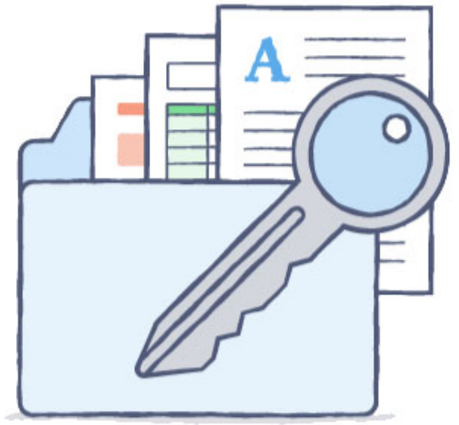
Dropbox security: 2014 in review

An update on our work to keep your stuff safe

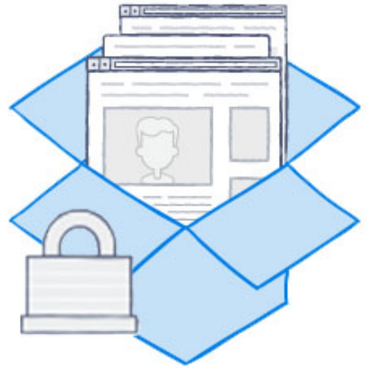
Here at Dropbox, keeping your information safe is a top priority. In addition to the work we do behind the scenes to make that happen, we believe it's important to be open about that work. So as we come to the close of 2014, we wanted to highlight some significant updates we made in the security realm this year.



At a high level, we focus on protecting users and customers from evolving security threats, while providing effective tools to help manage their most important information. Our teams do this by: 1) enhancing our security techniques, 2) joining industry efforts to strengthen online security across the board, and 3) building product controls. Here's a little bit more detail about our work this year in each of those areas.

Improving SSL for dropbox.com

SSL refers to the way we encrypt—or encode—the information you send to Dropbox. It keeps people from snooping on your stuff, regardless of what device you're using to access your files or if you're on public WiFi.



We've always had your back by encrypting your file data in transit between you and us, and while at rest on our servers. But this year, a number of high-profile SSL bugs that affected the entire tech industry were disclosed, showing that we always need to be on our toes no matter what code we rely on. In addition to patching our services in response to these bugs, we changed the SSL settings on www.dropbox.com and disabled the vulnerable SSLv3 protocol. As a result, we are now one of the very few major sites to get an A+ rating from SSL Labs.

To tighten controls over SSL connections, we've integrated with Chrome and Firefox to enable certificate pinning on www.dropbox.com. This means we've worked with the Chrome and Firefox teams to preload our certificate so that these browsers will only connect to www.dropbox.com after verifying that it's really Dropbox you are connecting to and no one is snooping on your connection.

So that you're able to verify you're really connecting to Dropbox on your end, we changed the certificate we serve on www.dropbox.com to an Extended Validation Certificate, so you'll have a visual cue. When you visit https://www.dropbox.com now, you'll see a green bar saying "Dropbox, Inc" instead of just a simple lock icon. It's a visible signal that you can count on to make sure you're not tricked into logging on to a spoofed site.

Protecting users against password attacks

Password attacks often happen when people use stolen usernames and passwords from compromised sites and try to use them to log in to other services. These attackers are only getting more sophisticated—many of them use automated botnets of more than 100,000 machines or IP addresses to cycle through username/password combinations in attempts to hijack accounts. They're able to get these lists because many people reuse the same passwords across multiple sites, or simply because the passwords are too easy to guess.

Like many large Internet services, Dropbox is a regular target for these types of attacks, so we're constantly working to strengthen our defenses. Fortunately, our team has been able to block 99% of attempted password attacks automatically. We've built systems to automatically detect patterns that look like suspicious activity, like when we see an exceptionally high number of attempted logins from a single computer or a certain set of IP addresses. In the vast majority of cases, we identify and block the attack before attackers can access any information stored in the account. We've also worked throughout the year to keep our detection mechanisms ahead of the curve, so we can spot and then block new signals related to the latest tricks attackers try to use.

