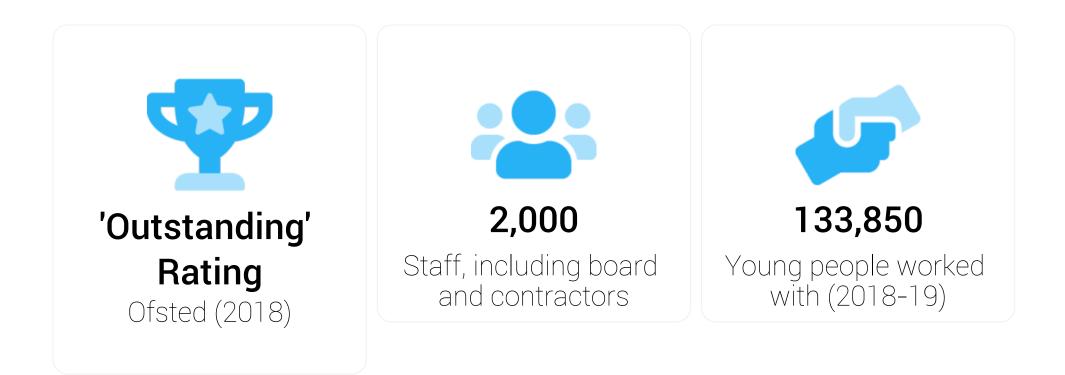# iboss cloud becomes an integral part of the Cafcass cloud architecture by providing cloud security that seamlessly integrates with the NCSC Protective DNS Service

Learn how the largest employer of qualified social workers in the UK leveraged iboss to prevent malware, phishing, and other cyberthreats

Quick Facts About Cafcass

'Outstanding' Rating
Ofsted (2018)

2,000
Staff, including board and contractors

133,850
Young people worked with (2018-19)

The Challenge

Matching the needs of an advanced cloud-based government organisation

When adults are deciding where a child should live or when a local authority has serious concerns about their safety, the family court may ask Cafcass (Children and Family Court Advisory and Support Service) to help it make decisions about their future.

Cafcass is the largest employer of qualified social workers in the UK and independently advises the family courts in England about what is safe for children and in their best interests when parents have separated or divorced, are in care proceedings, or in adoption cases. Cafcass supports more than 130,000 children every year by understanding their experiences and speaking up for them when the family court makes critical decisions about their futures.

Like any government organisation, Cafcass is under constant scrutiny when it comes to the security of its IT systems and data, and its role in safeguarding children and young people magnifies this requirement. At the same time, it is also expected to demonstrate clear value for money for any investment, including its information systems.

Through its commitment to identifying solutions that improve how the organisation supports children and families, Cafcass has a forward-looking approach to technology, not least the decision to migrate its IT infrastructure to the cloud. This has dramatically reduced the cost of IT management, including the need to patch and update software. The resulting budget savings have been diverted to front-line activities.

Robert Langley, CIO and Head of IT and lead for the organisation's cloud initiative, says: "We migrated most of our infrastructure to the cloud from 2016 onwards. By 2018 we had retired the last of our on-premise physical servers."

Seeking a unique connection to the cloud

Maintaining cutting-edge cyber-security is a core element of the Cafcass cloud strategy. This includes protecting the organisation and its data from cyber-criminals and other online risks. With the launch of the government's own protective system, PDNS (Protective DNS) in 2017, and especially as the requirement to use it was extended to organisations such as Cafcass in late 2018, Peter Clark (Technical Analyst and security lead) was keen to connect Cafcass with the latest security features available through the new technology.

Created by the National Cyber Security Centre (NCSC), PDNS prevents access to malicious domains by not resolving them. This shields end users from malware, ransomware, phishing attacks, viruses, malicious sites and spyware. PDNS also stops malware already on machines from calling home, again making cyber-attacks less effective. Unlike commercial competitors, PDNS is supported by the British intelligence community in gathering and using data to protect government organisations from targeted threats.

Cafcass had an incumbent solution, but this was focused only on DNS-based protection, inspecting queries which translate domain names to IP destinations. But the Minimum Cyber Security Standard (MCSS), which is defined by NCSC, demanded that Cafcass do more to protect its staff and data, including scanning traffic (whether encrypted or not) for malware.

Moving to an alternative secure cloud gateway was the obvious solution, but there was another challenge: Integration with PDNS requires that the source IP address for DNS requests be identifiable as coming from Cafcass. This wasn't possible with the current solution, where source IP addresses could come from Cafcass offices, personal broadband, mobile hotspots or public WiFi. Cafcass needed a solution that would funnel all its DNS requests through a specific list of IP addresses.

The Solution

Integrating the cloud with PDNS

Clark began investigating how best to connect with PDNS at the start of 2019. He and his colleagues identified two potential partners, including iboss. But the question remained. Was it possible to integrate either of the cloud solutions with PDNS?

