

White Paper by Bloor

Author **Paul Bevan**

March 2024

## The importance of assuring the digital experience in delivering business services



As businesses have increasingly adopted a wide range of external services, many of which are highly interconnected with one another, they no longer possess complete control over the infrastructure and applications they depend on. This increased reliance on external services can lead to a greater risk of business disruption, reduced workforce productivity, and damage to the brand's reputation. To mitigate these risks, organisations must take complete ownership of the entire service delivery chain that their business relies on. This involves implementing a continuous approach to the service lifecycle, which includes planning, baselining, troubleshooting, and optimisation. Capabilities such as automated incident analysis, diagnostics, remediation, forecasting, and recommendations can be leveraged.

# Executive summary

**N**etworks are critical to the success of your business. Whether you are a digital startup, or a major global organisation, loss or degradation of network connectivity – and the critical apps and services that run on them – will cause you problems and lead to potential impacts on revenue, profits and reputation. The only questions are, how quickly will the impacts be felt, and how much it will cost your business. If the answers are, very quickly and very costly, then business leaders will need assurance from their Information Technology (IT) organisations that their networks which, critically, encompass users' digital experience are up to the task. To do that, organisations must take complete ownership of the entire service delivery chain that their businesses relies on.

The irony of IT in the 21st Century is that the ability of cloud computing, mobile technology and a plethora of new application development tools and methodologies make it easier for all of us to consume technology quickly and easily, it has made the task of implementing and managing the underlying IT infrastructure, and in particular the network, vastly more complex. The modular, API-centric nature of modern applications and the broad adoption of business Software-as-a-Service (SaaS) have created a vast and rapidly changing web of interdependence, with the cloud at its centre. At the same time, the global pandemic placed a greater demand on digital services and accelerated the shift to "cloud first" and more flexible working patterns, leading to more and more services and service dependencies being concentrated within the major cloud providers than ever before. This has caused problems for traditional monitoring tools being deployed by enterprises partly, initially, because they weren't able to "see" into public cloud or the public internet. It caused a visibility gap.

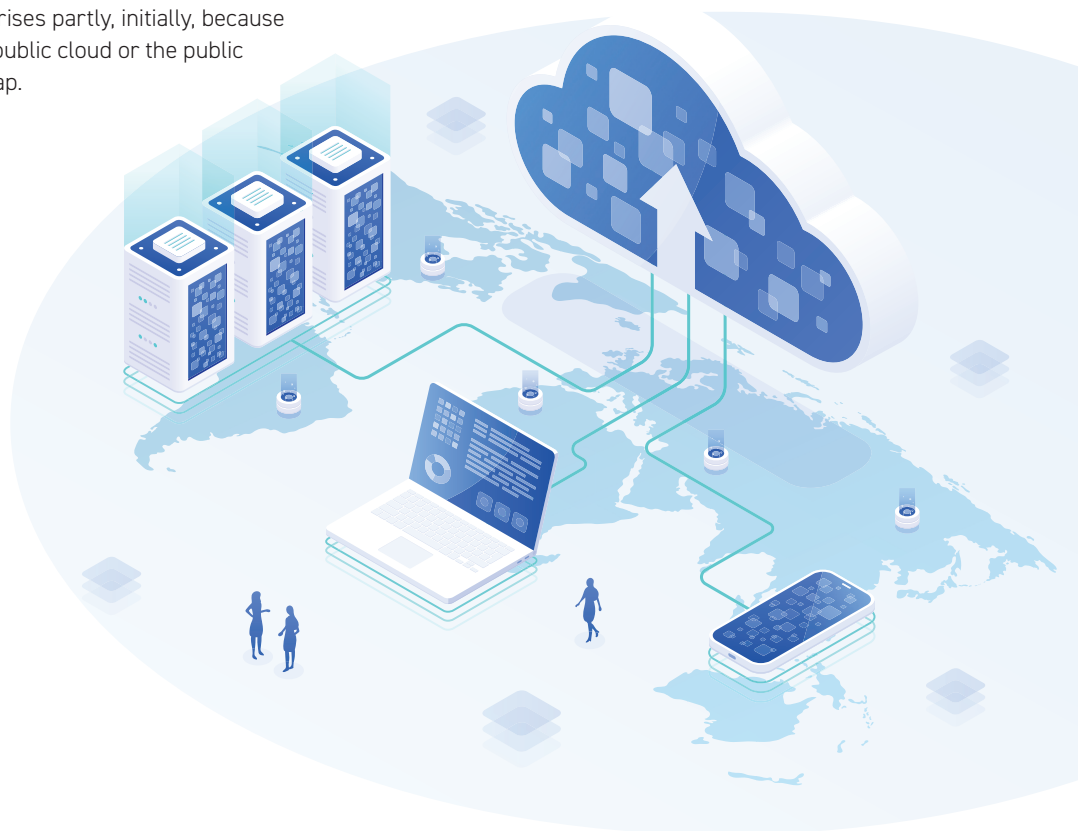
Now, new solutions and services enable IT operations teams to close that visibility gap and, crucially, to be able to see and understand the end-to-end relationships between critical business services and the IT infrastructure that supports them. However, Assurance for flawless digital experience does not rely solely on deploying new technology solutions. It is as much about people and process, relationships and collaboration, both internally and with business partners as it is about shiny new technology.

