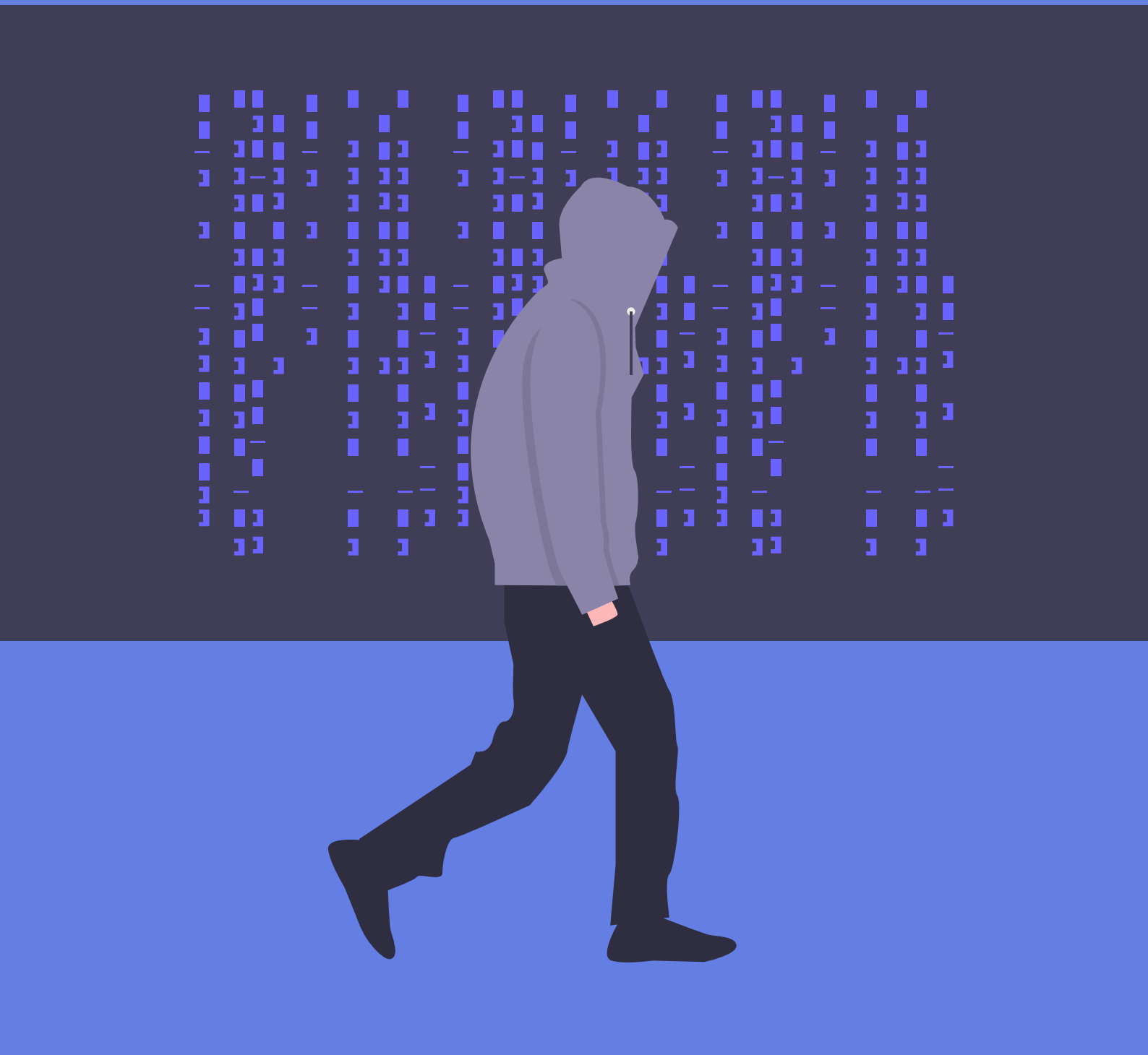
The ProtonMail Guide to IT Security

for Small Businesses

Adopt top IT security solutions for small businessess



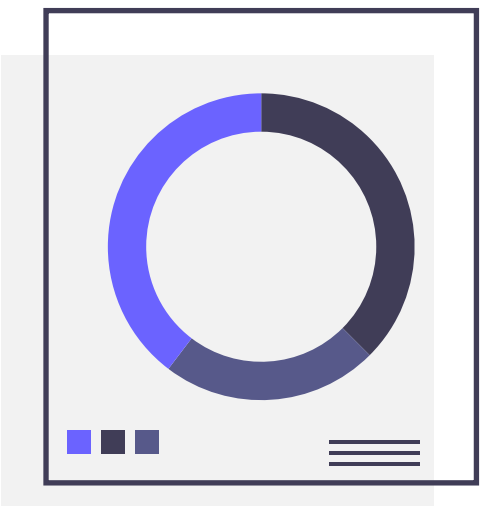
Adopt top IT security solutions for small businesses

READ THIS CHAPTER to see all the different apps, programs, and services that offer your company increased IT security and data protection. This list includes both free and paid services for

- Communications
- Storage
- Productivity
- Security
- Advanced network security

We made this the last chapter of our ebook because IT security is primarily about creating a culture of IT security awareness. Merely switching to encrypted services will not solve all of your IT security issues. The previous four chapters that describe how to implement IT security best practices form the foundation of a sound IT security policy. However, the following encrypted services will reduce your company's exposure, and, when paired with a security-conscious workforce, can go a long way to preventing a data breach or hack.

Note that while some of these tools will be good solutions for companies of any size, others will work best for smaller businesses that have not created their own internal network. We describe some tools that larger companies can use to secure their network (See Chapter 3), but other tools will require expert help to implement correctly.



Communication

Email provider

Most small businesses rely on emails to handle both their internal and external communications. Email security best practices are essential to keeping your business's data safe, but some email providers can offer your company more security than others.

ProtonMail

ProtonMail offers its users automatic end-to-end encryption. Your emails are encrypted before they leave your device so that only you and your intended recipient can access them. You can even secure your messages to non-ProtonMail users by sending password-protected emails.

