



GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Maria, Gitanjali

“Small Business Technology Insight: Cybersecurity”

Getapp.com

10 October 2018

URL: <https://lab.getapp.com/small-business-cybersecurity-guide/>

Accessed: 12 July 2019

Synopsis: Security concerns rank No. 2 among the challenges faced by small and midsize businesses, according to our survey.

To safeguard your business from hackers and harmful bots, you must have multiple defense mechanisms to ward off attackers from different fronts.

The key challenge for small business owners is tackling cybersecurity with limited budgets and IT expertise, while juggling other pressing business and customer issues that take up the bulk of their time and resources.

Small businesses' cybersecurity strategies must include investment in a combination of antivirus, firewall, spam filter, data encryption, data backup, and password management applications, or else they will leave components of their IT infrastructure exposed, inviting attacks that will result in heavy recovery and opportunity costs.

This article will discuss these cybersecurity applications, their features, and other technical considerations that you must keep in mind when choosing and implementing security solutions.



Small Business Technology Insight: Cybersecurity

by Gitanjali Maria | Oct 10, 2018 | Insights, Security



Facebook



Twitter



LinkedIn

Security concerns rank No. 2 among the challenges faced by small and midsize businesses, according to our [survey](#).¹

[Seventy percent](#) of cyberattacks target small businesses, which, on an average, lose around [\\$80,000](#) per attack, not to mention the lost business opportunities and damaged reputation.

To safeguard your business from hackers and harmful bots, you must have multiple defense mechanisms to ward off attackers from different fronts.

The key challenge for small business owners is tackling cybersecurity with limited budgets and IT expertise, while juggling other pressing business and customer issues that take up the bulk of

their time and resources.

A cybersecurity solution can help your business meet its preliminary security needs.

Cybersecurity software detects and blocks malicious applications; these solutions comprise different types of security applications such as antivirus, firewalls, anti-spam, and data loss prevention.

Small businesses' cybersecurity strategies must include investment in a combination of antivirus, firewall, spam filter, data encryption, data backup, and password management applications, or else they will leave components of their IT infrastructure exposed, inviting attacks that will result in heavy recovery and opportunity costs.

This article will discuss these cybersecurity applications, their features, and other technical considerations that you must keep in mind when choosing and implementing security solutions.

- [What is cybersecurity? The definition and goals](#)
- [Cybersecurity applications essential for small businesses](#)
- [Cybersecurity software selection criteria: 4 key considerations](#)
 1. [Integrated security suite vs. individual applications](#)
 2. [Core cybersecurity software features you must look for](#)
 3. [Cybersecurity software and CPU usage](#)
 4. [Cybersecurity software and OS compatibility](#)
- [Cybersecurity software: Understand the benefits and risks](#)
- [Popular cybersecurity software products](#)
- [Building a small business cybersecurity strategy](#)

What is cybersecurity? The definition and goals

According to [Gartner](#), cybersecurity is the domain that safeguards and protects all cyber assets such as data, information, and software tools. It generally includes the protection of all internet-connected systems from cyberattacks.

Cybersecurity covers different aspects such as protecting your applications, networks, and information as well as other components, including data backups, disaster recovery, and business continuity.

Cybersecurity goals and objectives

Here are some of the primary objectives and goals that cybersecurity software helps you achieve:



Detect and prevent cyberattacks before they happen:

Most often, businesses realize they have been attacked only when they are unable to open certain files, when their website crashes, or when their systems fail and won't reboot.

Cybersecurity software helps you detect signs of malicious activity before they cause major harm. It alerts you about malicious files and other malware. Cybersecurity solutions also help clean up your systems and remove the harmful elements before they knock you down.



Make online browsing safe:

Unsafe browsing and download practices can lead to viruses, Trojans, worms, ransomware, spyware, or keyloggers getting installed on your systems. This can lead to identity theft, stealing of passwords, and more. Cybersecurity software helps by flagging harmful websites and unsafe downloads.



Identify and plug vulnerabilities in the system:

Cybersecurity software helps detect weak points in your system such as unpatched software, legacy apps, phishing emails, etc. and allows you to autocorrect them. It also generates vulnerability reports.

Cybersecurity applications essential for small businesses

Cybersecurity involves fortifying your business against different threats emerging from multiple fronts such as internet usage, networks, emails, apps, and more.

There is no single cybersecurity solution that offers complete defense against all types of threats: **DDoS**, phishing, ransomware attacks, cryptojacking, etc. Instead, you must look at building an effective cybersecurity program by investing in multiple key security applications that offer specialized capabilities.

Some **common** cybersecurity applications that small businesses must have include:

Antivirus/Anti-malware: Antivirus is a type of software that scans your systems to detect and remove malicious files and applications. Most antivirus software today offers advanced capabilities and can also function as anti-malware, detecting and blocking different types of internet threats including ransomware, Trojans, and worms.