This white paper will outline the technical, organisational and cultural challenges that need to be addressed to be able to provide realistic, evidence-based, Assurance.

---

“The modular, API-centric nature of modern applications and the broad adoption of business Software-as-a-Service (SaaS) have created a vast and rapidly changing web of interdependence, with the cloud at its centre.”

---



# Assurance:

## A key component of business service assurance

Just ahead of an important quarterly Board meeting, the CEO contacts the CIO and asks her that, if challenged, will she be able to provide assurance that the organisation's entire IT ecosystem will provide the performance and availability to support the applications critical to the success of the business.

In the past Assurance was something that Telcos and Service Providers focused on more than enterprises, and it tended to refer to particular, siloed network domains such as wireless. Now, for an enterprise CIO, Assurance is part of a much wider business services assurance process that requires end-to-end visibility of all the applications and compute resources that go to delivering the objectives of the business.

---

“Giving an assurance is easy. But in today's globally connected, always-on environment, providing the evidence to support such a confident assurance has become extremely complex.”

---

Giving an assurance is easy. But in today's globally connected, always-on environment, providing the evidence to support such a confident assurance has become extremely complex. Businesses are now in a constant state of evolutionary change, responding to rapidly evolving business environments. As cloud networking and the internet become more critical to how fast enterprises are able to respond to the demands of innovation and growth, they want to know that their networks are secure, resilient and manageable. As cloud networks become more fundamental to business success, but also more complex and highly distributed, governance becomes more challenging.

Fortunately, over the last decade cloud service providers have started to provide their own tools for their customers to gain greater visibility into the performance of cloud networks. They have also provided APIs that enable 3rd party solutions to provide a single view into multi-clouds. Critically important for Assurance is the ability to predict potential performance problems and outages. The best solutions on the market are now beginning to use machine learning algorithms to help spot problems before they start to impact the user experience. In the near future we expect to see the use of Large Language Models and Generative Ai to significantly enrich data correlation and provide even more early warning of potential problems.



# Where is the network in a mutable business?

Bloor believes that the Future of Business lies with mutable businesses in a constant state of evolutionary change, responding to rapidly evolving business environments. In the short term, the journey to the Future of Business has been accelerated as a consequence of the COVID 19 pandemic and also the rapid development of Artificial Intelligence (AI) capabilities. However, it has been a trend for some time prior to these events.

Ten years ago, Amazon was already showing that every 100ms of latency cost them 1% in sales, while Google found an extra 0.5 seconds in search page generation time dropped traffic by 20%. In a real sense, in a modern hybrid multi-cloud environment, the network and network connectivity is the business (although not all of the business) and network management is an essential part of ensuring business continuity.

