Cloudbrink Report Summary Edition

A Broadband-Testing Report

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process. Gold Award is only available for a mixed vendor test.

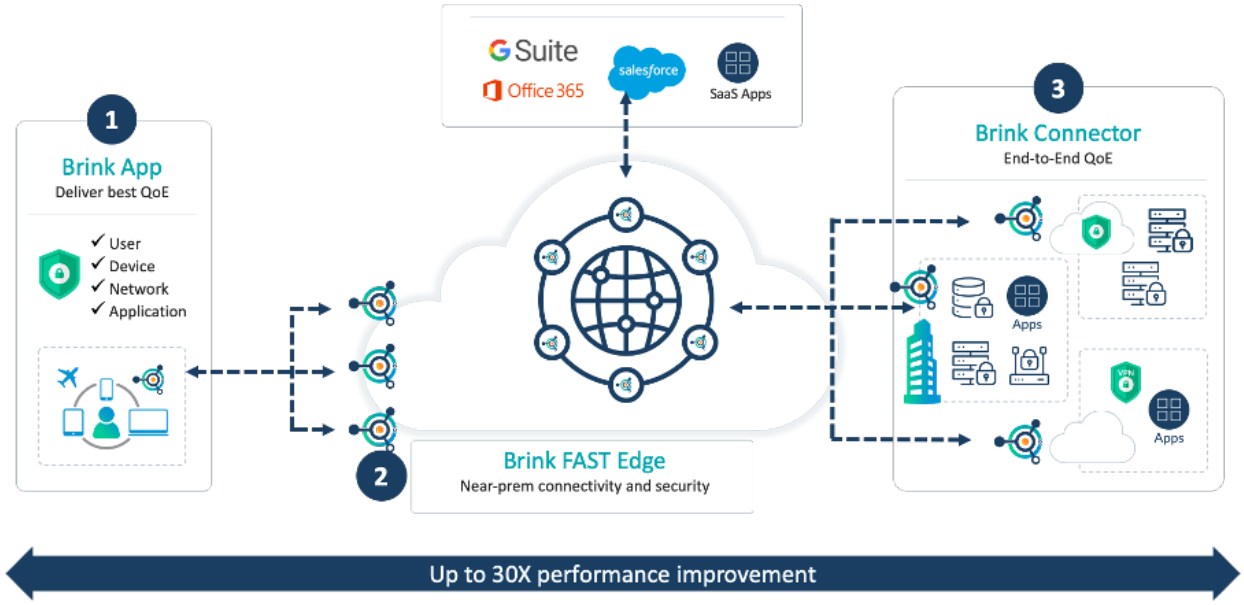
Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

CLOUDBRINK TESTING: SUMMARY & CONCLUSIONS

- Broadband-Testing was requested to carry out a product test and report for Cloudbrink to demonstrate the potential benefits its technology brings to application, data and service delivery globally. Please note: the full report is available for download from here: [Add URL linking to report on Cloudbrink website]

- For the performance testing we created a test environment that enabled us to test in ideal conditions and then simulate real-world conditions in different environments, but adding packet loss and latency. Our aim was to measure the impact of using Cloudbrink versus a "vanilla" configuration by creating a series of file transfer tests, combining different file sizes with varying levels of impairment, starting at zero and working through several iterations of increasingly challenging, real-world network states – see results summary later.

- Why is Cloudbrink required in the first place? The ever-increasingly complex IT landscape has reinvented the need for new forms of network optimization, security and management. Contemporary hybrid networks have effectively superseded the existing tools that were designed for a different kind of network topology and deployment. From an optimization perspective, even if we argue that – over the past two decades – uptake of such technology has been underwhelming (after all, who wouldn't want to optimize their application and data delivery?). there can be no argument now. Hybrid cloud/private networks mean more locations, more routes, more nodes and – therefore – more latency issues. Factor in the enormous increase in real-time traffic (especially video) as a result of the pandemic and that whole WFH/WFA (Work From Home/Anywhere) initiative, commonly called the "new norm" and those latency issues become greater than ever.