Firewalls: A firewall is a network protection tool that monitors and filters traffic to and from your network. It is capable of detecting malicious traffic and blocking it out based on set rules. Artificial intelligence-powered firewalls (i.e., next-gen firewalls) are capable of detecting and blocking malicious traffic based on context, in addition to the administrator-defined rules.

Spam filters: Spam filters are mechanisms of email protection that detect and remove unwanted emails from users' inboxes. Spam filters identify suspicious emails by identifying word patterns and context using a combination of techniques such as rule-based workflows, heuristic filters, and artificial intelligence.

Data encryption: Data encryption tools translate your data into a different form of code that only people with a decryption key can read. It is used to protect highly sensitive and confidential data, both while at rest and in transit.

Data backup: Data backup solutions are an essential component to ensure data protection, recovery, and [business continuity](#). Data backup applications store a copy of your data. They can either be on-premises or cloud-based. Small businesses such as yours that don't want to spend on data storage infrastructure and maintenance can opt for managed cloud-based data backup services.

Password manager: [Eighty-one percent](#) of hacking-related data breaches used weak and stolen passwords. [Fifty-nine percent](#) of small and midsize businesses have no visibility into employee password practices. Password manager tools help employees store and manage multiple passwords safely. Small businesses must implement strong password policies and must consider using password manager tools.

Cybersecurity software selection criteria: 4 key considerations

With so many cybersecurity applications on the market from over [1,300](#) software vendors, choosing the right one for your business can be difficult.

In the next few sections, we discuss in the detail some factors you must consider when purchasing cybersecurity software.

1. Integrated security suite vs. individual applications

Cybersecurity involves constantly protecting your business and its different IT systems—desktops, mobile devices, networks, browsers, software applications, and emails—from threats such as [DDoS attacks](#), ransomware, data hacking, etc.

This cannot be done with just one tool. As I discussed in the previous section, cybersecurity solutions are actually a combination or package of various applications such as anti-virus, firewalls, spam filters, and data loss prevention tools.

If you are worried that investing in multiple software applications is going to be too costly, there is an alternative: Many software vendors today provide integrated internet security packages that cover anti-virus, spam filters, anti-malware, privacy protection, and firewalls.

The advanced versions also offer ransomware protection, online data backup, and password managers. Security suite solutions remove the hassle of having to manage different security components, come cheaper, and serve all your basic needs.

Suite vs. stand-alone security solutions: Tips for choosing

Here are some tips to help you make the choice between integrated and stand-alone security solutions:

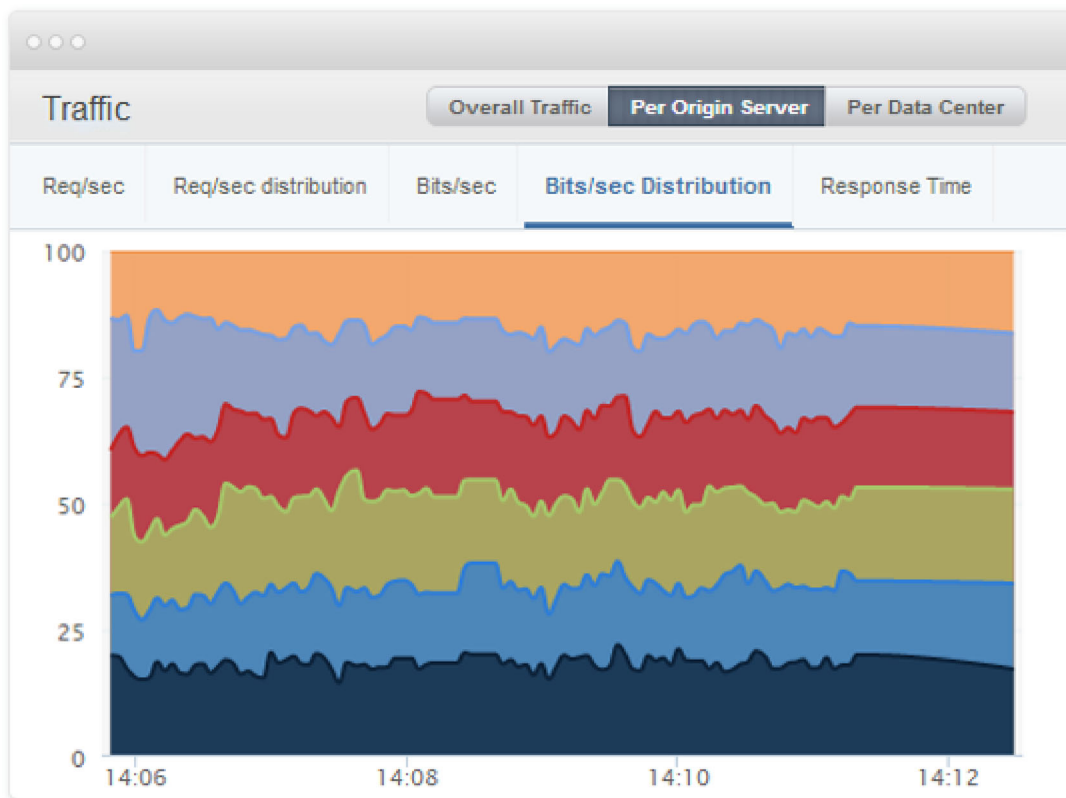
- If you require advanced protection in a specific area, such as networks, online browsing, data backups, or business continuity, opt for stand-alone solutions with specific capabilities that can integrate with one another.
- If you are a first-time buyer of security software or your requirement is only basic all-round protection, consider a security software suite.
- If you are buying or already have a suite solution and want additional capabilities, add relevant specialized security tools that can integrate with your current software.

