Forcepoint

Solution Brief

Forcepoint CASB Custom Application Mapping

Security for every cloud application

Forcepoint CASB (Cloud Access Security Broker) automatically discovers cloud application use, analyzes the risks, and enforces appropriate controls for cloud applications and services. With Forcepoint CASB, users get the apps they want and IT security gets the visibility and control they need.

The average enterprise customer has over 500 XaaS (Anything as a Service) applications within their environment, but often lacks visibility into which applications are in use. It's not uncommon for IT security to uncover cloud application usage well after the application's introduction into the enterprise. An organization must be proactive in how they monitor and govern these apps and services, as their unchecked use brings elevated risk.

In most cases, IT security will choose to sanction and govern a select number of applications, typically the more common SaaS applications such as Office 365, SalesForce.com, Box, and others. However, cloud adoption in the enterprise is long-tailed—each company will undoubtedly have its own unique mix of secondary and custom applications, otherwise known as "Tier II" or "Tier III" applications (see Figure 1).

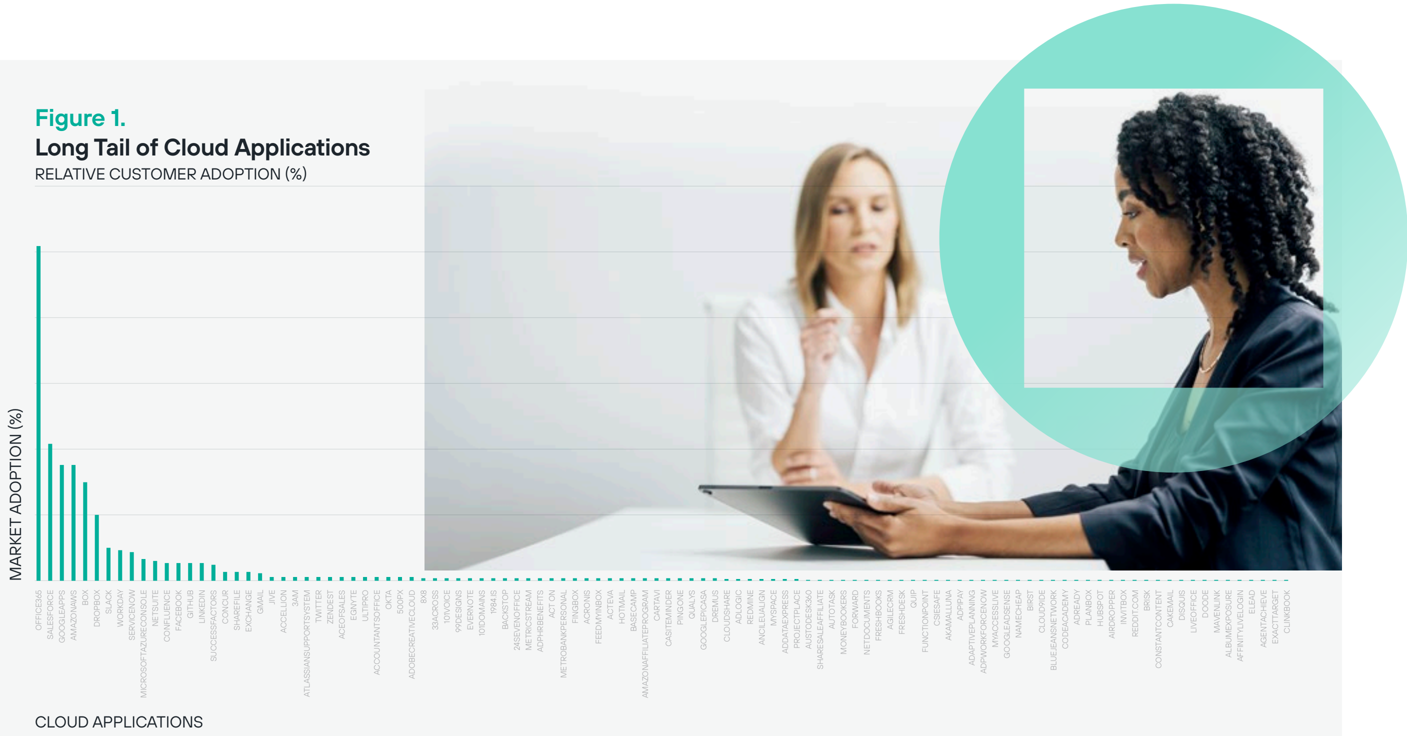


Figure 1.
Long Tail of Cloud Applications
RELATIVE CUSTOMER ADOPTION (%)

While it's possible to "discover" cloud apps using existing infrastructure and certain cloud security tools, they don't provide the visibility and control required for a comprehensive solution. Nearly all CASB solutions have discovery capabilities, but the majority can only secure more common, top-tier cloud applications. A CASB solution should offer both API and inline capabilities, since many Tier II or Tier III applications will not have an API that can be used by a CASB solution.

Forcepoint CASB

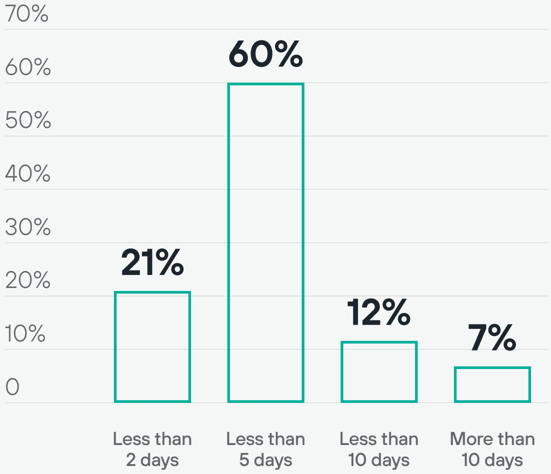
Unlike other CASB solutions, Forcepoint CASB secures any cloud application, whether PaaS, IaaS, SaaS, homegrown web, or cloud applications like HTTP or HTTPS. Its proxy analysis engine is architected to operate out-of-the-box, which allows for quick mapping with regard to each cloud application. Mapping explains to the engine how to interpret traffic going through the process and translates certain URL, cookie, header, and body information into detailed "security activity" (e.g., user identity, actions, device details, geo-location).

Time to map is important—if mapping takes too much time, it can cause a delay in the official rollout of the application or a compromise in the enterprise's security posture. Neither option is optimal, as one is a hinderance to business and the other raises the risk of a security breach. Forcepoint CASB maps for cloud applications across any activity, providing the foundation for granular control and protection.

100%

of customers have at least one critical Tier II-III XaaS or custom application in their top 10 assets

Figure 2.
Forcepoint Cloud Applications Mapping Time



Forcepoint CASB also offers the quickest support for any public or custom cloud application, allowing customers to secure bespoke cloud applications, modules, and activities in a matter of days. In fact, for more than 80% of applications, Forcepoint's mapping time is less than five days (see Figure 2). Other CASB solutions can take several weeks or months to complete, and only map a small set of activities.

For more information about Forcepoint CASB, please visit our website. To understand what our CASB solution can do for your enterprise get a demo.

forcepoint.com/contact