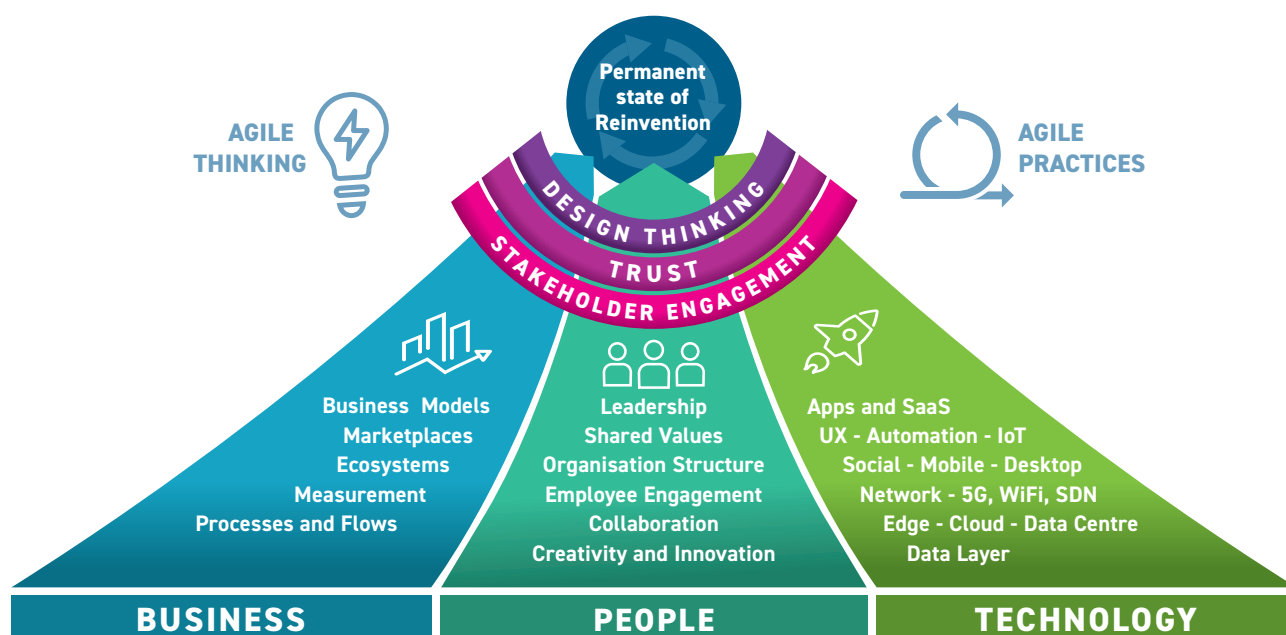
This growing focus on modern innovative technology and, in particular, in people-oriented technologies and user experience, means that it is increasingly important to understand what success looks like to all of the stakeholders on the network, and at how it can be delivered. This involves managing multiple data sources to the appropriate service levels and making use of the latest network monitoring tools and techniques.

It will involve identifying both the criteria for demonstrating success; and the success factors necessary for actual successful delivery – and it is worth noting that success may well look different to the business and to the IT/Network operations teams.

What this means overall, is that planning for success will be needed. This will entail investment in automation and, potentially, new tooling. This involves much more than just implementing AIOps (automation of traditional operations practices with embedded augmented intelligence). People issues matter and it is vital to build trust in your automation. Part of this will come from effective baselining, review of the results of automation against the baseline, and re-baselining before the next advance. If you have no historical reference data, how do you know if current performance is good or bad – or if it is improving?

“Ten years ago, Amazon was already showing that every 100ms of latency cost them 1% in sales.”

*Bloor's outline of a Mutable Business, illustrating how businesses can successfully transform in a continuous way*





# Governance of the network management function

No one organisation owns the network service delivery chain, or rather, no one organisation is accountable for every segment in that service delivery chain. However, the service user or customer, has responsibility for a seamless digital experience to all stakeholders. Even if they are able to have individual SLAs for each segment or group, they might all operate interdependently with no cohesive view or objective. Tying these disparate agreements together with the aim of continuously improving and delivering excellent digital experience is a fundamentally important part of the Assurance process.