2. Core cybersecurity software features you must look for

Some of the key features you must look out for while purchasing a cybersecurity suite solution or any of the individual cybersecurity products include:

- **Real-time monitoring**

Involves continuous monitoring of network traffic to and from your systems. It also checks your web applications' and other software's security posture at frequent intervals or on a continuous basis.

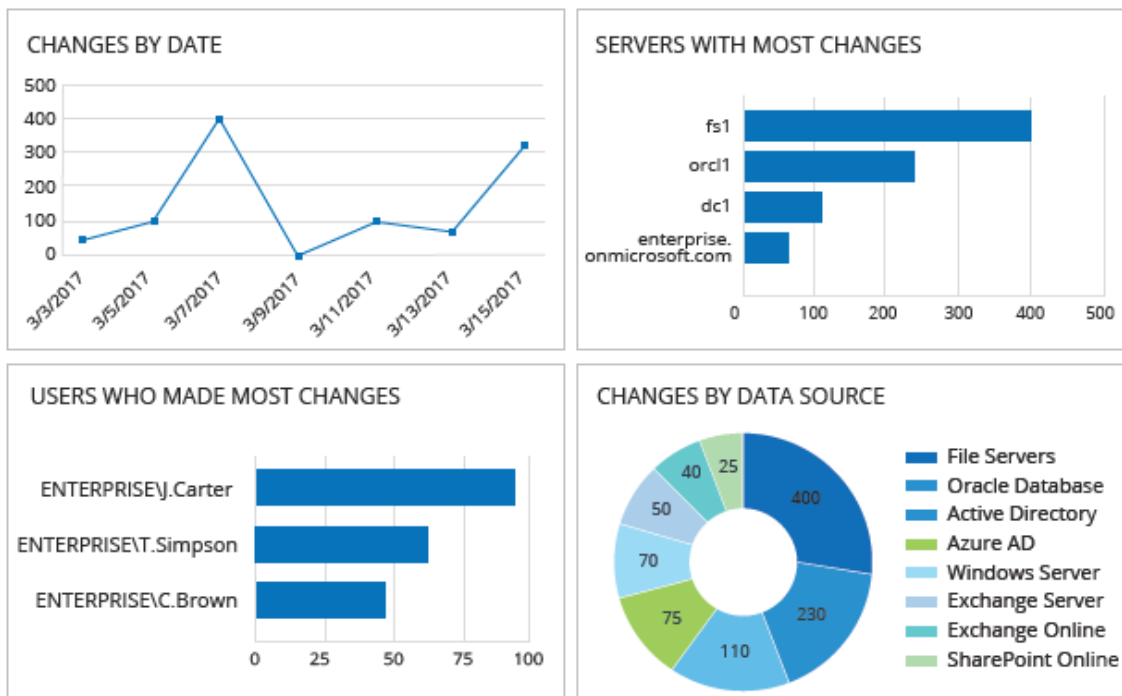


Real-time monitoring results of network traffic as shown in [Imperva Incapsula](#), a network monitoring and endpoint solution ([Source](#))

- **Dashboards**

Provides real-time visual data on the security performance of your systems. This capability helps administrators get a high-level picture of security performance, as well as enabling them to quickly identify anomalies in critical components.