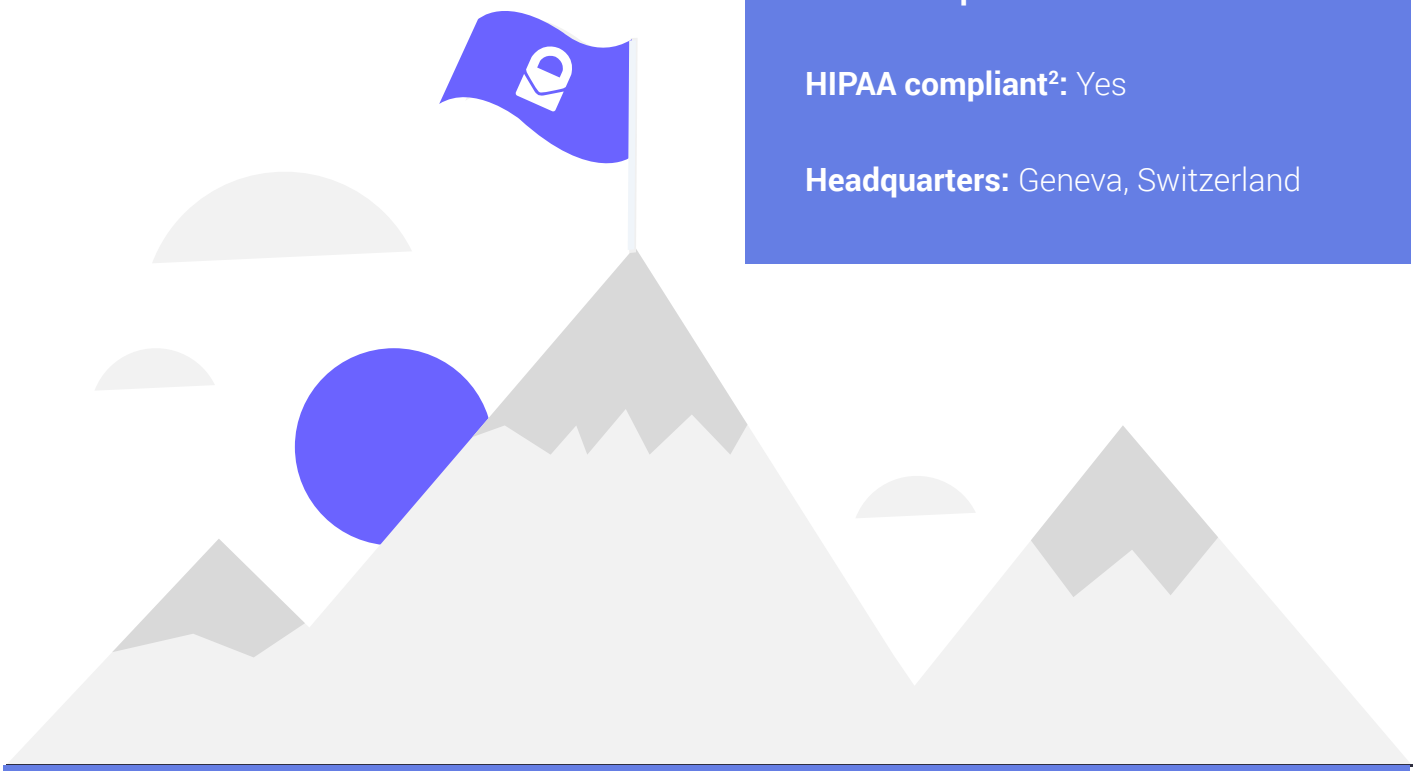
Platforms:
Android, iOS, and web app. Also has Bridge integration with Microsoft Outlook, Mozilla Thunderbird, and Apple Mail

Price: Has a free option. Premium plans begin at $5 per user per month.

GDPR compliant[1]: Yes

HIPAA compliant[2]: Yes

Headquarters: Geneva, Switzerland



1 This signifies that this tool adheres to the technical safeguards defined in the GDPR guidelines, which means that it can contribute to an organization complying with GDPR. It does not mean that just by using this tool your organization will be GDPR compliant.

2 This signifies that this tool adheres to the technical safeguards defined in the HIPAA guidelines, which means that it can contribute to an organization complying with HIPAA. It does not mean that just by using this tool your organization will be HIPAA compliant.

Team collaboration

Many businesses have employees and contractors working remotely. This can make coordinating a challenge unless you use a team collaboration app. Given the amount of information that can be exchanged and stored on these platforms, using one that is encrypted is a necessity.

Wire

Wire is one of the only end-to-end encrypted services that allows for group calls, which makes it more secure than Slack when trying to manage team communication. Wire has been independently audited and is entirely open source, giving you some assurance that Wire's code is doing exactly what they say it is.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at €6 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zug, Switzerland

Messaging

For companies that do not need all the functionality of a collaboration app but still want their communications to be secure, there are end-to-end encrypted messaging apps.

Signal

Signal is widely considered to be the most secure encrypted messaging app. It supports texts, group texts, as well as voice and video calls. Conference calls between more than two people, however, are not possible.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

HIPAA compliant: Yes (with caveats)

Headquarters: Mountain View, California, USA

Threema

Threema, unlike Signal, does not require a phone number to create an account, which means Threema is as close as you can get to truly anonymous messaging. The company headquarters is in Switzerland, giving its service strong legal privacy protections.

