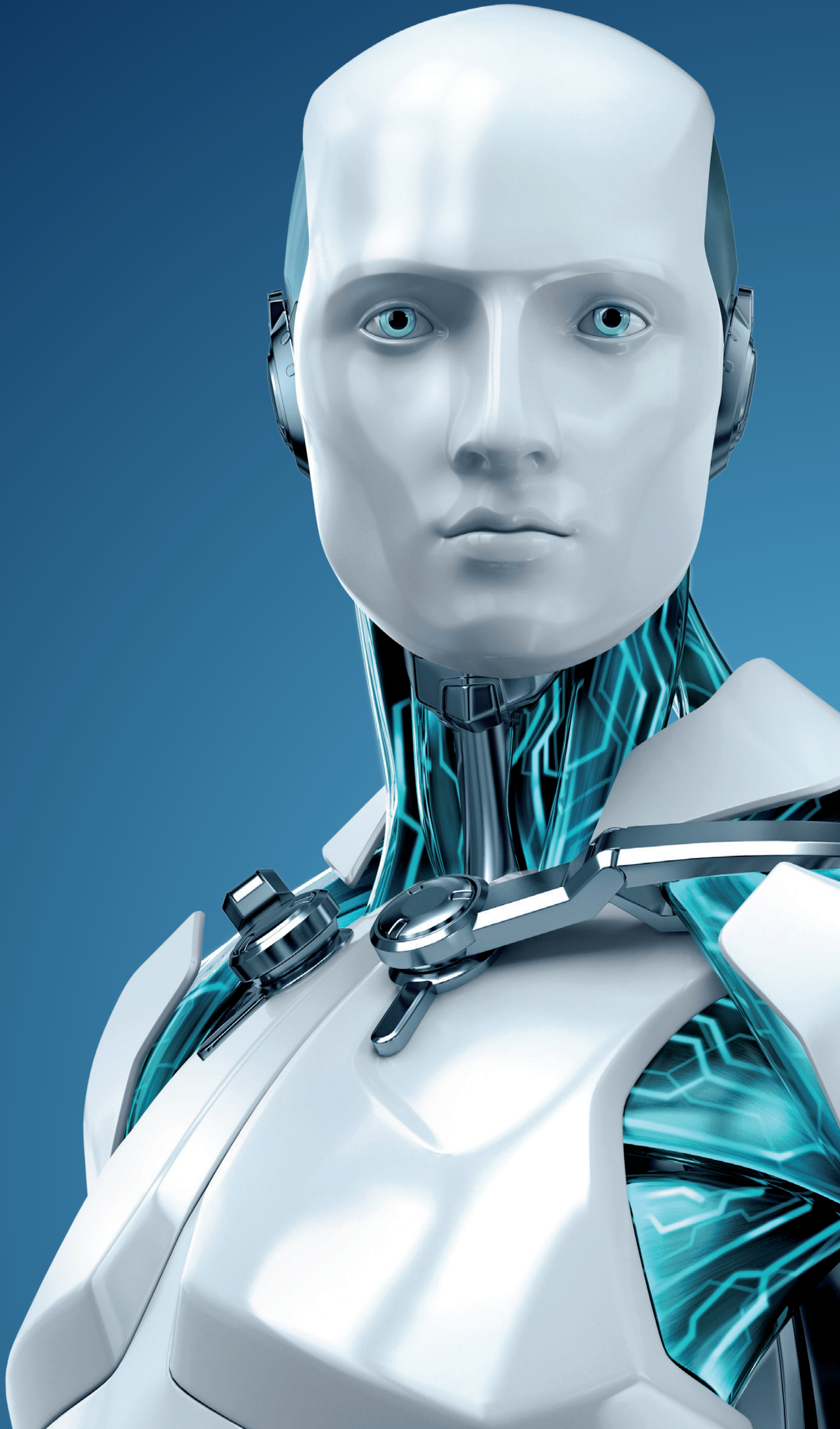
TECH BRIEF

Three keys to secure collaboration



ENJOY SAFER TECHNOLOGY™

THREE KEYS TO SECURE COLLABORATION

Anywhere, anytime collaboration is one of the greatest advantages of technology. Whether you enable shared access within local offices or between remote offices, by mobile workers or with business partners, the ability to share business knowledge and act on it decisively is a significant business edge.

Collaboration through access to shared repositories and the use of Big Data tools unlocks new insights that can lead to greater innovation and performance. The more users are able to contribute, the greater the potential value you can uncover and create.

The rewards are great – if you can foster collaboration by authorized users while locking out unauthorized access to your valuable data. Here are three practices that can minimize the risk.

1. Deploy defense in depth

The more users inside and outside of your company who have access to your information assets, the more important it is to apply a defense-in-depth strategy to protect them. Security at the server ensures that no file or object coming in or out of your central repository is tainted with malware. But equally important is protecting the systems that access that information against compromise, by deploying antimalware on desktops, laptops and other mobile devices as well.

2. Consider two-factor authentication

Giving external partners or vendors access to your data opens the door to ways of applying that data that you can't duplicate in-house. But it has pitfalls in that you don't know how secure those systems are. Employing password protection alone can provide an opening to unauthorized entry if the passwords are compromised, guessed or stolen. Using a two-factor authentication system provides an extra layer of protection. In addition to passwords, partners need a second "factor" – a device that generates a one-time passcode. Two-factor systems that use a smartphone app to generate the passcode leverage hardware that many individuals already carry. With these systems, your company avoids investing in and distributing special-purpose devices.

3. Encrypt when necessary – or when prudent

Sensitive data can always benefit from encryption. If you're dealing with personal information that is encrypted, some regulations, such as HIPAA, can give you safe harbor from customer-notification requirements and penalties in the event of a data breach. But despite the value that this protection provides, all too often, convenient access trumps security because traditional encryption solutions are complex to manage. A solution that allows you to share encryption keys with project groups, remote teams and partners through a Web-based management console makes the extra security of encryption practical for collaborative teams.

ESET's layered security approach for collaboration includes ESET Secure Authentication, DESlock+ Encryption, ESET Endpoint Security and ESET Security for Microsoft SharePoint Server. You can collaborate with confidence, sharing information inside and outside of your organization without being overly burdened by security processes and procedures. Instead, you and your partners can focus on unlocking the value that collaborative solutions can deliver.