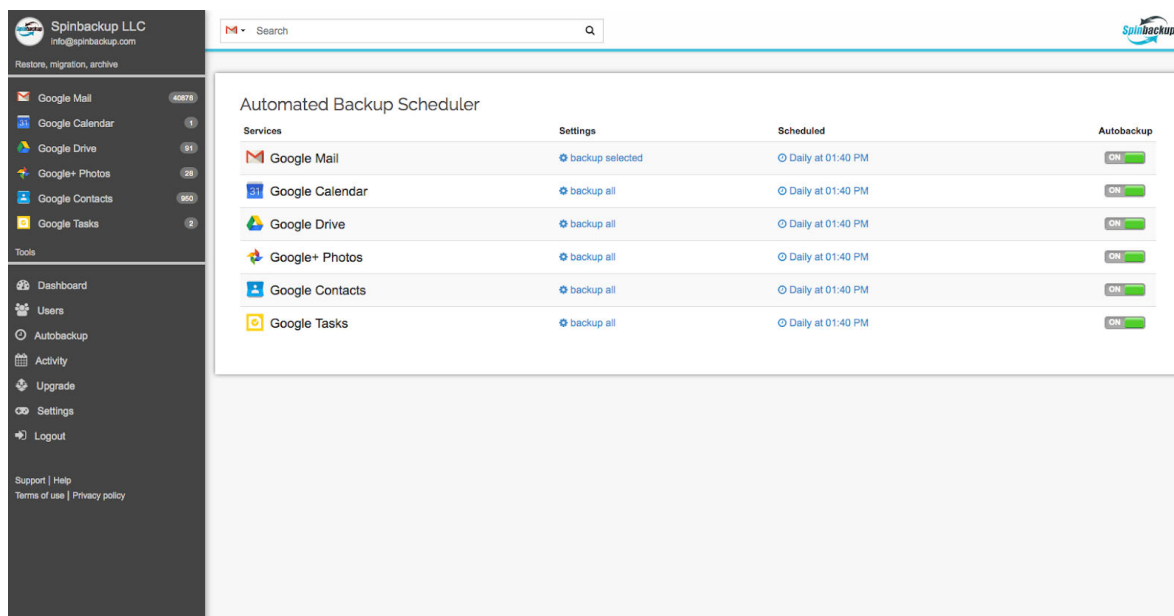
Enterprise Overview



Activity dashboard in [Netwrix Auditor](#), a cybersecurity software tool ([Source](#))

- **Automated actions**

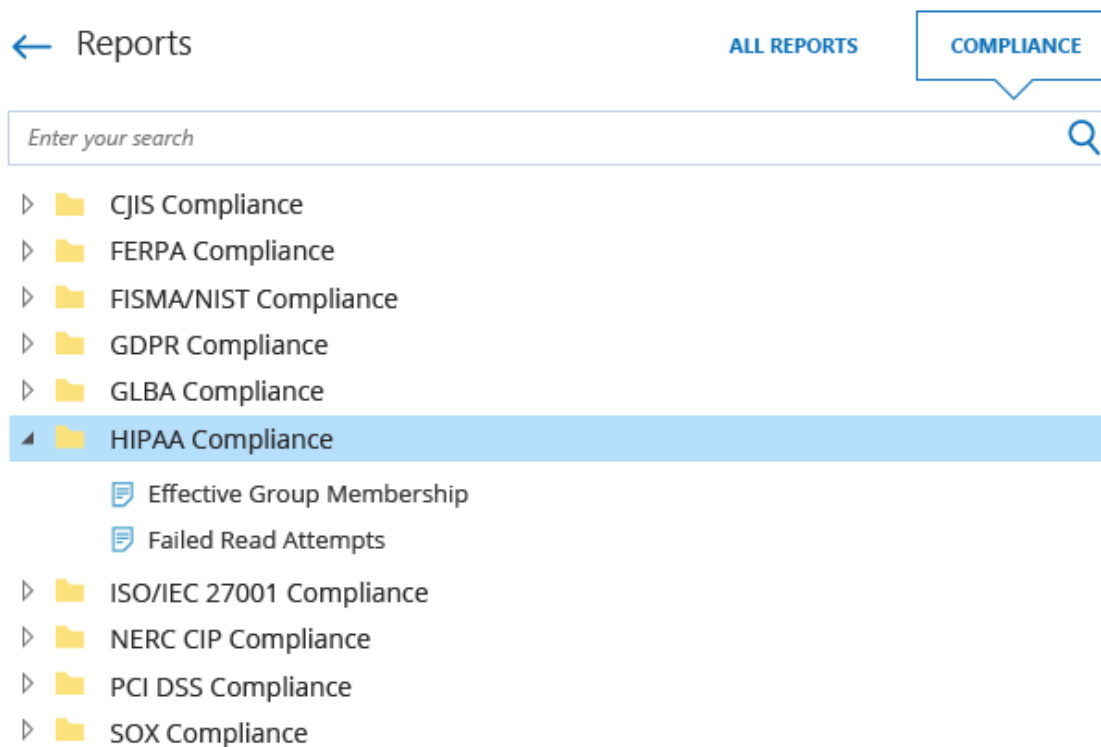
Your cybersecurity software must be able to complete certain critical actions such as installing updates, data backups, etc. with little human intervention. This helps to ensure that data is protected at all times, even if employees forget about security updates.



