficiencies in how network team resource is used. The ability of these tools to complete analysis of network and performance issues, and to provide suggested remediation, potentially means that a larger proportion of network incidents can be resolved by first and second line support staff. Similarly, automation within the Smart Management solutions can remove or simplify tasks that previously needed to be completed by senior network staff. For example, the ability to automatically recognise and classify applications and configure appropriate Quality of Service on switches.

The previous section outlined how Smart Network Management can reduce the power consumption of the network infrastructure, as well as offering environmental benefits which also reduces the NHS organisations' power and cooling costs.

There are similar cost saving benefits associated with the ability to use Digital Twins and planning tools to minimise the amount of equipment required to offer services and reduce travel costs where zero touch setup of new devices can be used.

4. Case Studies

4. Case Studies

4.1 Calderdale & Huddersfield NHS Foundation Trust

Calderdale & Huddersfield NHS Foundation Trust operates a Cisco wired and wireless network that supports a range of users, clients and applications.

The Trust has a high density of access points to support increasing numbers of wireless clients. This includes device tracking of medical devices and IoT devices, currently numbering in the hundreds and used for monitoring fridges, pharmacy stock monitoring, door access, and for building management systems. The dense wireless coverage also supports Wi-Fi telephony, which is offered on corporate mobiles and helps address issues with poor mobile telephone network coverage within the hospitals.

The wireless network supports a range of users, including partner access (using GovRoam) and patient Wi-Fi (with restricted bandwidth). Clients joining the network are automatically posture checked and provided with an appropriate profile. 802.1x is used to apply VLANs.

The Cisco DNA Centre is used to manage switches, while the Firewall Management Centre is used to manage firewalls and IPS. ThousandEyes is used to monitor application performance and to assist with fault management.

While the Trust uses management tools to help identify and diagnose network and application performance issues, it is not currently using any automated remediation of issues. This is due to nervousness about unsupervised changes being made to the network, particularly outside normal office hours when the IT Team is not onsite.

NHS Calderdale & Huddersfield

4.2 Milton Keynes University Hospital NHS Foundation Trust

The Milton Keynes University Hospital NHS Trust has an extensive wired and wireless data network that supports around 7,000 devices daily and a wide range of user types and use cases. The network is based on Cisco technology and upgraded to new hardware around 18 months ago.

The wired network utilises 10G connections, while the wireless network comprises around 650 access points, providing Wi-Fi 6 and 6e connectivity, including to outdoor areas, such as car parks.

These networks support a range of use cases, including guest internet access for visitors and patients.

Wireless connectivity is becoming increasingly important. Seamless roaming is already available across the organisation, and this supports Wi-Fi telephone handsets. The wireless network also supports clinical pagers and an increasing number of IoT devices. These already number in the hundreds and are used for building management, such as monitoring air conditioning and pumps. Increasing demand for wireless connectivity means that the Trust believes it is possible that a 'wireless first' or 'wireless-only' approach to providing client connections for some use cases is not too far away.

This large network is managed by 2 network staff. Network management is simplified using a range of network management tools, and through standardisation - only 3 models of switch are used across the network. The Trust uses the Cisco DNA solution. The Meraki Dashboard is used to monitor the wireless network and automatically back up device configurations. The ThousandEyes platform provides details on network and application performance to assist the IT team with incident identification and triage.

The ThousandEyes solution is useful for identifying the supplier that should be allocated incidents, particularly for cloud-based services, where the internal IT and multiple suppliers are involved in their end-to-end delivery. ThousandEyes access is also provided to staff who are responsible for the management of these cloud applications, for example, the EPR support team. This means that they are able to identify and triage issues with the applications without the involvement of the IT team.

The Trust is currently introducing Cisco's Software-Defined Access solution. This will initially be used to assist with connecting new devices to the network.

NHS
Milton Keynes University Hospital
NHS Foundation Trust

4.3 West Suffolk NHS Foundation Trust

West Suffolk NHS Foundation Trust has implemented a wired and wireless network solution from Extreme Networks, utilising ExtremeWireless and ExtremeSwitching equipment. The network supports around 4,500 clients across 4 locations and a range of use cases, including support for EPR, mobile workstations, and IP telephony.

The Trust has a small network team. The ExtremeContol and ExtremeAnalytics solutions provide visibility and control of network and application performance and security from a single location.

The Trust also uses ExtremeCloud IQ for troubleshooting and network management and believes the solution supports faster resolution of issues and reduces the amount of resources required to manage the network. The solution provides visibility of application traffic flows through the wired and wireless network, and into the cloud. This means that issues that occur outside the on-premise infrastructure can be identified and resolved[11].

