Balancing Data Access and Security Supports This Hospital's Highest Priority—Patient Safety

The major UK hospital reduces security incidents by over 99% while better safeguarding patient data.

With no other choice, this hospital had to report a lost USB drive with sensitive data to the UK's Information Commissioner's Office—requiring board-level visibility. For the organization's IT leaders, reducing data vulnerabilities rocketed to the top of their priority list. They turned to Forcepoint for a solution that transformed them into a model for data security in UK healthcare.

CUSTOMER PROFILE:
This healthcare delivery network serves nearly 1 million patients per year with a staff of 6,000.

INDUSTRY:
Healthcare

HQ COUNTRY:
United Kingdom

PRODUCTS:
- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint DLP

By 2017, the world had become grimly accustomed to destructive cyber viruses and malware attacks. A number of the world's largest companies had, more than once, discovered just how vulnerable their IT environments really were. So when the WannaCry ransomware attack paralyzed computers all over the world, it was just the latest—and one of the worst—example.

The attack hit NHS facilities in the United Kingdom particularly hard. Hospitals and medical facilities that normally provided critical and important care were locked out of devices, forced to shut down systems, cancel appointments, and divert emergency services. It was a hospital IT professional's worst nightmare, come to life.

> "We had a real incident, and we needed to do something about it."
>
> HOSPITAL INFORMATION MANAGEMENT AND TECHNOLOGY DIRECTOR

This hospital, however, remained unscathed—thanks to the help of an integrated Forcepoint solution that helped them safeguard their environment.

Committing the resources for security health

Perfectly secure cyber environments are impossible to achieve under the best of conditions. For national healthcare organizations, it can be even more challenging, since their IT environments are often older than those in the for-profit sector while the stakes are higher—protecting not only the most sensitive of patient data, but ensuring access and availability of that data when lives are on the line. Tightening budgets for NHS organizations make cybersecurity challenges more difficult and force staff to do more with less. Or, as Forcepoint sales representative Nadim Alam said, "Often, the money doesn't come until a significant event is discovered."

The hospital came face-to-face with their significant event when a USB drive storing sensitive data was lost. It was forced to report the breach to the ICO (Information Security Commissioner's Office), requiring board-level visibility.

Prior to this data loss incident, the hospital was in a better position than many public sector organizations. It had a comprehensive cybersecurity infrastructure including firewalls, encryption, intrusion and hacking detection systems, and Forcepoint Web Security and Email Security solutions. This infrastructure performed very well on an annual penetration test run by NCC, a CESG-approved third party.

But with a data breach that could potentially cost the organization up to £500,000 in fines, the hospital knew it had to go further with a dedicated data loss prevention solution.

The hospital's Information Management and Technology Director said it simply: "We had a real incident, and we needed to do something about it."

Fingerprinting 1.6 million patient records to safeguard data beyond the network

Since the hospital already relied on Forcepoint for Web and Email Security, it was natural for the organization to extend its protection with Forcepoint DLP.

The initial phase of building the solution involved a close partnership with Forcepoint, during which Forcepoint spent time listening so they could truly understand and document the hospital's needs.

The first issue: the hospital did not know where its data was—on the organization's servers, within employees' personal email, or stored in cloud applications. There were no rules or restrictions in place to keep patient data from leaving the premises. Forcepoint DLP Discovery helped find where all sensitive data was located across endpoint devices, networks, and cloud apps. This helped to provide a scope for the project and a map for protection.

Challenges

Protecting 1.6 million patient records without restricting necessary access and slowing down patient care.

Approach

Boost data security by locating sensitive data and implementing processes around movement with Forcepoint DLP.

From there, the team discovered which data and activities demanded careful monitoring and began to outline basic operating rules. The analysis revealed information on non-routine transactions—such as when sensitive data is sent to an unexpected person. This would allow IT to reach out and ask for more context.

The next step took the organization even closer to the data. Fingerprinting each one of the hospital's 1.6 million patient records helped the organization monitor data movement and apply appropriate controls both internally and if data left the premises.

Finally, Forcepoint helped the hospital tailor the out-of-the-box process templates to ensure that the movement of these critical patient records and other data wasn't blocked unnecessarily. "If you make it unworkable, it will not be any use to anyone. We had to get a balance," said the organization's IMT Director.

Implementation took just one month and, given the complexity of the typical security installation, the security team was impressed. "It exceeded our expectations because it was quick," the director said.

With every breach prevented, the solution pays for itself

Results were also quickly positive: while previously there were 6,000 to 10,000 security incidents the IT staff were required to investigate each month, rigorous filtering reduced that to just 10–20 marked for review by the hospital's information governance manager. This reduced number of alerts frees up management's time to investigate risks likely to pose the most threat to the organization.

Once fully deployed, it was clear the solution ran smoothly, required little maintenance, and provided the visibility needed to monitor the flow of data in the hospital. And as for ROI? "If we lose data, we potentially have a fine of £500,000, and we spent far less on the solution. It is an investment to safeguard the patients; we are talking about you and me—our data being safe," said the IMT Director. For each individual data breach prevented, the solution pays for itself.

Justin Hedley, the Forcepoint engineer serving the hospital's technical needs, adds, "Customers using our DLP are protected from breach. But they also have the information to be able to report relevant information to the authorities, if they ever need it."

From losing a USB drive to a model of safety

Perhaps the hospital's biggest return on their relationship with Forcepoint was realized in 2017, when the ransomware attack WannaCry paralyzed computers all over the world—and hit NHS facilities in the UK particularly hard. Hospitals and medical facilities that normally provided critical and important care were locked out of devices, forced to shut down systems, cancel appointments, and divert emergency services. With an integrated solution of Forcepoint Web, Email, and DLP, this hospital remained unaffected. Afterward, the IT team was even more confident about security, knowing that should another significant attack come, they're well prepared.

10,000

security incidents requiring high-level investigation ***before*** Forcepoint Web, Email, and DLP

20

security incidents requiring high-level investigation ***after*** Forcepoint Web, Email, and DLP

Results

Reduced security incidents requiring high-level investigation from 10,000 per month to 20 per month.

Avoided infection from 2017 WannaCry attacks.

Standardized Forcepoint cybersecurity solutions across organization helped expand trust.

"It exceeded our expectations because it was quick."

HOSPITAL INFORMATION MANAGEMENT AND TECHNOLOGY DIRECTOR