Forcepoint

Solution Brief

Secure Your Hospital's Staff and Data, Wherever They Are

Flex to protect with a single, converged service for web, data, and cloud security

Challenges

- **The disruption of telemedicine:** More clinicians are working remotely and providing consultations via wireless networks and videoconferencing.
- **Drive-thru COVID-19 testing:** Pop-up testing sites require remote access for EHR data entry.
- **Temporary medical facilities:** ICU units have been set up in parking lots and other spaces beyond hospital security perimeters.

Our Solution

Forcepoint Cloud Security Gateway

- Delivers web, data, and cloud security in a single, cloud-delivered, centrally managed service.
- Protects remote staff from malicious attacks with deep-content inspection, cloud sandboxing, and remote browser isolation (available as an add-on).
- Secures staff access from anywhere to on-premises patient/medical data and business-critical cloud applications.
- Provides controls for BYOD, managed devices, and real-time compliance.

Benefits

- Protects remote teams as they use the web, email, and cloud.
- Stops malware, viruses, and phishing, wherever staff is working.
- Provides complete web and data protection with uniform policies for every user, everywhere.
- Uncovers risky cloud applications and Shadow IT while securing cloud access across your organization.
- Single-vendor, converged solution.
- Streamlines compliance with HIPAA and other regulations via predefined policies.

Your clinicians and care staff are on the move, working harder than ever to save lives. Meanwhile, your attack surface is expanding. With Forcepoint, you can secure a smooth-operating future for your hospital.

Forcepoint Cloud Security Gateway (CSG) gives you the fluid and scalable protection you need to flex and adapt in the face of dynamic risks.

Your #1 priority has always been patient care. But in today's digital age, cybersecurity is a critical component of patient safety—even more so as your risk landscape shifts and expands.

The pandemic has changed the way you care for patients. Your employees are working outside your hospital's traditional security perimeters. Maybe you've made emergency technology purchases to secure your data in this new way of working. Most likely, these changes have created new gaps within your existing privacy and security policies and procedures. These blind spots, combined with the use of wireless connections and unmanaged devices by your remote-working staff, create an open invitation to malicious or unintentional data exfiltration.

As you think about how to protect your remote workforce—and the data they work with—consider these questions:

- → **How can we scale** our security to protect our patient and medical data, wherever it is?
- → **How do we identify** risky cloud applications (both sanctioned and unsanctioned)?
- → **How do we securely embrace the cloud** to enable productivity and business continuity without sacrificing security and compliance?
- → **How can we secure a collaborative environment** for our distributed care teams?

Rethinking data protection for your hospital's future

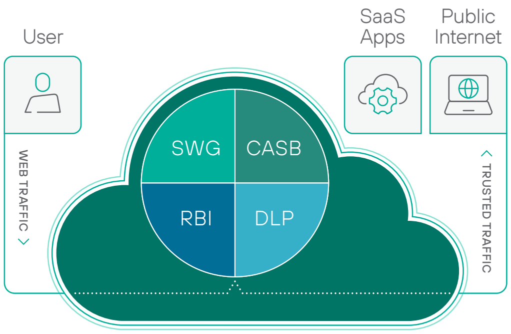
As more of your clinicians work outside hospital walls, more data circulates outside your network. How much data are we talking about? Consider these recent statistics: During the COVID-19 lockdown, hospitals saw an 80% increase in the movement of data outside their networks, including a 123% increase in the volume of data moving to USB drives and a large spike in data uploaded to cloud storage services (Data Guardian, 2020).

For cybercriminals, much of this data is extremely valuable. PHI, for example, is 50x more valuable on the black market than personal financial information. But cybercriminals can also target your hospital for other information, such as:

- → **Lab results** they can use for extortion or identity theft
- → **Medical licenses** to impersonate doctors and forge medical documents
- → **Health insurance company login details** to fraudulently submit health insurance claims
- → **Administrative paperwork** to create fake health insurance cards, counterfeit prescriptions, and forge drug labels

Is your security flexible enough to protect all this data as your staff works with it remotely? Have you closed the security gaps COVID-19 has created? How are you planning to scale your protection so your hospital is prepared if another health crisis happens?