Automated backup scheduler in [Spinbackup](#), a cybersecurity and backup tool ([Source](#))

- **Reports**

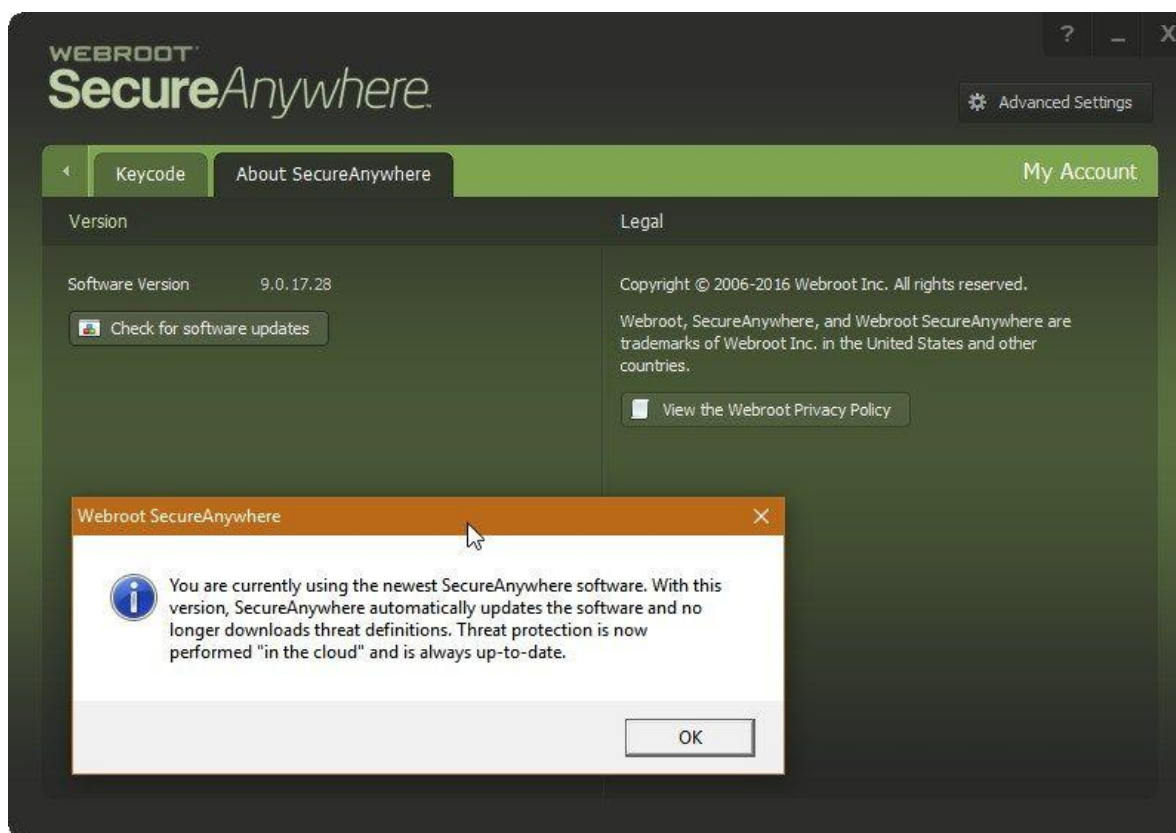
Custom reports and autogenerated reports help system administrators keep a record of different actions such as external logins, new devices connected to the network, bandwidth usage, etc. for the entire IT system. It also helps in using security analytics to identify weaknesses as well as for conducting incident investigations, post a breach or attack.



Reports generated in [Netwrix Auditor](#), a cybersecurity software solution ([Source](#))

- **Regular updates**

Regular security software updates from the security vendor is a most essential component of any security software. [Two hundred thousand](#) new malicious programs are created every day, and keeping your software updated to detect these strains of malware is very important. Ask your security vendor about its update/patch policy and frequency.



Automated updates as available in [Webroot](#), a cybersecurity software tool ([Source](#))

- **Alerts**

The software must alert and notify you about malicious files detected and the action—remove or quarantine—it plans to take. This helps you to be cognizant of the risks your system is facing.

Netwrix Auditor Alert

Possible ransomware activity

The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2017 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Details:	Size changed from "807936 bytes" to "831488 bytes"

This message was sent by Netwrix Auditor from `au-srv-fin.enterprise.com`.

Alerts on ransomware as shown in [Netwrix Auditor \(Source\)](#)

3. Cybersecurity software and CPU usage

While your security solution is a critical component of your IT infrastructure, it is an application that runs in the background. And ideally, it will function continuously.