Platforms: Android, iOS, Windows phone, and web app

Price: Starts at 1.40 CHF per device per month

GDPR compliant: Yes

HIPAA compliant: No

Headquarters: Zurich, Switzerland

Storage

Cloud storage

Cloud storage has redefined how offices can work. By storing files on the cloud, your business can maintain a backup of all critical documents in case of a catastrophic system failure as well as easily share documents and sync progress between different employees. Protecting these files and the data they contain should be one of your business's top priorities.

Tresorit

Tresorit is an end-to-end encrypted cloud storage service. It has optimized its service for businesses, allowing you to create different levels of access for various documents and to revoke users' and devices' access to files.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Starts at $25 for two users per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zurich, Switzerland

Sync

Sync is another end-to-end encrypted cloud storage service, similar to Tresorit. It gives businesses admin control, allowing supervisors to create different levels of access for different employees. Sync also allows you to preview your files before you open them.

Platforms: Android, iOS, macOS, and Windows

Price: Starts at $10 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Toronto, Canada

Boxcryptor

Boxcryptor is slightly different. It allows you to encrypt your documents before you save them on a separate cloud service, like DropBox or Google Drive. Your team can still easily collaborate and share files over the cloud, but now your documents are secure.

Platforms:
Android, iOS, Linux, macOS, Windows, and a Chrome web browser add-on

Price: Starts at $600 for five users per year. (There is also an individual Business plan that is $96 per user per year, but it has less functionality.)

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Augsburg, Germany

Cryptomator

Cryptomator is the free, open source version of Boxcryptor. With Cryptomator, your employees can create a virtual hard drive that is connected to a folder (called a "vault") on their cloud storage service and protect it with a password. Any document they drag and drop into the virtual hard drive is automatically encrypted and backed up in the vault. There is also Cryptomator Server, for larger businesses

Platforms: Android, iOS, macOS, and Windows

Price: Free (There is a one-time fee of $9.49 to download the Android app and $9.99 to download the iOS app.)

GDPR compliant: Yes

HIPAA compliant: Yes

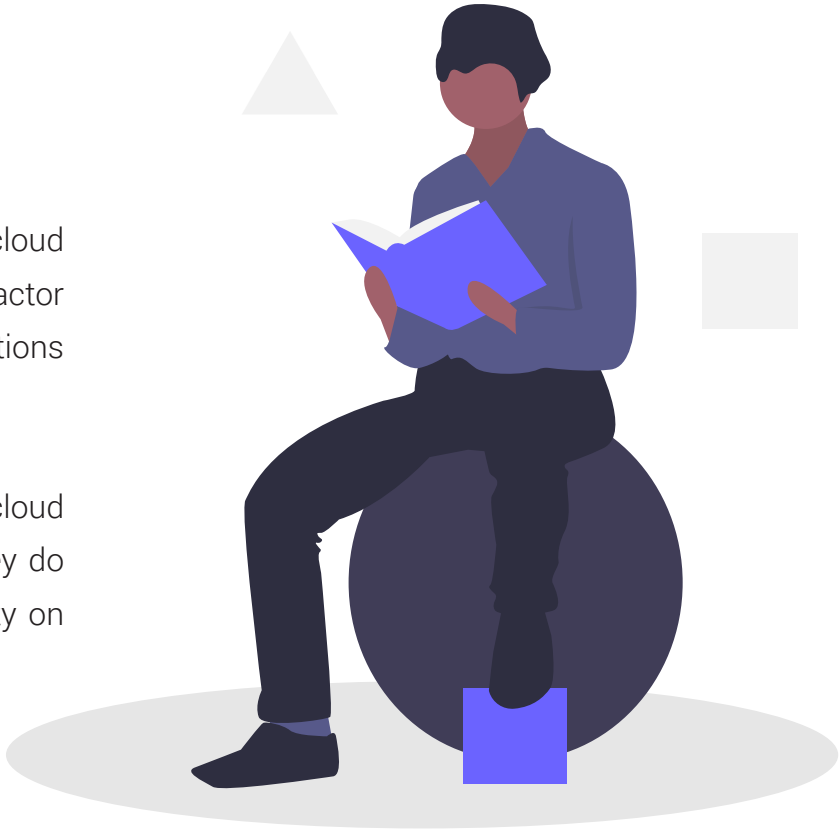
Headquarters: Sankt Augustin, Germany

looking to add encryption to the files on their company servers.