The Trust uses the Digital Twin capabilities of the Extreme solution to design and test new network infrastructure prior to deploying it. They believe this improves security, reduces operational costs, and accelerates innovation.

[11] Source: Futuriom report for Extreme Networks: One Network, One Cloud, One Extreme: A unique architecture. https://www.futuriom.com/articles/news/one-network-one-cloud-one-extreme-a-unique-architecture/2023/11

4.4 Loughborough University

Loughborough University had a large number of devices on the network, a growing wireless demand, and separate wireless and wired networks, which resulted in complex and congested networks. Their typical solution of adding more capacity to the network was no longer suitable and required a rethink. Device permissions and onboarding were completed manually, requiring significant resources and was prone to human error.

The University worked with Cisco to implement a Cisco Software-Defined Access Network & Cisco DNA Centre. The Software Defined Access Network meant new devices could be easily added to the network, segmented, automated for security profiling, and monitored. The DNA Centre also provides a greater understanding of what is happening on the network, the devices and users and indicates any potential issues. The DNA centre also provides a historical lens for trend analysis and appropriate escalation pathways for any issues that emerge.

The solution has resulted in improved network access for staff, students, and visitors, who can more easily remain connected when moving around campus. It has also reduced the resources required to manage network access and issues, improve network security and provide greater network visibility.

5. Market Overview

5. Market Overview

This section provides an overview of a selection of vendors' Smart Network Management offerings. The overview covers a selection of the main products / services available; it does not provide an exhaustive list of each vendor's offering.

Details have been provided for Juniper, HPE (Aruba), Cisco, and Extreme Networks. These vendors were selected as they are all in the top right of Gartner's® Magic Quadrant™ for Wired and Wireless LAN Infrastructure 2024[12], meaning that they have been independently judged by Gartner to be market leaders in terms of the quality of their strategic vision and their ability to deliver it.

5.1 HPE (Aruba & Juniper)

In 2015 HPE acquired Aruba Networks to form **HPE Aruba Networking Central**[13], a cloud-native network management solution. Aruba Networking offers a single location to view and manage all wired and wireless LANs, WANs and VPNs across multiple site locations. The solution also provides advanced analytics to help troubleshoot and optimise network performance. Future versions of Aruba Networking Central will include the ability to automatically reconfigure the network in response to any potential or identified faults and threats.

Aruba Central is available in on-premise and cloud-hosted variants. AI functionality is only available when using the cloud variant, and most customers use this version.

HPE Aruba Networking Central integrates with various ITSM platforms such as Service Now[14] and BMC[15], allowing service tickets to be automatically raised once an incident is detected[16] whilst also enabling incident categorisation (e.g. hardware failure, software issue) and prioritisation (impact and urgency).

HPE Aruba also provide **ClearPass**[17], (Fig. 13) a policy management platform for onboarding new devices onto networks. The role-based solution provides unified network access enforcement across multi-vendor wireless, wired and VPN networks. ClearPass provides policy configuration templates and troubleshooting tools and supports multiple authentication sources. It uses a zero-trust approach and provides the ability for users to onboard their own devices through a self-service portal, a customisable process depending on the client.

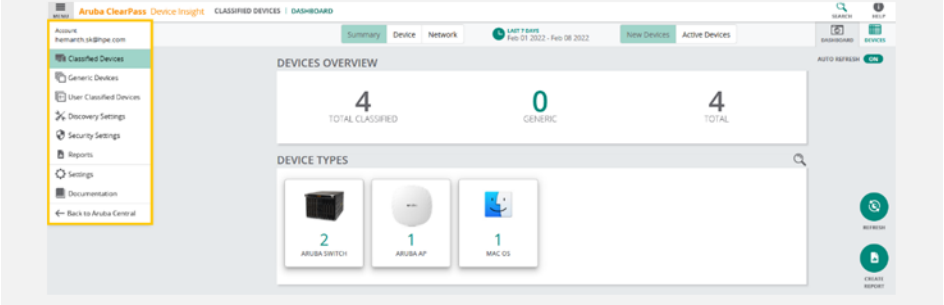


Figure 13. Aruba ClearPass Dashboard. Source: Aruba Networks18

[12] Available from Gartner at: https://www.gartner.com/en/documents/5253763. Quadrant also available at: https://www.extremenetworks.com/resources/report/gartner-magic-quadrant-wireless-wired-access-points

[13] https://www.hpe.com/uk/en/aruba-central.html

[14] https://www.servicenow.com/uk/products/itsm.html

[15] https://www.bmc.com/it-solutions/remedy-itsm.html

[16] https://www.arubanetworks.com/techdocs/central/2.5.7/content/nms/api/servicenow-webhook.htm

[17] https://www.hpe.com/uk/en/aruba-clearpass-policy-manager.html

[18] https://www.arubanetworks.com/techdocs/central/2.5.7/content/allowlist/cpdi-dashboard.htm

Developed by Aruba, but available to everyone, the **Open Locate**[19] initiative standardises the methods for sharing location information (Fig. 14). Using APs' built-in GPS receivers, fine time measures (FTM) and intelligent location software, exact location of users/devices can be identified. Open Locate supports multiple services such as geofencing, space analytics and wayfinding. Devices that don't have FTM can still participate through Bluetooth Radio and Wi-Fi calculations. Open Locate can help users to navigate environments, locate equipment and can support building management systems.

