Independent market research and competitive analysis of next-generation business and technology solutions for service providers and vendors

HEAVY READING
CUSTOM REPORTS

Connectivity and Cybersecurity in the Transformative Cloud Era:
The Jisc Case Study

A Heavy Reading case study produced for NETSCOUT

NETSCOUT®

AUTHOR: JIM HODGES, CHIEF ANALYST, HEAVY READING

INTRODUCTION

The impact of services digitization and the migration of applications to the cloud is transformative for end users and enterprises of all types. Among these end users are academic and research institutions that already rely on the agility of the cloud to gain access to leading-edge research tools and teaching resources. Such resources will drive the next wave of technology innovation.

In response to these needs, companies such as Jisc in the U.K. are creating technology and security strategies to deliver cloud services. Jisc's roots go back more than 30 years, when it was formed as a nonprofit to support universities and research facilities in England, Scotland, and Wales. While Jisc's role and value proposition have not fundamentally changed, digital technology adoption is driving the company to evolve and turn to the cloud.

This case study documents the steps and strategies that Jisc has implemented to enable its academic and research members to thrive in the cloud era. The study is based on an interview conducted with a senior security architect from the Jisc network team.

THE TRANSFORMATIVE CLOUD

The cloud is transformative on both a technological and business level. On a business level, while higher education and research faculties require advanced tools and capabilities, research and operational budgets are finite resources that must be carefully managed.

Since cloud computing represents the most cost-effective compute model, it has garnered a strong level of business support in the academic and research sectors. On the technology side, the inherent agility of a flexible software environment is critical to scale existing services and cost-effectively launch new intelligent connectivity services.

In response to these drivers, Jisc's network and service delivery strategies have continued to evolve over the past few years. Currently, Jisc provides connectivity and consulting services to users from the academic and research membership-based administrations that fund the company. These services fall into three categories:

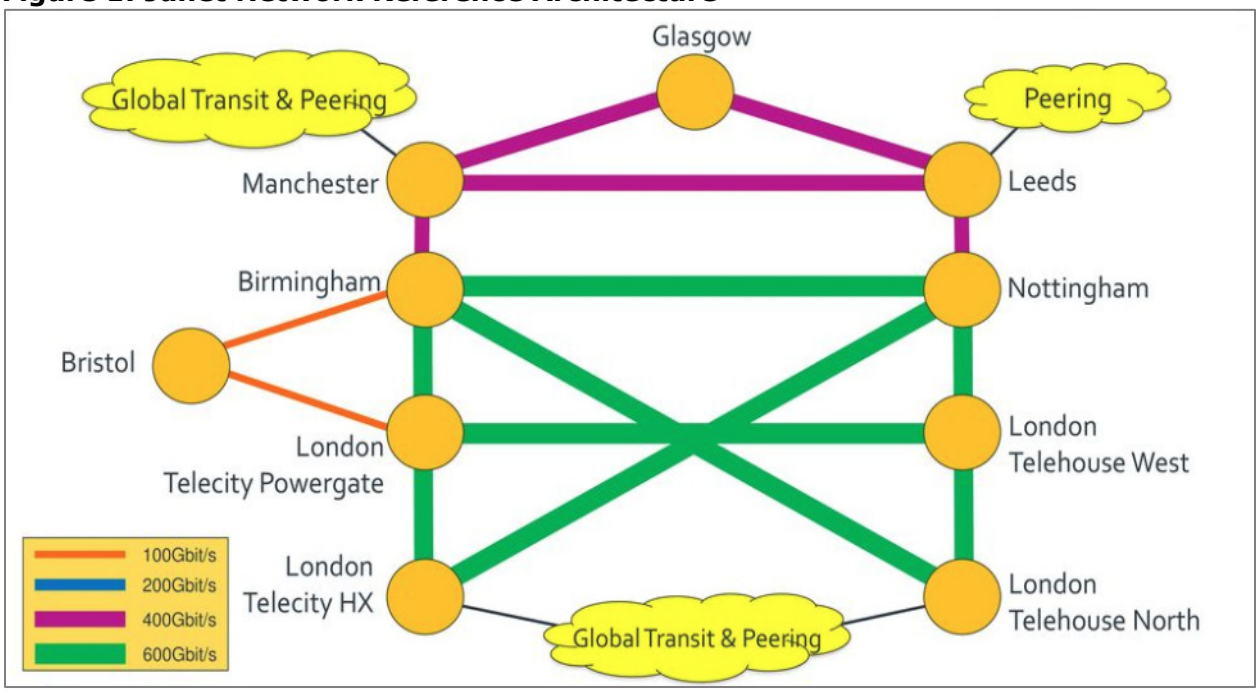
- **Connectivity:** Connectivity trust and identity services
- **Cloud:** Consultancy, support, and reseller of services
- **Cybersecurity:** Support of a suite of security services, including distributed denial-of-service (DDoS) mitigation

Jisc's Connectivity and Cloud Strategy

Stable and scalable **connectivity** is the lifeblood of any successful academic or research organization. In order to meet these requirements, Jisc utilizes its own purpose-built network – the Janet Network.