The business should come first. Part of what this means for technology is that low-level technical performance data should be accompanied by impact assessments in business terms (which implies that the relationship between technology and business systems is actively maintained as technology evolves). Low-level data should automatically be aggregated (via dashboards) up to the business service level and made available to all stakeholders at an appropriate level and using language they can understand. Don't tell your stakeholders that things are better, show them metrics they can understand and let them see for themselves.

---

“...many, if not most, of the factors impacting your network performance may be outside your control.”

---

Of course, another implication is that the SLAs with any service suppliers should be expressed in business terms, as well as with technical detail if necessary. Always work to a business case – trying to rationalise your toolset to just one tool or one vendor, for example, risks impacting business service levels. Better to monitor business service levels and integrate and reduce the number of existing monitoring tools, just as long as the business isn't being impacted and the cost savings can be measured.

One fundamental technology issue lies in reducing the mean time to identifying real points of failure (or, better, impending failure), so that time is not wasted in finger-pointing and failures can be corrected quickly or, ideally, prevented. This involves identifying the barriers to efficiently reporting and addressing outages and performance degradation. It also involves building a culture of co-operation between the different domain operating teams, both technical and business – DevOps and AIOps go part of the way towards removing silos but can, if not managed well, become silos themselves.

Another key technology issue now is the prevalence of public cloud and internet networks in the enterprise. This means that many, if not most, of the factors impacting your network performance may be outside your control. Until recently, if you hadn't written your service provider contracts carefully, some of the data you needed to manage your performance issues may not have belonged to you and may have been hard to access. However, there are now tools and services that give you visibility into the performance of your network traffic as it traverses multiple, globally distributed public networks to reach the intended Cloud destination. Indeed, such tools and services are beginning to provide visibility behind the CSPs firewall in collaboration with those providers own management tools. The bottom line here is network management in the Cloud relies on a shared responsibility model. Don't assume that you needn't understand networking technology issues and options today just because moving to cloud looks easy and any issues are now someone else's problem.

From a technology point of view, hybrid cloud and edge infrastructures involve more communication between independent components than traditional approaches. Modern micro-services architectures rely on APIs. It is likely therefore that there will be an increased need to monitor and manage far more service-to-service communications, with API availability and performance becoming an increasingly important component of overall service delivery. Ignoring this, or viewing it out of context of the whole service delivery chain, can lead to performance and resilience issues that impact your business.

A final issue is that of holistic metrics. The business pays network management to, in effect, deliver business outcomes. Measure both network and servers – and anything else that impacts the business service. Get rid of demarcation contests between silos – and never tell a business that is suffering from an unusable service provision about just how well the network contribution to the service is performing.

# Public and private network management for all stakeholders

Managing and assuring effective performance management of all IT infrastructure, including networks and SaaS applications, should be a key business priority. This means making sure that you can provide the right data at the right time to the right people – remembering that some of this may not be under your direct control. It is necessary to identify the minimum data necessary and any extra data that will be useful. Remember that timeliness matters (real-time, near real-time, point-in-time – with clear definition of these terms); and quality (source, SLA) matters. Storing data is low cost, managing data often isn't, so don't collect data that you won't use, although never cut off the possibility of collecting data in future.

Managing the possibility of alert overload; and setting up exception reporting will be important. You need to know what is causing alert overloads and how you can reduce the first line support load. You should always be aware of the impact of false positives – 100% detection of an issue isn't very useful if it is also being reported erroneously a similar number of times.

This sort of thing should seem familiar to anyone with experience of IT Service Management or ITIL. We are, in effect talking about an evolution of Configuration Management for Hybrid Cloud and Edge Infrastructures.