Figure 14. Aruba Open Locate. Source: HPE Aruba Networking[20]

HPE Aruba provide **Networking User Experience Insight (UXI)**[21], a digital experience monitoring solution that monitors network health, application performance and troubleshoots everyday user problems (Fig. 15). It can monitor and simulate the user experience of using key applications, reporting on performance and alerting if issues arise. Machine Learning can be used to identify typical behaviours and traffic pattens and provide alerts where anomalies are detected. The UXI solution can be integrated with Networking Central or accessed via a standalone portal. Up to 30 days' data is stored, allowing historical issues to be investigated.

Figure 15. HPE Aruba Networking User Experience Insight (UXI) Agent. Source: HPE Aruba Networking[22]

[19] https://www.arubanetworks.com/en-gb/faq/what-are-location-based-services/

[20] https://www.arubanetworks.com/products/location-services/

[21] https://www.arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-sensors/

[22] https://www.arubanetworks.com/me/products/network-management-operations/analytics-monitoring/user-experience-insight/

At the beginning of 2024, HPE acquired Juniper Networks, Inc., a specialist in Cloud and AI Networks. Juniper's **Marvis** Virtual Network Assistant (VNA) uses Juniper's Mist AI to help IT teams manage wired and wireless access (Fig. 16).

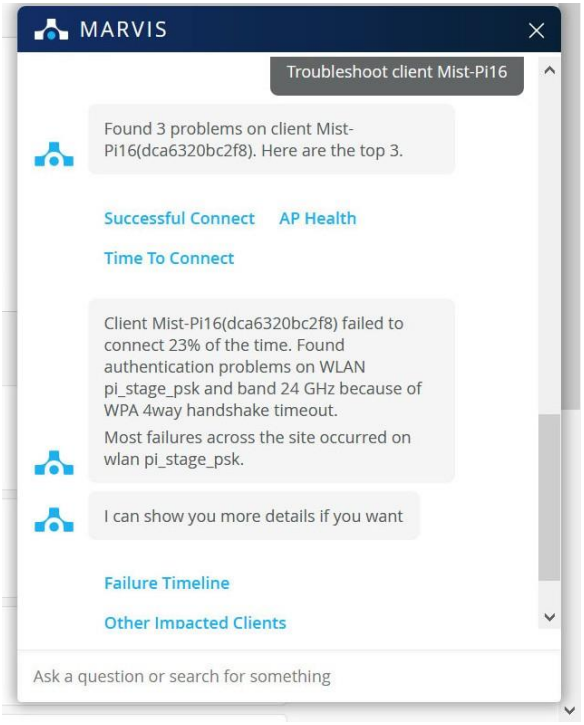


Figure 16. Marvis Virtual Network Assistant. Source: Juniper Networks[23]

Marvis is part of Juniper's AI-native network support model which uses data from network applications and learns from it. The solution provides proactive and prescriptive actions, self-driving network operations, digital experience twinning and integrated help desk functions.

Juniper claims that Marvis provides faster issue resolutions for clients, greater network insights, the ability to proactively identify and resolve issues, improve network visibility and quickly support ticket responses through the use of Mist AI.

Juniper also offers **Marvis Minis** (Fig. 17) which are simulated user connections that learn network configuration using machine learning. Marvis Minis simulate user application use and can proactively highlight network issues such as misconfigured VLANs, application errors and incorrect firewall rules.

