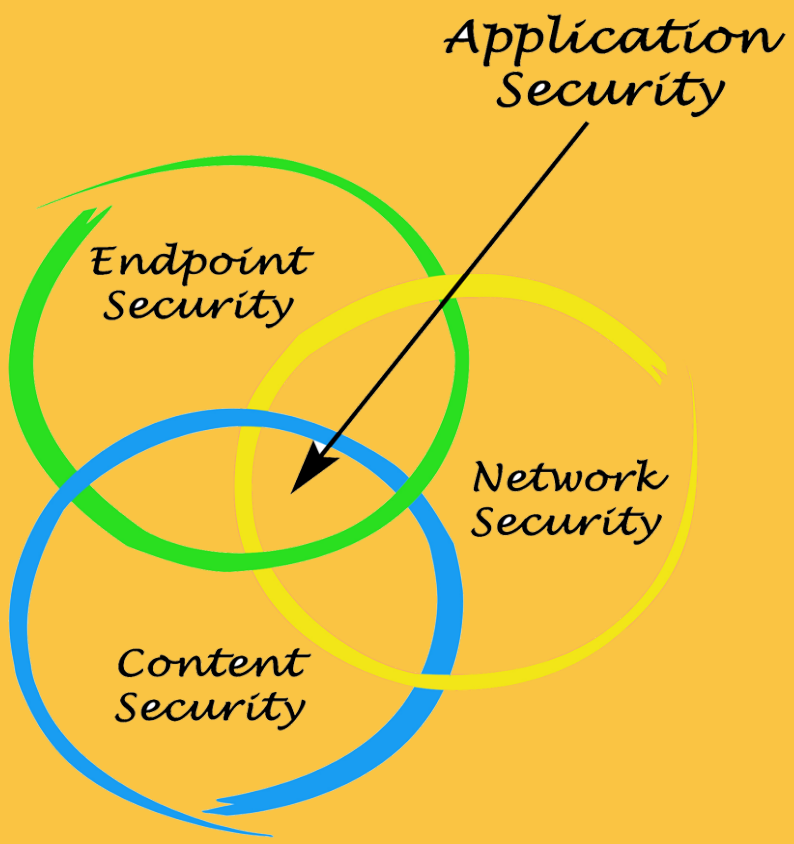
Top Endpoint Security Software Requirements & Features Checklist



SelectHub

Endpoint Antivirus vs Endpoint Security

Did you know cyber attacks cost the global economy a staggering $400 billion per year? With advanced technology, cyber criminals are smuggling themselves into devices all around the world. However, there is software available to block these cyber attacks in the form of antivirus and endpoint security software. Both systems work to protect your company's data and the systems that support your business. And while they're not interchangeable terms for the same systems, there's quite a bit of overlap between the two. To help you decide which product is best for you, we've broken down endpoint antivirus vs endpoint security.

What is Antivirus Software?

To understand the two systems, we'll start with antivirus (AV) software. Antivirus software prevents, detects and removes malware. Malware is any software intended to harm a computer network or its sub-components. Viruses are actually only one kind of malware, but today's antivirus vendors typically protect against a wide variety. The following are some of the most common threats you may encounter online:

Viruses:

This type of malware, aptly named after the ineffective biological agent, duplicates itself using the existing software on your computer. When you run the infected programs, the virus runs and replicates as well. Viruses cause damage in a multitude of ways. They can corrupt your data, waste your network's resources and shut down your system altogether.

Worms:

Worms are similar to viruses but are able to replicate on their own and don't need to utilize any existing software.

Bots:

Bots are another type of malware when used for malicious activity. However, bots are not always malware. For instance, Googlebot is the software used to index the internet for their search engine. Bots perform processes that would be done by an end-user on a computer. They can gather knowledge on sensitive information such as keystrokes, financial information, passwords and more. Botnet attacks are performed using a network of infected devices to attack targets remotely.

Trojans:

Trojans are disguised to look like genuinely useful software but are actually harmful. This is meant to lull the user into a sense of false security so they execute the software on their device. Trojans spread through user action alone, as they cannot duplicate themselves or use other systems to do so.

Ransomware:

This type of malware is used to extort something of value from a user by threatening to publish user information or lock access to their files. In the past, ransomware has often been carried out using Trojans or Worms.