As always, we also highly recommend everyone take steps to improve their own safety on Dropbox and elsewhere online. The safest thing to do is to choose unique passwords for each service you use and guard them closely. If you've ever used the same password for more than one website, you should create new unique passwords for each of them. Tools like 1Password can help you manage strong passwords across multiple sites and help make your accounts safer.

Two-step verification will also add an extra layer of security to your account. Every time you sign in to Dropbox, you'll be required to enter the code sent to your phone or a one-time, time-limited code generated from a supported mobile app, like Google Authenticator. This is a highly effective way to protect your account from unauthorized access.

Getting involved in the security community

Many security challenges, like password attacks, aren't unique to Dropbox. That's why we've joined industry groups like Simply Secure and Hacker One, which focus on strengthening security online for everyone. Simply Secure, for example, aims to make it easier and simpler for people who don't have technical skills to stay safe online. One of the biggest barriers to adopting secure tools and practices, like two-step verification, is that they're too complicated or cumbersome to implement. We'll be working hard to lower that barrier.

We also encourage the broader security community to report security vulnerabilities to us with a responsible disclosure policy and our public bounty program. No company's code is perfect, and it's always far better for engineers to learn of and patch a security vulnerability before attackers are able to exploit it. That's why many top tech companies—including Google, Facebook, and Twitter—have similar programs, allowing them to work with skilled hackers to help find and disclose vulnerabilities in exchange for public credit and/or monetary rewards.

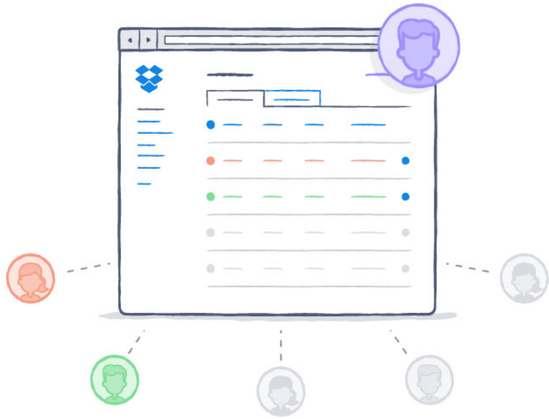
In January 2015, we'll be starting a partnership with Hacker One, a platform that allows us to engage with the extended hacker community in finding and bashing security bugs before they're exploited. We'll be able to leverage others' expertise and fix potential problems with our product well before they affect our users, making our product safer and better.

We're also champions of the National Cyber Security Alliance, members of the Cloud Security Alliance, and regularly speak at different security conferences around the world.

Providing more controls for IT administrators

Dropbox for Business customers often have unique internal standards and workflows, and need specific features to help Dropbox integrate well with both. In response, we launched view-only permissions for shared folders, passwords for shared links, and expirations for shared links. We also built in the ability for admins to specify the default settings for shared links (which individuals can change if needed), so company information is protected in a flexible way. Admins can also remove individual shared links created by team members, to give them further control over how company information is shared. And with new unified sharing settings, shared folder owners can ensure that any links created to folder content follow the same permission settings as the folder.

For businesses that want additional features, we recently launched the Dropbox for Business API to give developers access to the team-level functionality of Dropbox for Business. This way, admins can have additional visibility and control features through our growing network of apps. Specifically, enterprises can integrate enable eDiscovery and legal hold, security information and event management (SIEM) and analytics, data loss prevention (DLP), digital rights management (DRM), identity management and single sign-on (SSO), data migration and on-premises backup, and custom workflows enhanced by Dropbox.



Complying with standards and regulations

Finally, we were excited to announce that we added ISO 27001 Certification, a new SOC 1 report, and updated SOC 2 and 3 reports to our growing list of compliance milestones. These ongoing audits affirm that we've built a systematic approach and effective controls to maintain the security, confidentiality, integrity, and availability of your data.

Looking ahead

The safety and reliability of your information is the foundation of our business. We value the confidence you've put in us and take the responsibility of protecting your information very seriously. It's always at the top of our minds and we'll keep working hard to stay on top of our game, so stay tuned for more on this front in 2015!