"From the outset we were determined to avoid any architecture that required us to reintroduce on-premise hardware and software or use IaaS," says Clark. "We wanted a direct connection via the cloud with PDNS, but we were aware that most cloud partners don't offer the unique IP address space needed to achieve this."

Unlike other cloud security solutions, the iboss cloud provides 100% dedicated IP addresses to their customers. This allows users to always present a source IP that is associated with their organisation, whether they're in the office or on the road. For a large organisation that has many operations taking place at remote sites, this simplifies their integration with third-party services that restrict access to the organisation's IP range. This capability allows the iboss cloud to be integrated PDNS.

"We were impressed by their flexibility and the way they were able to configure our DNS to point at a different service. This meant we didn't lose any of the protection offered by PDNS. Not all vendors are so flexible, and it soon became clear that the other business in the running was far less able to adapt to our requirements," says Clark.

Another attraction of the iboss solution was the inclusion of protection for mobile devices in the same license package that protects their laptops. Clark says, "iboss are working with us to deploy their iboss Cloud Connector to our iOS managed devices. Our staff can be protected by consistent security policies wherever they log on."

Now that the Cafcass-iboss solution was 'pure cloud' it was possible to start migrating from the legacy content-filtering system. Clark says, "Speed of deployment was impressive. Migration from the legacy solution to iboss cloud user acceptance testing and roll out took place in a matter of weeks."

By the beginning of September 2019, iboss was up and running and Cafcass was fully protected by PDNS. The entire process from market research to deployment took less than six months.

The Results

We asked iboss to address this challenge and were struck by how quickly and effectively they came back with a solution. Not all vendors are so flexible.

Peter Clark
Technical Analyst | Cafcass

A versatile platform and multiple layers of security

By the beginning of September 2019, Cafcass had migrated successfully to the iboss cloud, fully protected by PDNS. The entire process from market research to deployment took less than six months.

"Speed of deployment was impressive. Migration from the legacy solution to iboss cloud user acceptance testing and rollout took place in a matter of weeks," said Clark.

The versatility of the iboss platform allows it to be integrated with other solutions, enabling multiple layers of security. This is useful for organisations that are required to use specific applications or services like PDNS.

The iboss cloud gives Cafcass plenty of options for filtering content. With the included SSL decryption, they can filter websites by web categories, domains, keywords, RegEx patterns, or even HTTP header content. The iboss platform captures useful details about user activity, including usernames and full URLs of sites visited. This makes it easier to identify users who are infected with malware or are engaging in high-risk activity. Like any organisation, Cafcass is at risk from phishing emails that lure the recipient into sharing confidential information. While PDNS blocks embedded links to suspicious sites, iboss scans files before they are downloaded, isolating attachments that pose a risk to the user.

> "We can configure iboss easily, taking into account the day-to-day responsibilities of employees. A good example is research into the impact of drug use where employees are dealing with allegations of illegal behaviour and substance abuse," says Clark.

The iboss cloud includes detailed event logs for auditing and reporting as well as real-time dashboards that help you quickly identify high-risk network activity. Clark and his team get an instant view of their cloud security performance at any time. Reports can be based on predesigned layouts or tailored to the needs of the recipient.

By migrating to the iboss cloud, Cafcass implemented a durable cloud security solution that readily adapts to future changes. They gained secure internet access from any location, though the cloud, integrated with PDNS, and extended their visibility into their network traffic and user behaviour—all while reducing costs.

According to Robert Langley, Cafcass CIO. Cafcass has "retired the last of our on-premise physical servers."

Highlights

These are some of the main improvements for Cafcass after switching to iboss cloud and connecting to PDNS.

Versatile product

iboss enabled Cafcass to deliver a fully cyber-secure environment in 'just one shot'. "We expect to reduce the time spent dealing with malware on laptops, smartphones and other devices significantly," says Clark.

Access to the Ministry of Justice (MOJ) intranet

It is now possible for organisations like the MOJ to 'white list' the Cafcass IP range. This is because all requests for access come via the iboss containerised architecture and not via cloud modified addresses or remote working IP addresses.

Improved return on investment

Unlike other content-filtering technologies, there's no impact on the speed of internet connection or data transfer. "We're far more secure, we work just as quickly, for effectively the same outlay," says Clark.

Uncomplicated licensing

With iboss, Cafcass gets everything it needs for a standard price, and the PDNS integration feature is available at no additional cost. This makes it easy to present a cost-benefit analysis and justify the investment to budget holders.

Greater efficiency

iboss is now a critical part of the Cafcass cloud architecture, reducing the costs of IT maintenance while enabling the organisation to move resources to front-line activities.

About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organizations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

To learn more, visit https://www.iboss.com