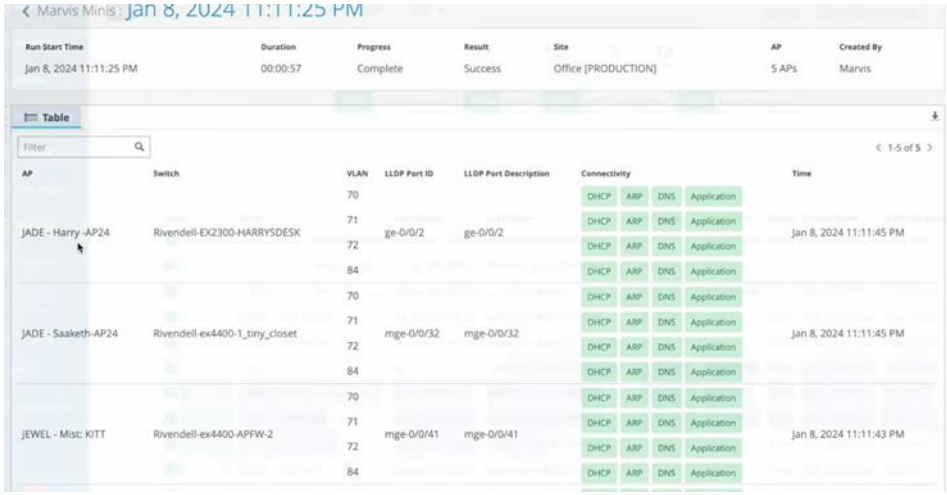


Figure 17: Marvis Mini Dashboard. Source: Juniper [24]

[23] https://www.juniper.net/us/en/products/cloud-services/marvis-virtual-network-assistant.html

[24] Source: Juniper: https://www.juniper.net/gb/en/products/cloud-services/marvis-virtual-network-assistant/marvis-minis.html

5.2 Cisco

Cisco has a long history of involvement in wired and wireless LAN management across many sectors, including healthcare. Cisco's development roadmap is moving the organisation from hardware-based solutions to software solutions and increasing interoperability with other manufacturers' solutions. The driving principle is to "*enable platforms that are adaptable, easier to deploy and manage, and provide users with actionable insights that were previously unavailable or were extremely complex to maintain*[25]*.*". To deliver this, there is a focus on automation, orchestration, visibility, and open standards-based integration.

Their primary offering related to smart network management is the **Cisco Catalyst Centre**[26]. Formerly known as the DNA Centre, the Catalyst Centre provides a network management system for wired and wireless networks, with additional network tools for design, development, visibility, analysis, dimensioning and reporting. The system and associated platforms enable efficient network management, with the ability to use machine learning for network analysis and artificial intelligence to support task automation.

Cisco Identity Services Engine (ISE)[27] is a security policy management platform that provides a single point for network management. The platform helps network managers control all endpoints on the network, understand who is accessing them and manage resource use. The platform supports integration of security policies across networks and device authentication, onboarding and guest management.

Cisco ThousandEyes[28] monitors the performance of applications and services across the cloud and the Internet and enables visibility of different types of networks. The solution enables network managers to identify and resolve issues using real-time insights about network behaviour.

Another relevant Cisco solution is **Cisco AI EndPoint Analytics**[29]**.** This solution leverages Artificial Intelligence and Machine Learning to generate network insights about endpoints and network behaviour. The solution helps organisations identify threats and anomalies and improve network performance through the real-time data the analytics platform produces. The solution can help identify compromised devices and identify steps for network managers to protect infrastructure.

Cisco Meraki[30] is a cloud-managed networking and security solution supporting quick deployment and configuration of networks. The solution enables the configuration of user devices, AP management, firewalls, security appliances, switches and gateway administration, and cloud management.

Cisco Spaces[31] is a cloud-based location service platform that provides network managers with a dashboard for locating and visualising user/device locations (Fig. 18). This can enable the identification of key healthcare assets across various locations, business insights, improved customer experience, safety and compliance, and IoT integration.

[25] Source: https://www.cisco.com/c/dam/global/en_uk/solutions/industries/pdfs/healthcare-secure-infrastructure.pdf

[26] https://www.cisco.com/site/uk/en/products/networking/catalyst-center/index.html

[27] https://www.cisco.com/site/uk/en/products/security/identity-services-engine/index.html

[28] https://www.cisco.com/c/en/us/products/cloud-systems-management/internet-cloud-intelligence/index.html

[29] https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html

[30] https://meraki.cisco.com/en-uk/

[31] https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-spaces/index.html