## Service enablers

Identify everything that is necessary for delivering an effective business service, at whatever level you are happy with (some of this will be technology, but you might want to include SLAs or key people). If you don't know what you have, you can hardly expect to manage it.

## Service metrics

For each of these “*configuration items*”, identify the metric data that will let you manage its performance and effectiveness. Only collect data that you will use, you can add more later, if it is useful.

## Federated data

Remember that we are not suggesting moving all of this configuration information that we are talking about into new data stores. A federated database is fine – leave the data where it is and point at it, unless there is a good reason (usually performance or cost) not to. This does, of course, imply effective monitoring of usage and network traffic.

---

“ 100% detection of an issue isn't very useful if it is also being reported erroneously a similar number of times. ”

---

# Key components of Assurance

Assurance in a hybrid and multi-cloud IT environment encompasses various elements. Let's explore these components in a little detail.

## Performance monitoring

Monitoring the performance of your network infrastructure is essential to ensure that it meets your organisation's requirements. In a hybrid and multi-cloud setup, this involves monitoring not only the on-premises network and the cloud-based components, but also internet and wireless networks that are being used increasingly due to the rise of working from home and growth of the internet of things (IoT).

- **End-to-end performance monitoring**

Employ performance monitoring solutions that can track both traditional and cloud-based applications. You need to monitor network performance from end to end. This includes user experience, application response times, and data transfer rates. It is important to note that, the prevalence of micro-services-based architectures means that there needs to be a focus on the performance and availability of all Application Programming Interfaces (APIs) not just on the application code itself.

It would be preferable to use an integrated platform that collects all the sensor and agent data, correlates and enriches that data, uses machine learning and artificial intelligence to improve prediction of problems before they impact and, where possible, automate remediations or, at least, automate the incident response process. There should be an objective to reduce the number of tools being used, and an integrated platform is a key component in this. However, the complex and rapidly changing nature of the IT and network environment, combined with numerous technical, organisational and cultural issues tends to make it difficult for a single integrated solution or platform to eliminate all the separate monitoring and management tools. In this event, use of open standards such as OpenTelemetry and published, simple to implement KPIs will ease the challenges of tool integration.

- **Network visibility**

Utilise tools and technologies like network traffic analysis, packet capture, and flow analysis to achieve visibility to gain a comprehensive view of the entire network, including on-premises data centres, virtualised infrastructure, and cloud resources.

- **Synthetic and real user monitoring**

The resurgence of interest in, and focus on, the digital end-user experience, has highlighted the need to use real-time user data, but also synthetic data. By implication, real-user monitoring can inform you about what has just happened. Synthetic data on the other hand allows you to continually test proactively for problems that might prevent issues from occurring.

- **Real-time alerts**

Set up real-time alerts for network performance anomalies or deviations from predefined thresholds. Automate incident resolution where possible and appropriate. Where that is not possible, ensure rapid incident response to prevent or mitigate downtime and performance degradation.

## Security

People and device movements have become more "dynamic," and organisations need to protect their people, devices and information assets 'on the move' in a much broader range of locations and scenarios.

These scenarios may sometimes conflict with internal policy settings and risk appetites. An employee may find themselves transiting through international ports or working in locations where a third-party cloud service has little to no domestic servers or presence, where arranging secure cloud access could mean routing traffic to a geographically distant cloud region over a mix of terrestrial and subsea cables, adding latency and potentially extra security challenge 'inconvenience'.

Balancing the needs of security and usability in such a dynamic enterprise environment requires new thinking, new layering of security protections, and new approaches to the challenge generally.

- **Secure Access Service Edge (SASE)**

SASE is a broad, cloud-native approach that integrates various network security functions to provide secure and scalable access to resources regardless of location or device. It represents a comprehensive security architecture that combines wide-area networking (WAN) capabilities with network security services delivered as a cloud-based service.

SASE converges network security functions like secure web gateways (SWG), cloud access security brokers (CASB), firewall-as-a-service (FWaaS), Zero Trust Network Access (ZTNA), and more into a single integrated offering.



