United Kingdom

National Cyber Security Centre balances user needs and security using the cloud

Nova South, in London, is home to the National Cyber Security Centre

The UK government formed the National Cyber Security Centre (NCSC) in 2016 in support of a national ambition to make the UK the safest place in the world to live and do business online

Challenge

The UK government formed the National Cyber Security Centre (NCSC) in 2016 in support of a national ambition to make the UK the safest place in the world to live and do business online. The project leveraged expertise from several bodies with different IT systems. This included the information assurance arm of GCHQ, the National Technical Authority for Information Assurance (CESG), which had a record of providing trusted, independent research and intelligence-based service on information security. However, a unified system was needed to strike a new balance between security, usability and functionality. This system would:

1. Be highly resilient and secure for use with official data
2. Support mobile and multi-site working
3. Provide best-of-breed services that users want to work with
4. Set an example for how to build government IT with modern technology.

Users – civil servants and cybersecurity experts at the NCSC – wanted to collaborate and be confident that their work would be backed up. They wanted the same services on all their devices and for work internet to be as good as their home connection. And everything had to comply with NCSC's document retention and Freedom of Information Act obligations.

Solution

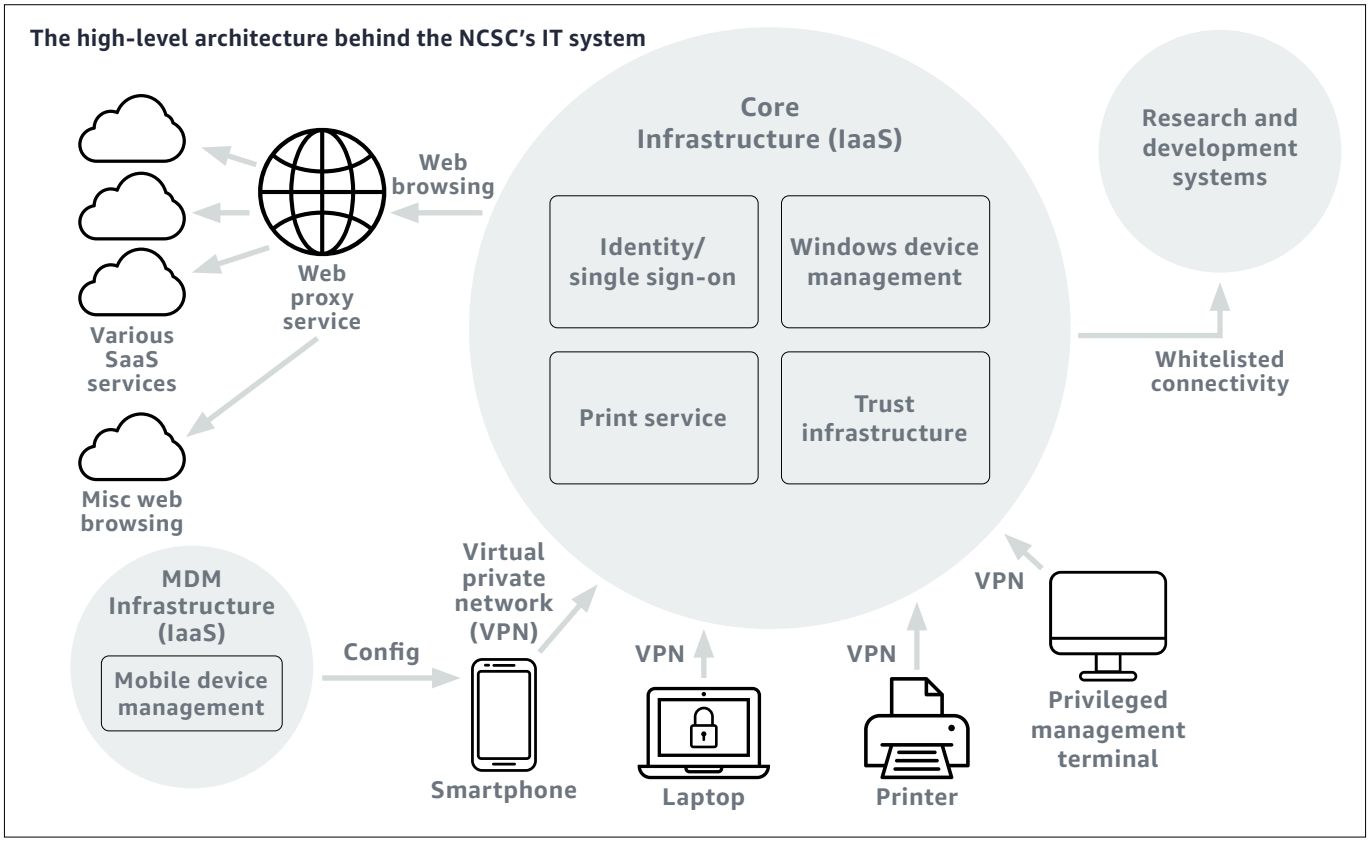
NCSC wanted to be cloud-first and use agile development techniques, so it created a multi-disciplinary team with the authority to make decisions. Some aspects of an infrastructure project are not compatible with Agile techniques, such as elements that need high certainty and predictability, but the team found it possible to build good, secure tech using an Agile approach. The system evolved iteratively, taking sensible risks while building in new functionality.

To assess cloud providers, the NCSC used its own cloud security guidance, matching available services to its 14 security principles. It wanted to use as much of the same software and cloud services as the rest of the tech sector, rather than rely on legacy or bespoke systems, and as much software-as-a-service (SaaS) as possible. This would enable a greater ability to interoperate and collaborate with partners, for example in industry and academia.

However, in some areas, notably device management, user identity and trust infrastructure, the team wasn't confident it could rely on SaaS. In these cases, it opted for an infrastructure-as-a-service (IaaS) model to provide a strong security boundary.

NCSC is confident in its user security because of its control over device provision, configuration and maintenance, combined with strong user-device authentication.

NCSC is confident in its user security because of its control over device provision, configuration and maintenance, combined with strong user-device authentication



Reproduced with thanks to the NCSC

Result

The NCSC created a software architecture from a set of SaaS services, along with the core infrastructure needed, so only trusted devices and users can connect to its resources.

The core infrastructure:

1. Provides a directory of users, devices and other infrastructure
2. Authenticates users and devices and provides single sign-on to let users reach cloud services
3. Provides filtered and protected internet access
4. Maintains secure configuration of devices
5. Manages software deployment to devices
6. Provides the means for specialists to connect to niche systems.

The resulting system balances user needs and security. Users have the tools and capabilities that work for them because a well-designed IT solution draws on the best of commodity technologies. At the same time, there is effective risk management.

Acknowledgement: Ian McCormack, deputy director of the Government Team, NCSC; Richard Crowther, deputy technical director; Carolyn Ainsworth, head of engineering