So, you wouldn't want your other systems—CRM, HR, ERP or BI—affected by its running. It should have low CPU usage and must not slow down your system.

Though, with 4 GB internet connections and more RAM, as is the case with newer devices, CPU usage may not ultimately be an issue, it is still advisable to do free trials of cybersecurity software to see whether it impacts the performance of your systems under different load scenarios.

4. Cybersecurity and OS compatibility

It is difficult to manage and trace the multiple types of devices that connect to your network, especially with the implementation of policies such as BYOD (bring your own device) and employees connecting personal accessories—smartphones, smartwatches, cameras, etc. These devices could be working on different operating systems: Windows, Mac, Linux, Android, and more.

You must ensure that your security software is able to detect and run on all types of devices and operating systems. Double check with your vendor and read some real [user reviews](#) to ensure that the software works smoothly on all system types.

Cybersecurity software: Understand the benefits and risks

Implementing cybersecurity software helps business not only protect their IT systems but also improves productivity. Here are the main benefits and risks of cybersecurity software.

Benefits

Reduces downtime

Cybersecurity tools help reduce downtime of web applications and websites. By ensuring that malware does not crash your systems, cybersecurity allows you to continue working uninterrupted. It also ensures that malicious codes that slow down your system are removed, helping you improve your productivity.

Protects your information:

Cybersecurity solutions prevent malicious programs from corrupting your system and ensure that all your data and files are safe to use. It protects your financial details and customer details, as well as other business data. Some cybersecurity tools also offer encryption facilities to safeguard your data.

Protects your privacy:

Cybersecurity solutions offer anti-spyware, anti-adware, and privacy protection features that ensure that your data or identity is not stolen. It prevents keylogger software and other malware from getting downloaded or used on your systems.

Risks

Software is not foolproof:

Cybersecurity tools, though they protect your systems against many threats, cannot guarantee you that you'll be safe from all threats. Hackers are intuitive and try new ways to bypass security mechanisms.

"Most people assume that once security software is installed, they're protected. This isn't the case. It's critical that companies be proactive in thinking about security on a long-term basis."

 *Kevin Mitnick*

Tip: Ensuring safe internet usage policies can minimize exposure to cyber risks. Build awareness and train employees on good internet usage policies, how to identify phishing emails, password policies, and basic security practices for safe browsing (checking for “https:,” reading cookie usage terms and conditions, etc.).

Also, keep your cybersecurity solutions updated all the time and conduct regular [security assessments](#). This removes vulnerability exposure even for a short time.

 Integrations can be a challenge:

According to a study of businesses using security software, 67 percent indicated that installation was stalled because of too many point security solutions that worked separately and didn’t integrate.

Most security management software vendors operate in silos, increasing the complexity of integrations. If you must have multiple security applications from different vendors, integrating them to optimize security actions, share intelligence reports, and ensure coordinated action becomes difficult.

Tip: For small businesses, using an integrated security solution would be the best option to overcome integration hurdles. If you plan to use multiple security products from different vendors, ensure that APIs are offered for connecting with other apps.

Popular cybersecurity software products

Choosing the best cybersecurity solution can be a challenge, especially when there are many products on the market. Based on user reviews and rating score (see our [methodology](#) below), here are some of the most popular cybersecurity software products preferred by small businesses:

Cybersecurity solutions	Antivirus software	Anti-spam software
Okta	ActivTrak	SpamTitan