Other cloud services

pCloud is an end-to-end encrypted cloud service. It is GDPR compliant, allows two-factor authentication, and its business subscriptions start at $7.99 user/month/TB.

Spideroak is an end-to-end encrypted cloud storage service similar to Tresorit, but they do not offer two-factor authentication security on their accounts.



Productivity

3

Notepad

Also known as a "text editor," a notepad is a program that allows you to write and edit plain text. A notepad can be used to keep notes, write documents, and alter configuration files or programming language source code.

Standard Notes

Standard Notes is a simple, end-to-end encrypted note-taking app that can sync your notes across all your devices. Its clean interface and numerous extensions mean that you can use Standard Notes for everything from writing yourself reminders to coding.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Has a free option. Premium plans begin at $9.99 per user per month.

Headquarters: USA

Joplin

Joplin is another end-to-end encrypted note-taking app, but unlike Standard Notes, users must manually activate the end-to-end encryption feature. Joplin relies on external services, like NextCloud or Dropbox to synchronize across devices.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

Headquarters: N/A

Security

VPN

A virtual private network is an effective way to add a layer of encryption to your online activity. It also allows your employees to safely work on public WiFi while they are on the road.

ProtonVPN

ProtonVPN secures your Internet connection with AES 256-bit encryption, the industry gold standard, and its use of Perfect Forward Secrecy means that even if your traffic is intercepted and saved, it can never be decrypted at a later date.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Has a free option. Premium plans begin at $5 per user per month.

Headquarters: Geneva, Switzerland

Password manager

Creating strong, unique passwords or passphrases for your accounts is one of the basics of IT security, but no employee can remember all the passwords necessary to log in to all the platforms they need to use for work. (Look how long this list is already!) A password manager changes all that. By safely encrypting all your passwords, a password manager allows you to create passwords that are impossible to crack, without having to remember them all. Using a trustworthy password manager to secure your passwords is one of the easiest ways to improve your company's security.

Bitwarden

Bitwarden is an open source, end-to-end encrypted password manager. It helps your employees create randomly generated passwords for all of their accounts, and then syncs those passwords across all their devices.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at $5 for five users per month

Headquarters: Florida, USA

1Password

1Password is another end-to-end encrypted password manager, but it has a few more bells and whistles. While it is only a paid service, it is considered to be one of the most secure password managers. Its Watchtower feature will alert you if any of your passwords have been exposed in recent data breaches.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at $3.99 per user per month

Headquarters: Toronto, Canada

Dashlane

Dashlane is also a premium end-to-end encrypted password manager. It will scan known security breaches and will send you an alert if it finds any of your passwords among those exposed. Its business plan also comes with an admin console that allows you to set permission levels for all your employees.

Platforms: Android, iOS, macOS, Windows, and web browser add-ons

Price: Starts at $4 per user per month

Headquarters: New York City, USA

Other password managers

LastPass: A premium password manager, but it does not alert its users if their password is exposed in a data breach.

KeePass / KeePassXC: These are both free, open source password managers, but neither of them offers official mobile apps.

Two-factor authentication

To ensure your critical accounts are secure, you should enable two-factor authentification (2FA) in addition to using a strong, unique password. The site Two Factor Auth will help you identify which services you can use 2FA on. By using 2FA on your accounts, you can prevent intruders from accessing your accounts even if they get a hold of your passwords.

YubiKey

The YubiKey is a hardware token (a specialized USB stick) that you can plug into your device to confirm your identity. While it is thought to be the most secure form of 2FA, relatively few services support hardware token 2FA.