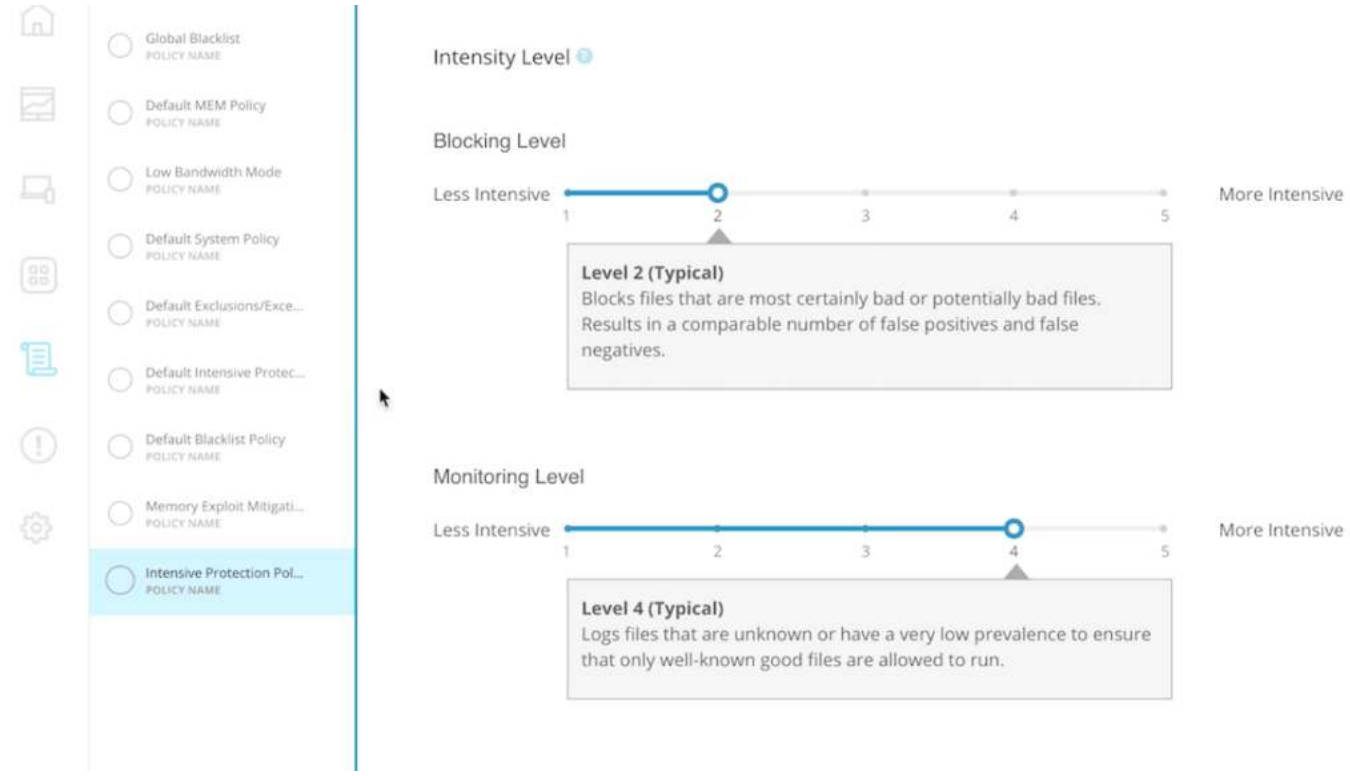
Spyware:

Spyware may use one or several different types of malware to gain and send information without the user knowing. Spyware can be hard to detect on your own, since its primary goal doesn't often involve harming any of your processes. Instead, spyware hides in your system so it can go undetected while it finds your valuable data. This may include credit card or social security numbers in an attempt to steal your identity.

Antivirus software is built to identify these types of malware, and in many cases, automatically remove them. Antivirus software uses both generic and specific heuristics to detect behaviors and techniques that match malware definitions. Some systems alert users to take action to remove threats.

What is Endpoint Security Software?

In case you're unfamiliar, let's start with what "endpoint" means. An endpoint is any device utilized by an end-user, usually in a corporate setting. This commonly includes desktop PCs, workstations, tablets, smartphones, servers and anything else that can connect to the internet. Endpoint security protects the devices within a company via a central management portal.



Many endpoint security systems provide an easy-to-use interface from which to customize your level of security.

