

Safeguard Your Clinical Laboratory's Collaboration

Get integrated security for your lab staff and your critical data, wherever they are



Challenge

- › **Cost reduction:** Reduce CapEx while protecting quality and maintaining service levels.
- › **Upsurge in data volumes:** Lab data has exponentially increased, requiring data protection that scales.
- › **Increased data-sharing:** Delivering more value beyond test results requires more collaboration within and beyond your lab walls.

Solution

Forcepoint Cloud Security Gateway

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

Outcome

- › Protects remote teams as they use the web, email, and cloud.
- › Stops malware, viruses, and phishing, wherever employees are working.
- › Provides complete web and data protection with uniform policies.
- › Uncovers risky cloud applications and Shadow IT while securing cloud access across your organization.
- › Streamlines compliance with HIPAA and other regulations via predefined policies.

In the near future, your lab will be expected to deliver more than test results. Your diagnostic guidance will be a critical contribution to better patient health. To advance toward this outcome, you'll need to collaborate more closely with clinicians, pharmaceutical companies, and other outside experts. Within this expanded circle of collaboration, how do you plan to keep your staff and critical data safe?

Many clinical labs came closer to answering this question when they moved to protect their remote staff during the global pandemic. During this time, remote employees introduced new security risks as they collaborated with coworkers, accessed critical data, and shared information from home using email, the cloud, and the web. To address these risks, some labs hastily adopted new security technologies and activated crisis-driven processes. While this approach may have checked the boxes on immediate security needs, it also created security blind spots and added operational complexity.

Forcepoint Cloud Security Gateway (CSG) is a converged service that simplifies your lab's security while safeguarding a collaborative environment for your remote and distributed staff. In short, CSG protects your data everywhere and safeguards your lab staff anywhere.

As you consider how to protect your lab professionals—as well as the data they work with—ask yourself these questions:

- How can we scale our security to protect our patient and medical data, wherever it is?
- How can we secure a collaborative environment for our distributed employees?
- How can we operate "lean," reducing current costs while strengthening our security?
- 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?

CSG can help you achieve all of these goals while laying a foundation for secure collaboration. If your lab intends to deliver value beyond test results (via diagnostic guidance), your staff must be able to collaborate safely with external experts.

Enhanced security with lower CapEX

Chances are, your lab is being pressured to do more with less. You may have felt this squeeze long before COVID-19, as reimbursement cuts dictated by the Protecting Access to Medicare Act (PAMA) were activated. However, tightening your budget doesn't automatically translate into shortchanging your security.

CSG actually lowers your operating costs. Because it is a 100% cloud-native, integrated security service, CSG replaces multiple product categories. With CSG, you get web, cloud, and data security converged into one cost-effective and convenient SaaS service.

Not only does CSG reduce your operational overload, it eliminates the need for—and the costs of—multiple point products while providing fluid and scalable protection for your lab staff and your data. You'll also have one relationship to manage and a single source of support, which means less negotiation, paperwork, and tracking.

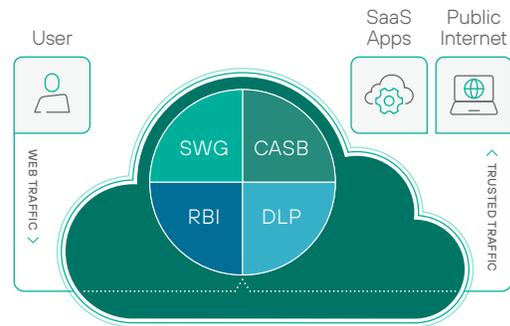
Simplified security

In the future, clinical labs will measure their success by value, not volume. You'll be measuring outcomes, not efforts. You'll be more focused on patient wellness, and less on the number of tests completed. You'll be increasing your collaboration with care teams and other professionals outside your lab.

This will place new demands on your security. How can you prepare? Streamline the solutions you have now and establish a foundation for secure data access and datasharing all the way to the service edge, where phones, laptops, robots, and sensors access the rest of your organization.

Safe access to web content and cloud applications for all your lab staff, everywhere

CSG is a single, cloud-native, centrally managed service. 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 enables true Zero Trust access to private applications without the complexity, bottlenecks, and risks of VPNs.



CSG is a smart security solution for your lab today, because it helps you to protect your users and your data while reducing product overlap, cutting costs, and reducing complexity. CSG is also a strategic foundation for your lab's future because it's an integrated service—not a multivendor product bundle—designed to adapt to the way your lab staff works. The security provided by CSG is human-centric; its protection secures your lab staff as they move through the world, work with sensitive data, and collaborate with other medical professionals. When you choose CSG, you get protection for what you need now—and for what's next.



Your Lab's Security Goals	How CSG Helps You Achieve Them
Decrease operational costs	<ul style="list-style-type: none"> • Reduces vendors and software by replacing multiple product categories with a single product • Gets rid of version management and upgrade overhead • Pares down the numbers of relationships you manage • Offers one source of support for all capabilities
Simplify security management	<ul style="list-style-type: none"> • Provides one interface with single sign on • Removes the need for expertise, appliance CapEx, or hardware lifecycle
Protect lab staff and data everywhere for safe collaboration	<ul style="list-style-type: none"> • Provides uniform protection for users at home, in the main lab, at branch locations, and on the go • Delivers full visibility across premises, remote locations, and in the cloud
Stop malicious cloud and web-borne threats	<ul style="list-style-type: none"> • Integrates zero-day protection for cloud or web-based threats • Detects both static and behavioral threats • Offers a Remote Browser Isolation add-on
Streamline regulatory compliance	<ul style="list-style-type: none"> • Supplies pre-defined regulatory policy templates • Provides one service that unifies governance policy for application and data use
Safeguard intellectual property	<ul style="list-style-type: none"> • Delivers real-time protection against unauthorized data egress to the cloud or web

Put your people at the center of your cybersecurity

Wondering what Cloud Security Gateway can do for your laboratory? 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

Request a demo of CSG today!

Need to bolster your network security?

Ask your representative about our Next Generation Firewall.

→ [Forcepoint NGFW](#)

forcepoint.com/contact