As shown in **Figure 1**, the Janet Network is a high-speed data network designed to provide highly scalable connectivity throughout the U.K. It does so by utilizing a series of peering and global transit points.

Figure 1: Janet Network Reference Architecture



Source: Jisc

Jisc continues to upgrade the Janet Network to support 400 Gbps and 600 Gbps optical backbone interfaces in the network. These upgrades meet the connectivity demands of Jisc's largest bandwidth-heavy clients. They also utilize existing installed connectivity to cost-effectively meet the much lower bandwidth requirements of its smallest clients, which is crucial from a cost perspective.

Another reason why bandwidth flexibility and programmability are so important is that Jisc's clients are now focusing on utilizing **cloud**-based applications such as Microsoft Azure to enhance research and teaching outcomes. To accommodate the integration of software as a service (SaaS), application scalability and low latency access is vital. Janet meets these stringent demands by supporting more than 600-plus global peering and transit points connecting more than 18 million clients to cloud services.

Jisc's Cybersecurity Strategy

The third essential component of Jisc's strategy is a comprehensive, scalable, and programmable **cybersecurity** strategy.

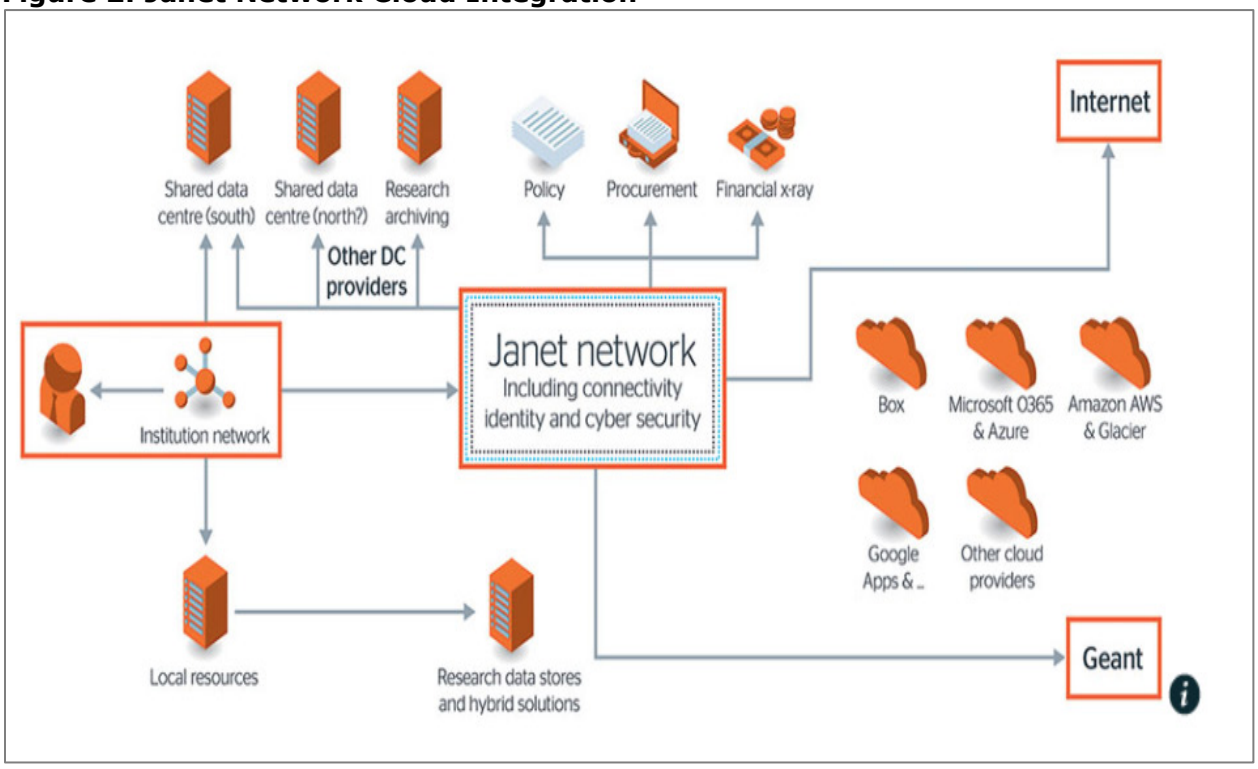
Jisc's Cybersecurity Strategy – Present Mode of Operation

Jisc's current cybersecurity strategy is based on the premise that any network connected to the cloud is seeing a constant rise in the cyberthreats designed to disrupt services access via DDoS attacks. It is also seeing data exfiltration threat vectors designed to steal high-value digital content.

In order to gain deeper insight into Jisc's cybersecurity strategy, Heavy Reading interviewed Lee Harrigan-Green, the chief security architect from the Jisc E-Infrastructure Division.