Most endpoint security software on the market today contain antivirus capabilities equal to what AV software can provide. However, endpoint security systems emphasize protection against internal threats as well. For instance, endpoint protection provides administrators with device control which allows only certain devices to be connected to an endpoint. An admin might let a USB mouse connect while disabling a USB hard drive. This is to prevent employees from stealing large amounts of valuable data. This data could be used to damage your company's reputation or sold to the competition.

Endpoint security also focuses on remote control of your devices. System administrators typically have access to all company devices through endpoint security software. This need has developed over the years as companies get larger and utilize more technology than your IT staff can manage on an individual basis. Additionally, more employees today are able to work remotely than ever before and offices are becoming more spread out.

With devices so far apart, keeping their software systems up to date is a major challenge. Some of the biggest cyberattacks targeted weaknesses in operating systems that the original developers already discovered and patched. But of course, if you neglect to patch your own system, you're left vulnerable. Endpoint protection's central security management allows your system administrator to deploy patch updates to all computers at once, greatly reducing the staff necessary for this task compared to if you were using standard AV software.

Key Differences

Choosing to implement endpoint security vs endpoint antivirus becomes a little easier after understanding what each system does and the benefits offered. However, there are still a few key differences to discuss.

Endpoint Antivirus vs Endpoint Security

Endpoint Security vs Antivirus Software

When endpoint security software was first introduced, many believed it to be a marketing tactic to reinvent antivirus software. However, endpoint security systems provide more extensive capability than antivirus solutions, making them a great fit for organizations looking to implement comprehensive security management.

	Endpoint Security	Antivirus
Malware Protection *Includes protection against viruses, trojans, worms and more. Blocks incoming threats and removes current ones.*	✓	✓
Mobile Device Protection *Protects against threats on desktop computers as well as mobile devices, such as phones and tablets.*	✓	✓
Web Blocker *Blocks and filters the web to prevent users from accidentally encountering malware on dangerous websites.*	✓	✓
Centralized Security Management *This feature enables a system administrator to manage security settings and devices from a remote location.*	✓	✗
Data Encryption *When files are sent or downloaded, this feature locks the data from being accessed by unauthorized parties.*	✓	✗
Data Access Hierarchies *Allows a system administrator to set up levels of access, preventing employees from accessing private company data.*	✓	✗

source: SelectHub

Endpoint Antivirus vs Endpoint Security

1. Endpoint security software is aimed at enterprises

While enterprise virus protection software exists, endpoint security software is built exclusively with organizations in mind. Antivirus software typically deals with devices on an individual basis. This means threat-detection alerts will only be available on the device affected. To resolve the issue, users will also likely need in-person access to the affected machine.

However, with endpoint security, a system administrator can monitor and solve device issues remotely. Endpoint security software provides an administrator portal through which he or she can configure and monitor company devices. This is not a standard among antivirus software products.

2. Endpoint security software protects against internal threats

This was mentioned in the definition above but merits a header to itself. Did you know over half of all cyberattacks are perpetrated by company insiders? Most antivirus software vendors do little if anything to protect your data from those who access it every day.

Endpoint security vendors provide a comprehensive suite of tools to prevent data loss. These tools include data access protocols which ensure that only authorized employees access certain data. They also include measures to encrypt data so thieves cannot access stolen information.

Endpoint protection software allows users to set allowances based on file extension.

3. Endpoint security solutions are customizable to fit your unique needs

This point goes along with the last one, as system administrators can block certain applications. For instance, if you're worried about your employees downloading files laden with malware, you can block torrenting applications to prevent them from accessing such files. Endpoint security also includes web filtering. This enables your system administrators to block websites known to trick users into downloading harmful software.

System administrators can also set up policies to manage which employees are able to gain access to privileged information. But in opposition to this, overrides may be put in place so higher-ups can quickly retrieve important information. Furthermore, overrides come with auditing tools to prevent abuse.

Which Solution is Right For Your Business?

Considering everything above, it's looking like endpoint protection products provide the most capability between the two systems. However, more capability doesn't always mean that one system will be better for your business over another. In fact, purchasing an overly complex system that you won't end up using can actually end up costing you money without providing enough benefits. Consider the following when choosing which type of solution to invest in:

Number of Users

One of the biggest benefits of endpoint protection is its ability to protect many devices from a central hub. But if only a couple people use internet-connected devices, it might be advantageous to choose antivirus software. This is especially true if your employees are pretty tech-savvy and you trust them to maintain their systems and updates. However, if trust is an issue, we encourage you to keep reading.