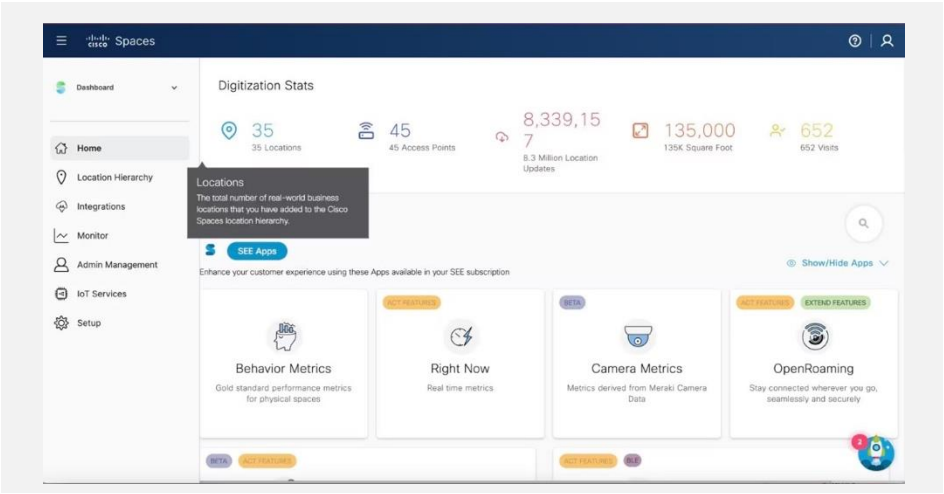
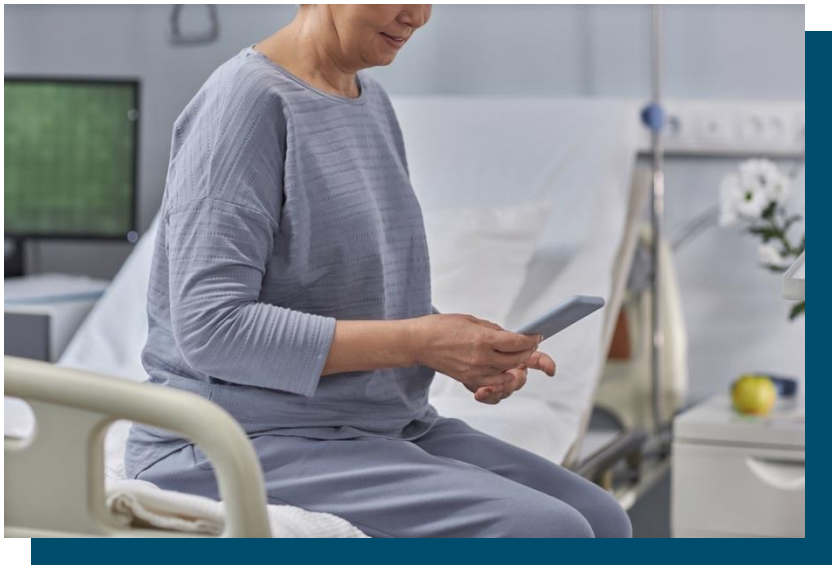


Figure 18. Cisco Spaces Dashboard. Source: Cisco Spaces[32]



Cisco Talos[33] offers actionable intelligence and vulnerability research for Cisco users and the wider population. Talos provides threat detection, malware detection and prevention systems. It harnesses a global network to automatically categorise threats and inform other users of the dangers. Talos uses advanced intelligence to identify weaknesses within systems and identify potential threats before they have even emerged.

In March 2024, Cisco acquired **Splunk**[34] to strengthen its data platforms that underpin many of the core functions of network management, including real-time analytics, cybersecurity and cloud management and business visibility.

[32] https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide/m-home.html

[33] https://talosintelligence.com/

[34] https://www.splunk.com/

5.4 Extreme Networks

Like other providers, Extreme Networks offers a range of products and services that come under the smart network management banner.

A core component of the Extreme Networks offer for smart network management is the **Extreme Cloud IQ**[35]. This product provides visibility of wired, wireless, SDWAN and Extreme Fabric networks. In addition, Extreme Cloud IQ offers a pilot/co-pilot model for developing a network digital twin so network managers can trial and test potential designs and configurations. The product offers initiative insights, network analysis, device management and network remediation.

In addition, the **Extreme Cloud IQ Site Engine**[36] offers end-to-end network management, with task automation, analytics service assurance and orchestration (Fig. 19). It provides a role-based network access control for devices and can support cloud migration and management. Site Engine offers an open API to support integrations with enterprise platforms such as ServiceNow, which enables automatic support tickets to be raised, reducing the administrative burden for network managers.

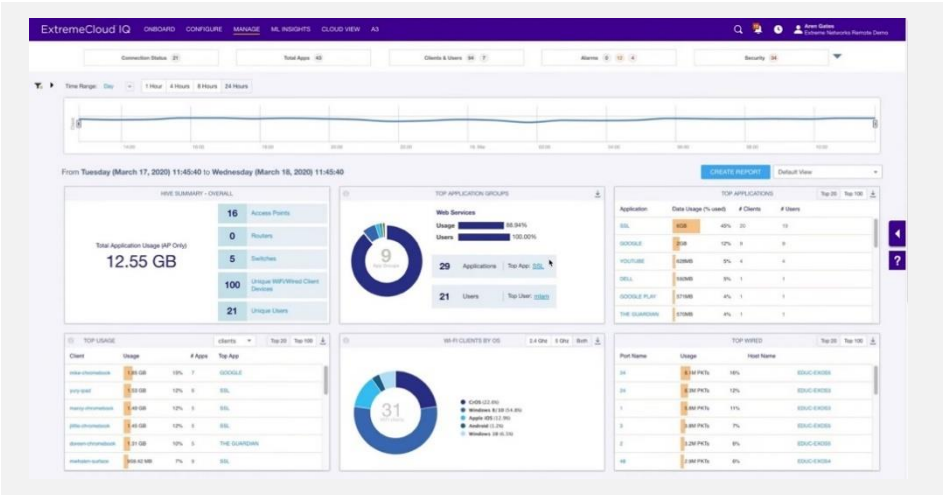


Figure 19. Extreme IQ Cloud Site Engine. Source: Netagen[37]