The first key point Harrigan-Green confirmed was that the integration of the Janet Network with cloud services, as depicted in **Figure 2**, was driving a greater focus on cybersecurity service delivery for Jisc's clients beyond basic connectivity.

Figure 2: Janet Network Cloud Integration



Source: Jisc, The Future of Cloud Computing

In the words of Harrigan-Green:

> *"We started first by integrating cloud providers such as Microsoft and AWS into the Janet Network by supporting direct peering. This was an important first step because it allowed us to create a cloud framework that lowered access costs for our users. As a nonprofit, we pass the savings along directly to our clients which are less expensive public internet access rates. The other important consideration is that our clients can forego the costs and complexity of having to negotiate commercial deals with cloud providers."*

However, the advance of cloud services has also driven Jisc to expand the scope of the services it delivers to clients. These services are listed in **Figure 3**.

Figure 3: Jisc Services Portfolio

Capability	Description
Anti-spam	Anti-spam solutions for detecting and eliminating viruses and spam mails.
Computer emergency response team/ Computer security incident response team (CERT/CSIRT)	A single point of contact for users to deal with computer security incidents and prevention.
Cloud storage	Browser-based virtual storage service for individuals.
DDoS mitigation	Tools and techniques for mitigating DDoS attacks.
Domain name registry	Administration/registration of top- and second-level domain names.
Eduroam	Inter-WLAN service to facilitate easy and secure internet access for roaming educational users.
Housing/co-location	Hosting of user equipment in a managed data center.

Source: Jisc, https://compendiumdatabase.geant.org/reports/nrens_services

The inclusion of DDoS mitigation and CERT/CSIRT capabilities is significant and has helped shape the evolution path of Jisc itself. According to Harrigan-Green:

> *"DDoS has become a critical service. It has transformed us into a managed security services provider. We now have a portal that members can utilize if their networks have been attacked so we can provide DDoS support. This is a high-value service for our clients since it ensures that fit for purpose means not only access but also fit for purpose from a security perspective. The key here is flexibility, the solution we have implemented from NETSCOUT provides the necessary level of flexibility to enable us to tailor DDoS protection for members of all sizes. Like access, security is not a one size fits all proposition."*

In addition to DDoS services, as noted in **Figure 3** above, Jisc also enhances the security of domain registry services. According to the interviewee:

> "*We are the domain provider for .AC.UK – so we provide these services for our members. We focus on policies to enforce eligibly criteria, to block rogue entries, and to eliminate domain squatting. We are continually examining our security requirements in a registry context and also implementing new security measures like DNS blocks or resolver-based services."*

Like any managed security service provider, Jisc must remain progressive and vigilant to stay ahead of more complex rapidly evolving threat vectors. To accomplish this, the company relies heavily on the security vendors it works with. As summarized by Harrigan-Green*:*

> *"… because of the speed and reach of the Janet Networks we rely on our vendors to provide the necessary tools and services – as a nonprofit we don't have the R&D budget to do it on our own. We do have R&D to build services, but not for the underlying technology – so the relationship with the security vendor is critical."*

Jisc's Cybersecurity Strategy – Future Mode of Operation

Jisc's cybersecurity strategy also has a future mode of operation focus. According to Harrigan-Green, the company is now examining how to unlock the value of the data running over its network. There are two use areas to consider here.

The first area is student-focused:

> *"We are developing analytics-based services that allow members to look at student behaviors to enhance the student learning experience. This important for helping institutions identify at-risk students much like you would in the commercial world to minimize customer churn. In this case, we are capturing the relationship between lack of access to books or digital content and drop out metrics."*

The second area is to apply analytics to network data. According to Harrigan-Green, some members often struggle how to aggregate and understand what the data means in a security context. Instead, they rely upon Jisc as a managed service provider to deliver meaningful security-based analytics data.

While analytics is valuable as a standalone resource, Harrigan-Green also felt that in the future, the pairing of analytics with automated processes would further push its members' maturity in the security landscape. This combination will use more than one of the security services that Jisc offer:

> "*We have already started this journey we are developing AI and analytics-based services – using analytics-based real-time data trends. This is a strategic position for us going forward. We are developing managed security services leveraging NETSCOUT's DDoS portfolio which supports the use of automated tools."*

In wrapping up the discussion, Heavy Reading asked Harrigan-Green how the advance of automation would affect relationships with security vendors. The interviewee indicated Jisc would likely see a greater focus on cloud-certified products and greater two-way feedback between managed security service providers and their vendors:

> *"Although we are not a solution engineer, we do have hands-on experience in applying leading-edge security solutions in commercial networks which is valuable for security vendors who require a gap assessment as they design their next-generation products. Similarly, we expect we will also rely on our security vendors more since they have a lot of insights into the current threat landscape that is valuable when we are planning software upgrades, cutovers, or introducing new managed security services for our members. At the end of the day, for both parties, a sense of trust is vital for staying ahead of both current and future threat curves."*