

Meet the Symantec DLP

and Norton Cloud Services teams!

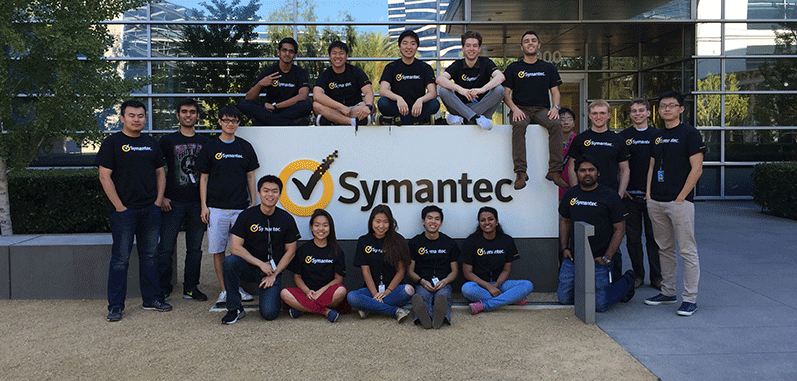
What do we do?

The Norton Cloud Services team builds high-scale, high-performance web services that support the Norton products, including our flagship **Norton Security**.

Our services field over one billion requests daily, from over 100 million endpoints worldwide!

The Cambridge Information Protection team builds cloud services for multiple products in the Enterprise group at Symantec, selling to the largest companies in the world. We have written cloud-integrations for the industry-leading Data Loss Prevention product, services for a rising Encryption product, and a new responsive portal for Symantec’s VIP product, which provides multifactor authentication.

The Intern Program at Symantec



Our intern program is incredibly successful and vibrant. Many of us are familiar with success stories including VPs, Senior VPs and even one of our Group Presidents who began their professional lives as Symantec interns; so it's a great starting point for your career!

We seek to build lasting professional relationships with promising young engineers.

 Our Cloud Services

Here are some examples of the largest services we’ve built:

The **Norton Reputation Service** services about 15 billion events daily. When your Norton Security product encounters a file that it is unfamiliar with, it may make a request for more information from NRS, providing info such as file name, hash, download URL, size, signer, etc. NRS will then respond with advice on how to handle the file (for example, the file can be trusted because it is signed by a reputable vendor, or is prevalent on machines that rarely experience infections).

If you are a Norton user, you may have seen **Norton Secure Login** as our single-sign-on portal for many Norton services, similar to Login with Facebook or Google; but NSL does much more: it is a full-fledged Identity Provider. A user with a Norton Secure Login may provide additional Identity Proofing information to prove they are who they say they are (for example, by answering financial history questions that can be verified with one of our partners, like ID Analytics); which proofing then allows the user to access more sensitive web-based services, such as collecting one's Veteran's Affairs benefits (which is possible today using NSL); or hopefully one day file one's taxes, or vote online.

The **Norton Datastore** APIs synchronizes policy data between user’s devices; and the **Norton Event Store** manages date and time based logs for search and reporting.

An example of a product leveraging these APIs is our parental control offering, Norton Family. A Norton Family user can update their family "rules" (usage curfew, website categorizations, social network settings, etc.), which Norton Datastore synchronizes between the family's devices. The Norton Family agent on those devices applies and enforces the policy; and reports usage data up to the Event Store, which is used to produce usage reports that parents can view on the Norton Family web portal.

The **Data Loss Prevention** integrationservices provide a way for internal and external clients to determine if a file is sensitive or not. We leverage several technologies and methodologies to perform a verdict on a file, whether it is forms recognition, file fingerprinting, or vector-support machine learning. By scanning potentially sensitive files we can detect data breaches and provide controls and remediation so that companies can be more confident and productive when sharing files. Our services scan tens of millions of files each day.

I hope this gives you a good idea of who we are and what we do.

And we hope you are interested in joining our team or learning more about us!