Extreme Analytics[38] extends the capability of Cloud IQ by providing network and application analytics and visibility (Fig. 20). Extreme Analytics generates traffic latency calculations and can provide insights on user behaviour, engagement and application delivery, whilst also offering accelerated troubleshooting and automatic performance alerts.

[35] https://www.extremenetworks.com/products/cloud-based-management/extremecloud-iq/extremecloud-iq

[36] https://www.extremenetworks.com/products/network-management/extremecloud-iq-site-engine/extremecloud-iq---site-engine

[37] https://netagen.com/solutions/cloud/extremecloud-iq/

[38] https://www.extremenetworks.com/products/network-analytics/extremeanalytics/extremeanalytics

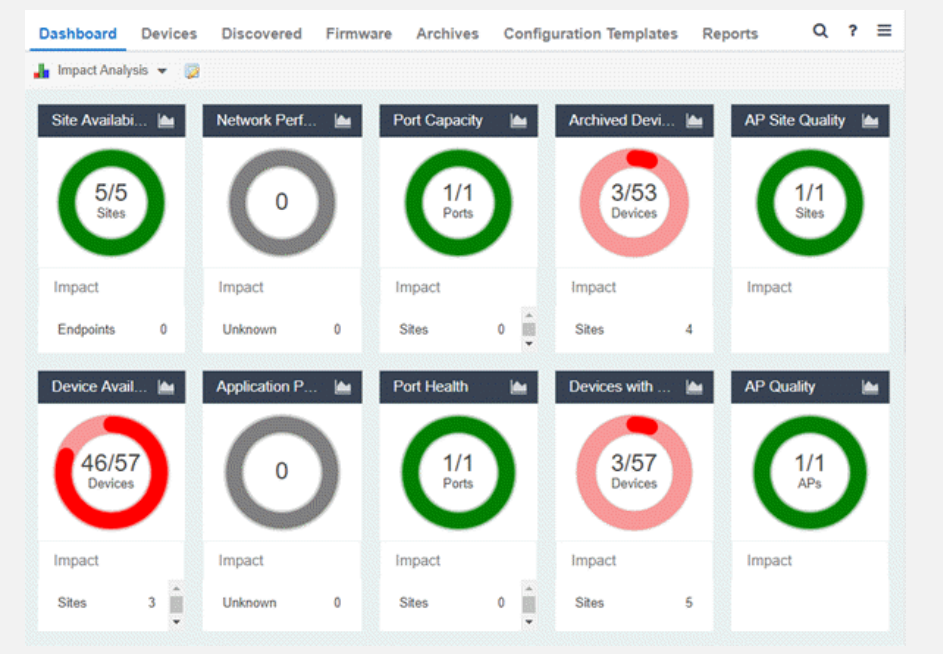


Figure 20. Extreme Analytics Dashboard. Source: Extreme Networks[39]

5.5 Future Developments

Smart Network Management functionality will continue to advance in the coming years as new technologies and capabilities become available.

As leading vendors have identified, Artificial Intelligence and Machine Learning already play a role within smart network management, although this can be limited by the emerging nature of this technology and customers' trust in it. Use is likely to increase in coming years as capabilities and levels of trust increase. This capability will likely include providing greater levels of analytics, diagnostics, troubleshooting and visualisation of networks and their use. In addition, these services will be able to carry out a higher degree of self-repair and other appropriate actions in response to any potential emerging issues.

As networks continue to become more complex with increased numbers and variety of devices and users, the threat of attacks also becomes greater. It is likely that smart networks will continue to evolve in terms of their cybersecurity capabilities, using Artificial Intelligence and Machine Learning to manage new threats, mitigate their impact and automatically designate and manage when any occur.

The continued shift to the cloud means that extending Smart Network Management to provide visibility of the user experience of these cloud applications will become increasingly important. This capability already exists and is likely to be increasingly used by health organisations as more of their services shift to the cloud.