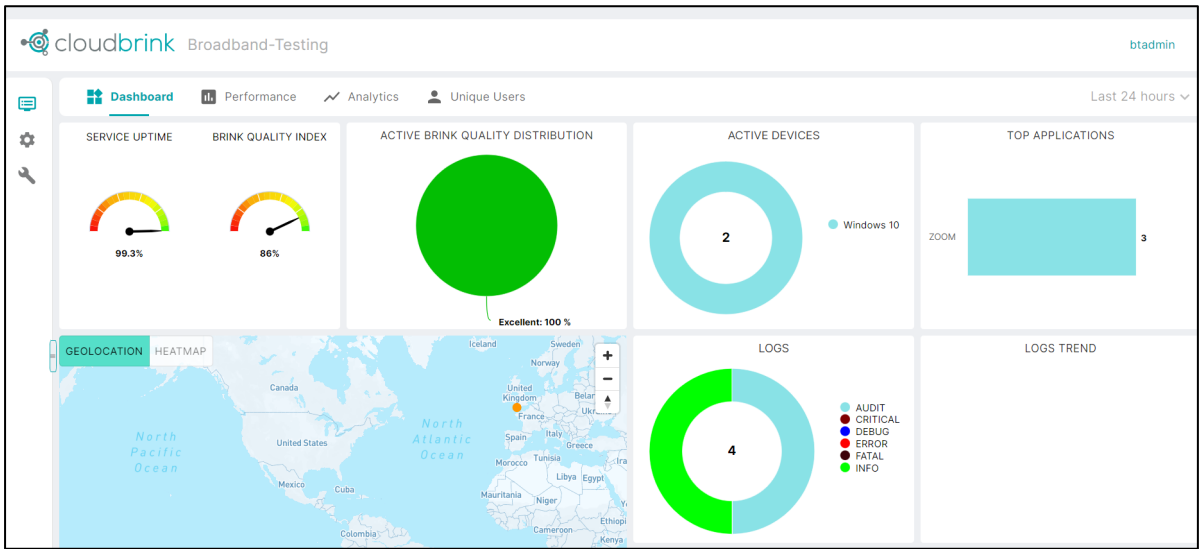
- The performance issues are further highlighted by the modern – and now almost de facto – method of delivering everything: software applications, platforms, unified comms and all – as a service. The lack of proximity to the closest delivery point (such as a PoP – Point of Presence) for many of these XaaS providers creates further latency and general performance issues, especially in areas of the world which are less well covered by the broadband and mobile operators.

- Those same hybrid networks have also created a significant security management question – how does an incumbent edge and centralized security infrastructure protect a hybrid network, where locations are not only both private and public, but where those public locations also vary – and without visibility? Hence there has been much talk of Zero Trust Network Architecture (ZTNA) and many offerings by many vendors, but the reality is that not all ZTNAs are equal.

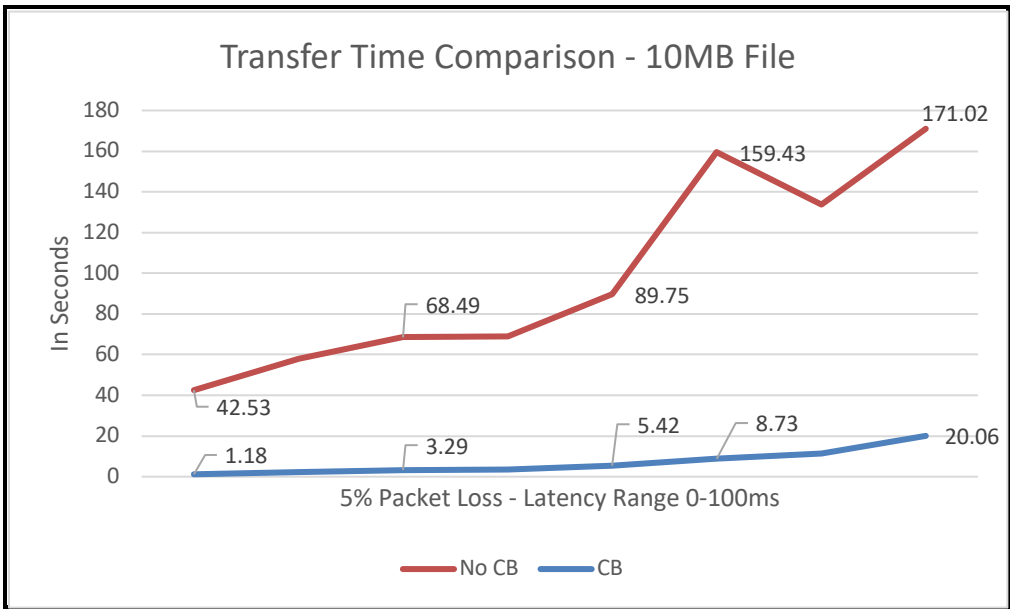
- Cloudbrink is looking to resolve all of the above problem areas with its take on delivering a software-based network architecture that meets the needs of the next generation of IT, both optimizing performance and securing those connections.