Platforms: YubiKey 5 NFC works with macOS, Windows, and NFC-equipped Android and iOS devices

Price: A YubiKey 5 NFC costs $45.

Headquarters: Palo Alto, USA

Duo

Duo offers several 2FA solutions, including ones that incorporate Yubikey hardware tokens, confirmation requests delivered to the Duo app that foil man-in-the-middle attacks, and time-based one-time passcodes.

Platforms: Duo app is available on Android and iOS

Price: Has a free option. Premium plans begin at $3 per user per month.

Headquarters: Austin, USA

Other two-factor authentication services

Google Authenticator app: Google offers a free authenticator app that creates time-based one-time passcodes for 2FA purposes. It does not have the same functionality as Duo or a YubiKey. of them offers official mobile apps.

Disk encryption

All your devices should use some form of disk encryption to prevent unauthorized access to your devices' data storage in the event they are stolen or lost. By encrypting your smartphone or computer's hard drive, you turn your sensitive data into illegible code that can only be decrypted by your password. All the options discussed below are examples of disk encryption software.

VeraCrypt

VeraCrypt is an open source disk encryption service. Using VeraCrypt, your employees can encrypt the hard drive on their device, encrypt their USB flash drive, or even hide how much volume they have on their hard drive.

Platforms: Linux, macOS, Windows

Price: Free

Headquarters: N/A

Other disk encryption services

FileVault: FileVault is available on macOS X Lion and later. You can use it to fully encrypt your startup disk.

BitLocker: BitLocker is available on most Windows 7 and Windows 10 devices. It is a strong, full disk encryption service.

LUKS: LUKS is a free, open source hard disk encryption service for Linux.

Native encryption for Android and iOS: Any 3G iOS device or later and any Lollipop (5.x) Android devices or later are equipped with their own native disk encryption services. To learn how to encrypt your Android device, click here. To encrypt your iOS device, click here.

Personal antivirus software

Antivirus software (AVS) is a preventative measure meant to keep your devices clean. AVS scans your device for any malware, from ransomware to rootkits. If it detects any, it will attempt to remove them. More modern AVS also provides malware prevention measures.

Bitdefender

Bitdefender has strong antivirus protection, but it is light enough that it won't slow your device down. The AVS receives daily updates so that no malware can take it by surprise. They also have a more advanced option for larger offices. It will protect your servers and all your endpoint workstations without bogging down your network.

Platforms: Android, macOS, Windows are available free. iOS is available with a paid plan.

Price: Has a free option. Small office security starts at $99 for one year for five devices.

Headquarters: Romania

Advanced network security

5

This is just an introduction to some of the advanced tools for businesses that have their own internal network. These tools will help you secure your network, prevent vulnerabilities from arising, and help you deal with any threats or malware that make it past your defenses. Most, if not all, of these tools will require an IT expert to properly install and configure. If your company does not have its own internal network, these tools are not necessary.

Intrusion detection/intrusion prevention system

An intrusion detection/prevention system (IDS / IPS) monitors your network for malicious activity, policy violations, or malware. If it detects any of these, it will notify your IT admin or send a report to your security information and event management (SIEM) system (more on that down below). Depending on the threat it finds, your IDS / IPS could also attempt to stop the malicious activity.

Snort

Snort is an open source IDS/IPS that can perform real-time traffic analysis and packet logging on Internet protocol networks. It can also detect a number of probes and attacks and take action to stop them.

Platforms: Fedora, Centos, FreeBSD, Windows

Price: Free

Headquarters: N/A

Suricata

Suricata is also an open source IDS/IPS that can perform real-time traffic analysis. By using the extensive rules it has built-in, Suricata can scan for complex threats.