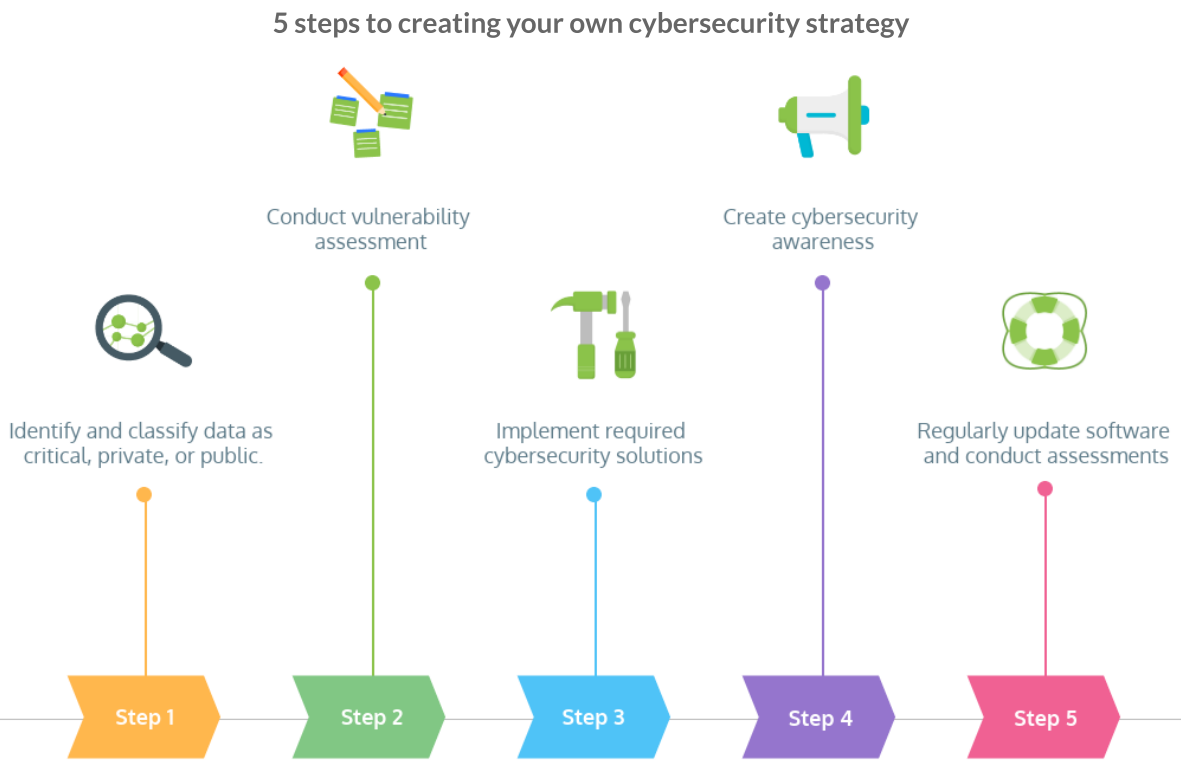
WebTitan	Avast for Business	ZeroBounce
Webroot	AVG Business edition	ZEROSPAM
Netwrix Auditor	WebTitan	Topsec email security
Teramind	Symantec Solutions	SpamPhobia

For a longer list of products and [user reviews](#), visit [GetApp’s IT security software directory](#). You can also use our [comparisons tool](#) to compare products on features, price, and integrations.

Building a small business cybersecurity strategy

Cybersecurity is not a visible business aspect that generates revenue. But fail to do it, and the costs will be high.

Preparing a cybersecurity plan and strategy requires you to cover every aspect of your IT organization—data, networks, devices, servers, and software applications. You need to prepare a foolproof plan that not only involves implementing software or hardware tools that secure your IT networks, but also includes training employees, creating awareness about cybersecurity best practices, and building a security-driven culture.



Source: [GetApp®](#)

Additional resources

If you would like to explore more resources on various IT security topics, visit our Security Lab. You may also like to read:

- [Endpoint security vs antivirus software: Which does your small business need?](#)
- [Everything you need to know about security assessments to safeguard your data](#)
- [A security assessment template for small businesses: Evaluate your IT security](#)
- [“Thou shalt backup thy data”: 10 commandments for small business data backup](#)

METHODOLOGY

Products identified in this article are among the top five with the highest average customer rating in their respective markets/categories. The highest average rating is a function of number of user reviews and star rating.

¹We conducted this survey in April and May 2017 among 699 U.S.-based SMBs, with more than 10 employees and annual revenue of less than \$100 million. The survey excluded nonprofit organizations. The qualified respondents are decision-makers, or have significant influence on the decisions related to purchasing technologies for their organization

Note: The information contained in this article has been obtained from sources believed to be reliable. The applications selected are examples to show a feature in context, and are not intended as endorsements or recommendations.

[Facebook](#)[Twitter](#)[LinkedIn](#)

0 Comments

GetApp Lab

1 Login ▾

 Recommend Tweet Share

Sort by Newest ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

Be the first to comment.

ALSO ON GETAPP LAB

Manage remote teams effectively for good project performance

1 comment • 3 months ago

**Nick Boyle** — With the right set of tools for work management and communication, remote work can be**IT security trends for 2019 and beyond: Cloud, IoT, and threat**

1 comment • 7 months ago

**James Peters** — Thanks for sharing great knowledge, we know that Several businesses are utilizing IoT solutions**5 top-rated collaboration apps for SMART project management**

1 comment • a year ago

**Madona** — Very well written article, For collaboration I'd love to recommend ProofHub. ProofHub brings a blend of**Want to build trust with customers? Use user-generated content**

1 comment • a year ago

**Benjamin** — This is an incredible article, it was a discovery for me. In fact, this is not the first article that talks Subscribe  Add Disqus to your siteAdd DisqusAdd

Subscribe To Our Newsletter



Join our mailing list to receive the latest news and updates from our team.