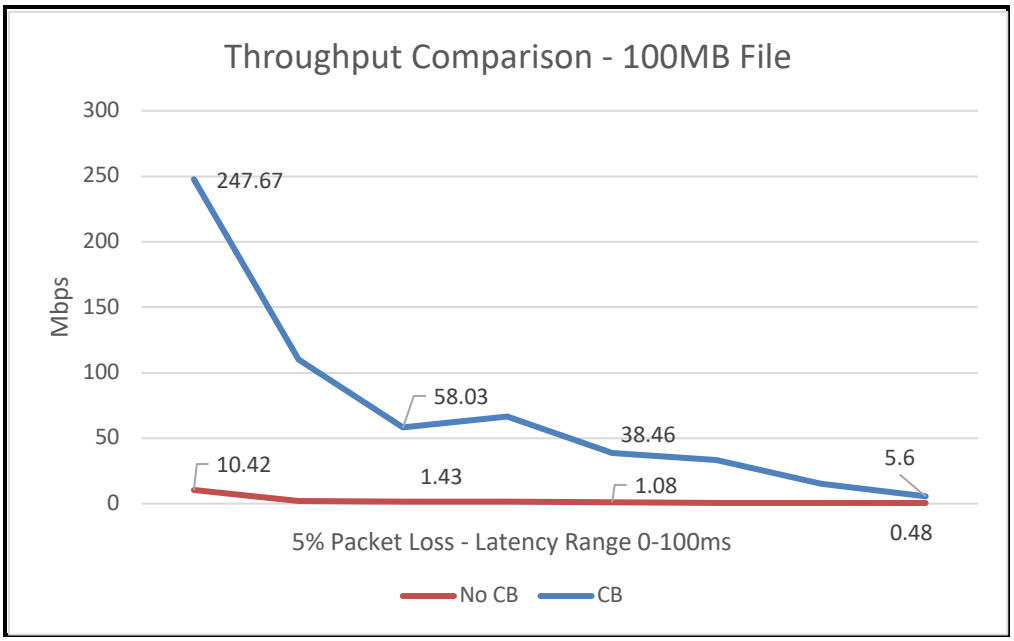
- From a security perspective, at the heart of a ZTNA is primarily TLS (Transport Layer Security) which has seen various updates, with v1.2 having been widely adopted. However, some fundamental flaws in TLS 1.2 resulted in the release of 1.3 to resolve those issues. Cloudbrink is keen to stress that its adoption of mutual TSL 1.3 is total – throughout its architecture, in every link of its communications chain – rather than a partial adoption, which can actually create more security issues than it fixes. It is also completely in line with Gartner's AMTD (Automated Moving Target Defence) definition enabling security teams to constantly change the attack surface, making it harder for attackers to identify and exploit vulnerabilities, such as rotating security certificates every 8 hours.

- A single management portal acts as both a user/admin configuration tool and as a monitoring system for user activity, performance, analytics and overall status. It can also be used to troubleshoot user issues.



- From a performance perspective, Cloudbrink claims up to a 30x performance improvement, but we found in a number of scenarios that this figure could be readily – and hugely in some instances – exceeded, especially when network conditions (latency, packet loss etc) become more challenging. At every data point, the Cloudbrink solution increased throughput and reduced transfer time, even in perfect network conditions.





- Note, this is in a fully secured test environment too; in past tests using VPNs, for example, we have seen up to 50% performance loss, simply because of the secure tunnelling of the

connection. In Cloudbrinks case, this is a complete ZTNA delivery model but performance was hugely accelerated, regardless.

- With such extensive changes in the networking landscape of recent, most networking deployments – if not all – require re-engineering and optimising. Older methodologies were simply not designed to manage a modern hybrid network that sees user endpoints, data and applications liberally strewn across the globe – and with regularly changing locations. Equally, the security challenge becomes not simply ever more intense as more and more threats emerge but, because of this huge decentralising of IT, the surface area to attack becomes ever larger.

- What Cloudbrink has achieved with its contemporary take on a network architecture is to both reduce that security threat and massively improve network performance. Even in ideal networking conditions we saw benefits from using Cloudbrink, but in a challenging network environment, with increase packet loss and/or latency, those benefits become of ever-increasing value.

- Overall, Cloudbrink has created a network delivery architecture that seems tailor-made for the contemporary hybrid networks and "everything as a service" IT world we now inhabit. It is designed to secure and accelerate performance of the user connection, wherever they might be, yet is all defined, supported and controlled from a single point of management, itself available from anywhere.