39 https://emc.extremenetworks.com/content/oneview/docs/network/docs/impactanalysis/c_imp_analysis_dashboard_overview.htm

6. Smart Network Management Deployment

6. Smart Network Management Deployment

6.1 Technology Considerations

This section provides an overview of some of the considerations health organisations need to address as part of any plans to deploy Smart Network Management based on information from two vendors.

Smart Network Management covers a wide range of functionality to manage a range of network equipment and services. Each health organisation will need to develop a detailed deployment approach based on its existing infrastructure, licenses, technology mix, and the functionality it is looking to utilise.

6.1.1. Cisco

Much of the Smart Network Management functionality offered by Cisco sits within the Catalyst Centre (previously called DNA Centre).

Cisco customers will already be entitled to use Catalyst Centre as part of the license subscription associated with their wired and wireless hardware. The level of functionality customers have access to depends on whether they have an Essentials or Advantage license subscription.

The functionality offered by each license tier for wired switching devices[40] shows that a range of functionality is available to Essential license users, though the features relating to Cisco Spaces, ThousandEyes, and AI Analytics are only available at the higher license tier.

Similarly, the functionality offered with wireless devices[41] shows that features such as 3D analyzer, AI analytics, and more advanced Spaces functionality require the Advantage license.

Catalyst Centre is compatible with switches using IOS15.x or more recent releases and Access Points procured in the last ~5 years. However, support can vary by switch / AP model and the Catalyst Centre functionality being used, so organisations should check compatibility for their specific needs.

Catalyst Centre can provide visibility of third party switches, though functionality is limited for non-Cisco devices. The third-party devices must support SNMP to be monitored.

6.1.2. HPE Aruba

Much of Aruba's Smart Network Management functionality sits within the Networking Central solution. As detailed in the previous section, this is offered as an on-premise or cloud-hosted service, although AI capabilities are only available with the cloud variant.

Customers with Aruba Wireless Access Points have access to Networking Central as part of their license subscription. However, the level of functionality depends on whether they have Foundation or Advance licenses[42].

[40] https://www.cisco.com/c/m/en_us/products/software/dna-subscription-switching/en-sw-sub-matrix-switching.html?OID=otren019471

[41] https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html?oid=porew018984

[42] https://www.arubanetworks.com/techdocs/central/2.5.6/content/nms/get-started/quick_start.htm

Wired switches can be procured without a Networking Central license, meaning customers may not have access to this capability unless they have procured a separate license.

Networking Central has limited ability to interface with third-party network devices. Third party equipment will be shown on network maps if it has an Aruba AP connected to it, with Networking Central discovering the devices using LLDP.

The User Experience Insight (UXI) monitor device can be used on any vendor's network. When the monitor is used on non-Aruba networks, monitoring data can be accessed using a dedicated UXI portal. When the customer is using the Aruba network, the UXI data is also available within the Networking Central solution.

6.2 Other Deployment Considerations

In addition to technology, other considerations may influence if, and how, health organisations deploy Smart Network Management solutions.

6.2.1. Impact of Vendor Choice

As outlined above, although Smart Network Management solutions offer support for other vendors' equipment, in many cases this support can be limited, meaning access to all features is only available if a single vendor approach is taken.

While a single vendor approach can offer some efficiencies in network management and support, it also limits health organisations' choice and commercial flexibility. NHS organisations need to understand the equipment and services they currently use, and consider the advantages offered by Smart Network Management, and the associated impact this will have on vendor choice and commercial flexibility.

This is likely to be a particular consideration for organisations with legacy infrastructure from several vendors, and for Integrated Care Systems (ICS) that are seeking to manage infrastructure inherited from several organisations.

6.2.2. Operational Impact

Smart Network Management simplifies the monitoring of application performance, and the identification and rectification of issues. To take full advantage of this capability health IT organisations need to change their operational processes and ways of working.

First and second line IT support staff are likely to be able to resolve a larger number of support tasks. Similarly, new client devices are likely to require less (or no) support from IT staff to get connected to the network. Operational processes, and communication plans for end users will need to be updated to reflect these changes.

Access to the Smart Network Management system needs to be extended beyond the IT team. Teams responsible for the management of applications, such as Patient Management Systems, can also be provided with access to allow them to monitor application performance and to help respond to any performance issues without the involvement of IT resource. Again, implementing these changes are likely to require update to existing operational procedures and communication plans.

6.2.3. Business Case

While health organisations are likely to have some Smart Network Management features provided from their existing licences, as outlined above, some of the more advanced features are separately licenced and so may come at an additional cost.

Health organisations are likely to need to evaluate the benefits offered by these advanced features against their cost. As Smart Network Management functionality becomes more widely deployed in health, further case studies and detail of the benefits obtained will be available from other organisations to support this evaluation.