It provides secure access to applications and resources regardless of the user's location (on-premises, remote, or cloud-based). Furthermore, SASE emphasises the transformation of legacy network architectures by incorporating security directly into the network, offering a more agile and scalable security approach.

Properly designed and implemented it ensures consistent security policies and controls across different edges (like branch offices, cloud services, or remote users) through a cloud-native architecture.

- **Cloud security services**

Remember that, while Cloud Service Providers (CSPs) are responsible for security of the Cloud, you are responsible for security in the Cloud. Leverage cloud-specific security services offered by CSPs, like AWS Security Hub or Azure Security Center. Pay attention to east-west traffic inside the Cloud perimeter and implement network security groups and firewalls to protect cloud resources.

## Redundancy and high availability

Ensuring network redundancy and high availability is critical to prevent downtime and data loss. In a hybrid and multi-cloud environment, this involves designing and implementing redundancy at multiple levels.

- **Load balancing**

Implement load balancers to evenly distribute network traffic across multiple servers or cloud instances. Use global server load balancing (GSLB) for seamless traffic management across multiple locations.

- **Multi-region deployment**

Deploy resources across multiple regions or availability zones provided by cloud providers. This ensures that network resources remain available even if one region experiences an outage.

- **Disaster recovery**

Your Assurance process should inform the development of an appropriate disaster recovery plan that includes backup, failover, and recovery strategies. Regularly test and update the plan to adapt to evolving network requirements.

## Scalability and resource management

Scalability is a fundamental benefit of hybrid and multi-cloud environments. Ensuring that your network can scale effectively is crucial for accommodating growth and fluctuations in demand.

- **Auto-scaling**

Implement auto-scaling mechanisms to automatically adjust resources in response to changing workloads. Leverage cloud-native services like AWS Auto Scaling or Azure Autoscale.

- **Resource optimisation**

Continuously monitor resource utilisation to identify and eliminate bottlenecks or underutilised resources. This can be facilitated by utilising cloud cost management tools to optimise spending while maintaining performance.

- **Resource tagging**

Use resource tagging to categorise and organise cloud resources. Tags facilitate resource management and cost allocation.

## Risk management

No assurance process, be it for networks, IT systems in general or business services, can be considered complete without effective risk management disciplines. Assessing risk contains two elements; how severe is the impact of the risk occurring, and the likelihood/frequency of the risk occurring?

Some risks, for example a complete system outage, are relatively easy to assess. Others, like balancing high levels of security against the impact on the end-user experience are harder to define. In such instances it can be tempting to use the "risk appetite" of an organisation to assess the risk. We advise very strongly against using risk appetite as a proxy for the potential impact and likelihood of an identified risk. These need to be applied first, then risk appetite can be used to decide how much, if any, mitigations are needed.

# What are the cultural issues impacting network infrastructure management?

The biggest issues you'll have with managing network platforms and making them just another part of your general cloud infrastructure, are probably cultural. Organisations workflows have been changing rapidly. New techniques and methodologies like DevOps and NetSecOps are changing work practices and relationships. The widespread use of third party networks means realignment of resources around end-to-end workflows that involve significant levels of service provider interaction. In the light of the changes, IT leaders have been making it clear that their biggest challenge in troubleshooting applications, networks, servers and storage, is finding requisite talent to solve performance issues. A cloud, app-oriented culture doesn't encourage the development of the low-level technical skills you'll need, especially across all platforms, including legacy systems of record. You will need people who can think technically and converse on a business level at the same time, and such people aren't common. Moreover, such technical experts as you do have may not feel valued in a world of Apps and "just try it and see". You might end up losing them. The sort of skills you may have issues with include:

- Management of services and service providers, as well as management of on-premises hardware and software contracts.
- Understanding the barriers to effective movement of bits and bytes across the network at the same time as managing the end user experience.
- Managing user expectations while fully understanding the limits imposed by computer science and the laws of physics.