Name

Email

SUBSCRIBE

Recent Posts

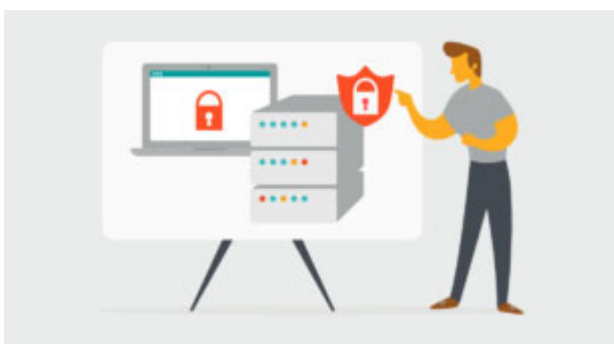
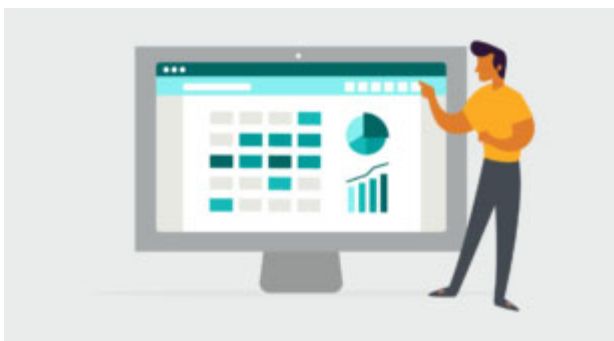


5 Top-Rated Accounting Apps for Keeping Track of Business Expenses



Record GDPR Fine Takes Flight—British Airways Faces \$230 Million Penalty

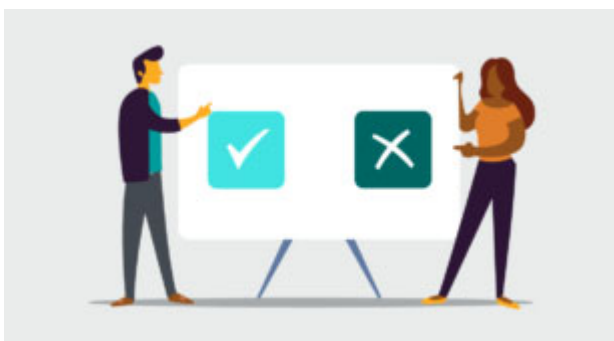
How Selecting Software Is Like Hiring a New Employee



4 Common Encryption
Methods to Shield
Sensitive Data From
Prying Eyes



Understanding Data
Science and Analytics in
Marketing

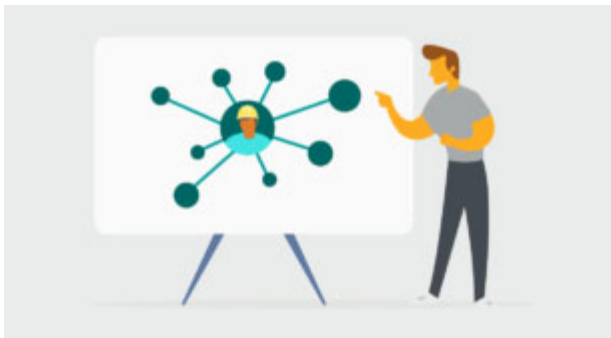


Everything Is Awesome—
According to Your Biased
Management Team

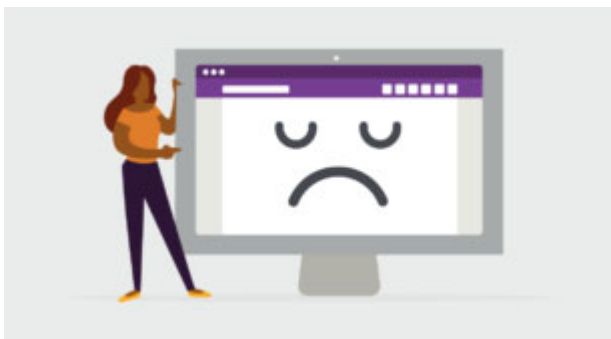
QuickBooks Online Tops GetApp's Latest Ranking of
Accounting Software



Salesforce Sales Cloud
Remains GetApp's
Category Leader in 2019
CRM Software Rankings



How to Boost Customer
Experience With Field
Service IoT



Don't Panic: At Least 20%
of Your Employees Don't
Believe in Your Product

Software Categories

Business Intelligence & Analytics Software

Collaboration Software

Customer Management Software

Customer Service & Support Software

Finance & Accounting Software

HR & Employee Management Software

Communications Software

IT Management Software

Marketing Software

Operations Management Software

Project Management & Planning Software

Sales Software



© 2017 GetApp. All Rights Reserved. GetApp® is a registered trademark of Nubera eBusiness S.L. Nubera eBusiness uses its own cookies and third-party cookies. By using the website you are accepting the use of these cookies. To get more information about our cookies **click here**.