Forcepoint Cloud Security Gateway



CSG delivers web, cloud, and data security in a single, converged service that is cloud-native and centrally managed. It provides Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Data Loss Prevention capabilities, all in one SKU.

Also available: Forcepoint Private Access, which provides true Zero Trust access to private applications without the complexity, bottlenecks, and risks of VPNs.

Your people = The new risk perimeter

Wherever your employees are working—inside your hospital or on the go—they are your new risk perimeter. Because of emergency or crisis situations, they may be accessing and sharing data in ways that don't conform to your typical protocol.

Forcepoint Cloud Security Gateway offers flexible and scalable protection to fit your hospital's new reality. It secures your staff's access to public applications via the web and the cloud, regardless of where they're working. With CSG, your critical data and IP are protected with simplified security policy management at reduced costs.

Flexible protection for current and future threats

Forcepoint Cloud Security Gateway empowers you to:

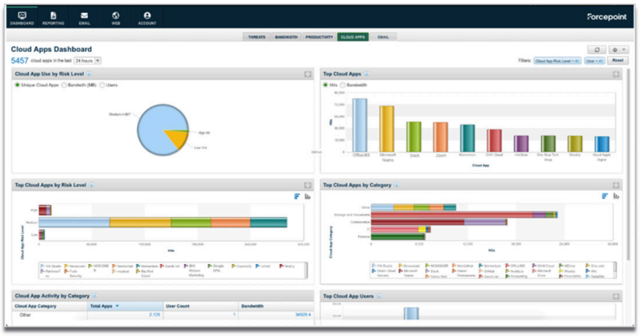
→ Gain visibility into the entire kill chain with deep content inspection, cloud sandboxing, and remote browser isolation (available as an add-on).

→ Identify anomalous and risky user behavior in the cloud to stop malicious users and clamp down on staff activities that don't meet best practices.

→ Reduce the risk of your remote staff exposing PHI and other sensitive data to unauthorized users in violation of governance rules and/or federal, state, and local regulations.

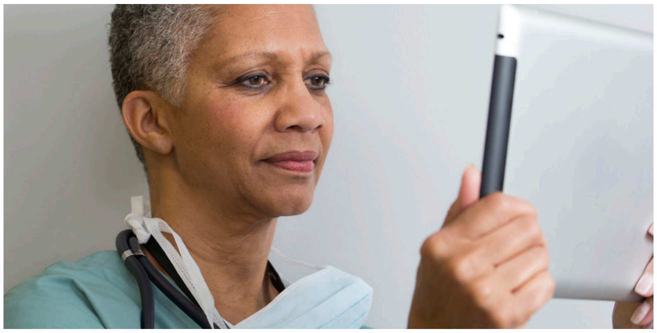
→ Identify potentially inappropriate privilege escalation and implement geolocation-based access and activity monitoring for legitimate remote staff and malicious actors.

→ Protect your clinical and research discoveries from low-and-slow data loss as well as large file theft.



Cloud App Category	Total Apps	User Count	Bandwidth
Other	2,129	1	34929.4

Forcepoint Cloud Security Gateway is the only 100% cloud-native, centrally managed security platform for users and data.



Put your people at the center of your cybersecurity

Wondering what Cloud Security Gateway can do for your hospital? Our cloud security experts will be happy to show you. See firsthand how our converged security service:

→ Reduces vendors and point products

→ Reduces operational overload and corresponding costs

→ Provides uniform web protection and policies for every user, everywhere

→ Uncovers Shadow IT and secures cloud access across your organization

+ Request a hospital-focused demo of CSG today!

forcepoint.com/contact

[Secure-Your-Hospitlas-Staff-and-Data-Solution-Brief-EN] 8Sept2020