Platforms: FreeBSD, Linux, macOS, Ubuntu, UNIX, Windows

Price: Free

Headquarters: N/A

Network scanner

A network scanner searches your system for vulnerabilities in your security. If it detects a weakness in your network, it will send a report back to your IT admin. They will then use this report to address the found vulnerabilities and make the network more resilient.

Nmap

Nmap is an open source network scanner. In addition to finding network vulnerabilities, you can use Nmap to identify open ports to prepare for a network audit or to generate traffic to hosts on a network and measure their response time.

Platforms: FreeBSD, Linux (all distributions), macOS, Windows

Price: Free

Headquarters: N/A

Security Content Automation Protocol

SCAP is an automated system that will scan your system, searching for vulnerable versions of software. SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive patch scanning tool.

OpenSCAP

OpenSCAP is an open source SCAP system that will make sure your system is conforming to the policies and rules the SCAP community creates. With dozens of different policies, you can find the one that is right for your organization.

Platforms: CentOS, Debian, Fedora, Scientific Linux, Red Hat Enterprise Linux, Ubuntu

Price: Free

Headquarters: N/A

Security information and event management

A SIEM system aggregates all data from your network and then uses rules-based or statistical correlation engines to identify a baseline for what qualifies as normal activity on your network. It then searches for any deviations from this baseline. If it finds something it thinks is not normal, it will take action to stop it. It is also a repository for your IT admin to monitor and search your network records.

Prelude

There are two Prelude products: Prelude OSS and Prelude SIEM. Prelude OSS is a universal, free, open source SIEM system, but it is meant for smaller networks or for research. The more powerful Prelude SIEM is available for businesses and to secure larger and more complex networks. Both systems aggregate data from all your IT security tools, regardless of their brand or mark. They will work with either of the two IDS/IPSs on this list.

Platforms: Arch Linux, CentOS, Debian, Fedora, Gentoo, Mageia, Red Hat Enterprise Linux, Ubuntu

Price: The cost of a license for Prelude SIEM depends primarily on the number of devices that send their data to the system, whatever the volume.

Headquarters : N/A

OSSIM AlienVault

AlienVault is now part of AT&T Cybersecurity, but their open source SIEM system, OSSIM, is still available for free. In addition to letting its users collect and correlate event logs, OSSIM is connected to AlienVault's Open Threat Exchange, which allows users to report and receive updates about the latest malicious hosts. It also works with Snort and Suricata. Be careful because OSSIM is not a log management solution. If that is what you want, you would need to use either USM (paid version of OSSIM) or another log management system such as Elastic Stack.

Platforms: Must be installed on a virtual machine

Price: Free

Headquarters: San Mateo, USA

Elastic Stack

Elastic Stack, or its previous iteration, ELK (which stands for Elastisearch, Logstash, and Kibana, the three primary projects), is more of a data visualization system than specifically a SIEM, but it can be used as one. All the products in the stack are open source, and together they let you have a complete picture of your system and your employees' activity.

Platforms: Docker, Linux, macOS, Windows

Price: Free

Headquarters: Mountain View, USA

Network firewall

A network firewall is a network security system that monitors and controls incoming and outgoing network traffic between two or more networks based on a series of predetermined security rules. A firewall typically establishes a barrier between your internal network and other external networks, such as the Internet. A network firewall runs on your network's hardware.

OPNSense

OPNsense is the open source fork of the pfSense firewall software distribution. It can be installed on a computer or virtual machine to create a network firewall.

Platforms: HardenedBSD

Price: Free

Headquarters: Middelharnis, The Netherlands

iptables

iptables allows system administrators to configure tables, chains, and rules in the Linux kernel firewall. This gives the admin control over how data packets enter and travel around the system.

Platforms: Linux

Price: Free

Headquarters: N/A

firewalld

Platforms: Linux

Price: Free

Headquarters: N/A

firewalld is an open source, dynamically managed firewall that allows you to establish different levels of trust around your network. It also works using the Linux system's iptables to filter data packets.

ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click here.