Automation and AI are certainly part of the solution – automation makes it easier to do things when you aren't familiar with the terminology or can't handle the volume of work, and machine learning can capture good practice for the neophyte. Nevertheless, this isn't an issue you can solve just by buying technology, as the introduction of new technology has its own cultural implications.

The solution will involve a focus on education and training, of course, but take expert advice on how you implement this. Possible new skills include SLA negotiation, and management of services, not just hardware, and if you are innovating, you may well not have the requisite skills in-house.

Just giving everyone training that they don't need yet won't work, and nor will pretending that everyone thinks the same way. There is nothing wrong with computer-based training (although face-to-face is better) but supplement it with role-playing in discussion groups, the availability of experienced mentors and so on. And make sure that you give training when the recipient can use it immediately, while it is still fresh in their mind; and rotate technical support around the various roles regularly. A traditional performance specialist may bring order and better user experience (UX) to the cloud app world, whereas a cloud specialist can promote more agility in the world of performance specialists.

Think about recognition and reward. Money is generally a poor motivator (although underpaying people is a strong de-motivator) unless money is the only score-card available, and that isn't a healthy situation. The best motivation is recognition and satisfaction in a job well done, by sending the right messages to your staff. Although, however much praise you give, you won't counterbalance the messaging sent by underpaying people. Similarly, you can't pay people enough to compensate effectively for treating them poorly.

---

“The biggest issues you'll have with managing network platforms and making them just another part of your general cloud infrastructure, are probably cultural.”

---

# Conclusion: Network visibility anywhere

Your network monitoring solution must reach applications and services beyond the edge of the data centre infrastructure. Given today's overwhelming dependence on the Internet and Cloud, comprehensive visibility into ISP and cloud provider network performance is critical. Forward-thinking organisations should be actively evaluating monitoring tools that can extend their visibility out beyond the enterprise data centre to internet monitoring, digital experience monitoring, active testing of network delivery, and network path tracing. Being equipped with such capabilities, you can assure the new 'work from anywhere' experience, that is underpinned by SaaS and Cloud adoption, along with modern network technologies like SD-WAN, and the intersection of networking and security as embodied by SASE. All these capabilities need to be compatible with classic network operations triage workflows that combine alarms, faults, performance, flows, logs, and configuration data available from any part of the new network.

For management to have a high level of confidence Assurance, these new network monitoring capabilities need to be supported by comprehensive and regularly reviewed security, compliance and business continuity plans. And, finally, Assurance will ultimately depend on a right skilled and positively motivated workforce.

“...comprehensive visibility into ISP and cloud provider network performance is critical.”



*Organisations should be actively evaluating monitoring tools that can extend their visibility out beyond the enterprise data centre*

## About the author

### PAUL BEVAN

Navigator,  
Research Director: IT Infrastructure



Paul has had a 40-year career in industry that started in logistics with a variety of operational management roles. For the last 33 years he has worked in the IT industry, mostly in sales and marketing, covering everything from mainframes to personal computers, development tools to specific industry applications, IT services and outsourcing. In the last few years he has been a keen commentator and analyst of the data centre and cloud world. Until recently he was also a non-executive director in an NHS Clinical Commissioning Group.

Paul has a deep knowledge and understanding about the IT services market and is particularly interested in the impact of Cloud, Software Defined infrastructure, OpenStack, the Open Compute Project and new data centre models on both business users and IT vendors. His mix of business and IT experience, allied to a passionate belief in customer focus and "grown-up" marketing, has given him a particular capability in understanding and articulating the business benefits of technology. This enables him to advise businesses on the impact and benefits of particular technologies and services, and to help IT vendors position and promote their offerings more effectively.



## Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

***We'll show you the future and help you deliver it.***

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

## Copyright and disclaimer





This document is copyright **Bloor 2023**. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



### **Bloor Research International Ltd**

-  20-22 Wenlock Road, London N1 7GU, United Kingdom
-  +44 (0)1494 291 992
-  [info@Bloorresearch.com](mailto:info@Bloorresearch.com)
-  [www.Bloorresearch.com](http://www.Bloorresearch.com)