6.3 Key Questions for Suppliers

Suggested questions health organisations should ask their suppliers to support the planning and deployment of Smart Network Management include:

- What Smart Network Management functionality and features do our existing licenses provide access to?
- What licenses, services, or equipment is required to add further Smart Network Management capabilities?
- How can the Smart Network Solution help us better understand the network infrastructure and licences we have, if they are being used, potentially highlighting unused or underutilised elements?
- Which elements of our existing infrastructure are compatible with the Smart Network Management solution?
- Which of our existing client devices are compatible with the Smart Network Management solution?
- Do client devices require any software or configuration to be compatible with the Smart Network Management solution?
- Are there any limitations in Smart Network Management functionality due to use of older hardware, firmware, or third party equipment?
- What advantages, functionality and/or commercial, are obtained if network infrastructure is sourced from a single vendor?
- What examples do you have of health organisations obtaining benefits from implementing the Smart Network Management functionality?

Appendix: Glossary

Glossary

802.1x	IEEE framework standard for encrypting and authenticating a user trying to associate to a wired or wireless network.
Access Points	Networking hardware device that enables other Wi-Fi devices to connect to a network.
Artificial Intelligence (AI)	The use of computers to simulate human intelligence and complete problem-solving.
BYOD	Bring Your Own Device
Data lake	A repository of structured and unstructured data.
Digital Twin	A virtual representation of a system. Used in Smart Network Management to develop digital simulations of IT network designs and configurations to support virtual testing.
Electronic Patient Record (EPR)	A digital store of patient information and medical history. See also, Patient Management System.
Integrated Care Systems (ICS)	Local partnerships between Health, Local Authorities, and the Third Sector.
Internet of Things (IoT)	A network of sensors, software and other technologies that communicate over the internet and other communication networks allowing monitoring and control of a range of environments and systems.
Intrusion Detection Solution (IDS)	A system that that monitors network traffic for malware, malicious activity and violations of security policies.
Link Layer Discovery Protocol (LLDP)	A network protocol that supports the discovery and identification of network equipment.
Machine Learning (ML)	Related to Artificial Intelligence. Machine Learning is the process AI systems use to develop their intelligence and support decisions.
Patient Management System (PMS)	A digital store of patient information and medical history. See also, Electronic Patient Record.
Picture Archiving and Communication System (PACS)	Systems that store and share images generated by medical imaging devices, such as X-Ray and Magnetic Resonance Imaging (MRI) scanners.
Quality of Service (QoS)	Controls used on networks to identify and prioritise network traffic. QoS is particularly important where there is potential for data flows to exceed the available network capacity. This allows, for example, business / safety critical users, devices, or applications to have prioritised access to network capacity and resources.
Role-Based Network Access Control (RBAC)	Mechanism that restricts a user's network and system access to ensure they have access only to the data and services required for their role.
Secure Access Service Edge (SASE)	An architecture that combines a range of network services and technologies. It is designed to support

	cloud-based environments, locating services and controls at the network edge.
Simple Network Management Protocol (SNMP)	A network protocol used to monitor, manage and control network devices.
Single pane of glass	Dashboard or platform that provides a centralised location to visualise different sources of data on network and application configuration and performance.
Software-Defined Networking (SDN)	A technology that supports intelligent and dynamic control and configuration of networks.
Virtual Local Area Network (VLAN)	A means of dividing a network into separate 'virtual' networks. VLANs are used to control the network access of users/devices, to improve network performance, and to implement security controls.
Virtual Private Network (VPN)	Mechanism for creating a secure connection between a device and a computer network, using an insecure communication medium such a public Internet.
Zero touch provision	A mechanism that allows devices to be automatically set up onto networks. Allows network managers to install networking devices without manual intervention.
Zero trust	Security model that states nobody is trusted by default inside or outside a network, meaning verification is required from anyone trying to access the network.

Version Control

Owner	**Richard Parkinson**
Classification	**Client Confidential**

Revision	Description	Author	Checked	Reviewed	Authorised	Date
1.0	Issued	RP / JCh	AM	AM	RP	07/06/24
2.0	Updated with Client Comments	RP / JCh	AM	AM	RP	18/06/24

FarrPoint

Visit

farrpoint.com

Certified B Corporation

Edinburgh
93 George St
Edinburgh
EH2 3ES

T: +44 (0)131 202 6018

London
1st Floor
99 Bishopsgate
London
EC2M 3XD

T: +44 (0)20 3693 7310

Manchester
3 Hardman Square
Spinningfields
Manchester
M3 3EB

T: +44 (0)161 669 5821

Halifax, Canada
1300-1969
Upper Water Street,
Halifax, Canada
NS B3J 3R7

T: +1 902 5001414

Boston, USA
100 Cambridge Street,
Boston,
MA 02114

T: +1 857 356 1414