Remote Employees

If your employees work from home or you have several offices, endpoint security software may be beneficial. Even if you don't have many employees, the distance between them could make it impossible to manage their devices in person. Endpoint security makes it possible for your system administrator to access the device remotely and solve any issues an employee may have.

Information Value

If there's any reason why someone with access to your company devices would steal information, an endpoint security system is highly recommended. Some businesses house confidential information that could hurt clients. There's also information that could damage your business reputation and information that could be sold to the competition. As you've read above, internal attacks are a major threat to businesses. In these situations, antivirus software just won't cut it. To fully protect your information from those closest to it, you'll need endpoint security software.

Bottom Line

Ultimately, a good endpoint security system should encapsulate all the functions of antivirus software while also protecting against internal threats. Endpoint protection software also provides centralized security management, which is a highly valuable asset at the enterprise level. If you think endpoint security software is the right solution for you, make sure to check out our in-depth comparison report of the top systems on the market.

Endpoint Security Software Requirements & Features Checklist

Did you know that 60 percent of cyber attacks on corporations come from people and devices inside the company? Whether the attacks are by malicious employees trying to steal information or by external hackers finding vulnerabilities in your infrastructure, endpoint security software can help protect your company's valuable resources.

Endpoint security systems provide your company with the means to protect all endpoint devices, such as PCs, workstations, tablets, phones and servers. But in order to get the right functionality from your endpoint protection system, you'll need to come up with a list of requirements. As luck would have it, we've created an endpoint security software requirements checklist to help you decide what features your company needs. Use it in conjunction with our customizable template, included in this document, to create your own list of requirements.

Top Requirements

Policy Management

Policy management is really just a fancy term for what kind of rules you can set for users and devices. Companies can use policy management tools to decide who gets access to certain data and what tasks they have to perform to get it. You can set up policies custom to the user and to the device. You can also set up policy override protocols to allow higher ups access to data wherever they may need it. Additionally, override procedures include alerts and audit trails, making it easy to trace unauthorized access.

- ✔ **Device Based Policies**
- ✔ **User Based Policies**
- ✔ **Override Policies**

Patch Management

Patch management ensures that any security vulnerability is repaired in a timely manner. Many cyber attacks target weak points in a system for which a patch has already been created. But it takes a certain level of vigilance to ensure each device in a company is up to date, especially when using end-of-life operating systems or with a number of employees working remotely.

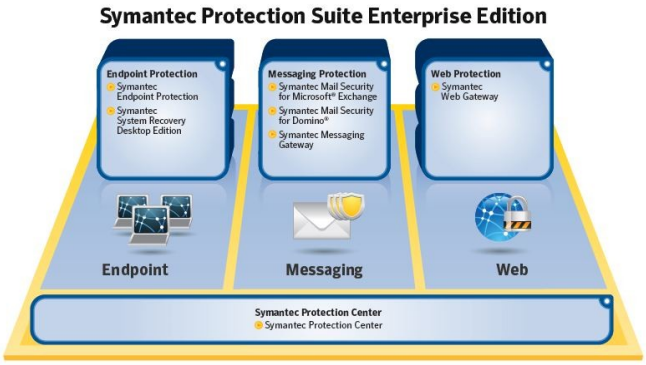
Patch management automates the collection and delivery of patches company-wide. Some systems can create a convenient list of devices that need patching and allow users to schedule and deploy patches remotely. Patch management also uses machine-learning and analysis to determine patch priority. If multiple patches are needed for one device, your endpoint security solution should be able to determine which is addressed first.

- ✔ **OS and Applications**
- ✔ **Asset Management and Discovery**
- ✔ **Remote Devices**
- ✔ **Deployment Architecture**
- ✔ **Scheduling Updates**

Configuration Management and Management Options

These tools provides a centralized control panel to manage all your other endpoint security features. System administrators use configuration management to edit and establish policies, receive alerts, view audit trails and detect when users are attempting an override. This allows greater visibility into threats and gives administrators the ability to make exceptions when users need to access certain applications or information.

Endpoint Security Software Requirements & Features Checklist



Customize your level of aggression when it comes to protecting your endpoint devices.

Conversely, system administrators have the ability to completely shut down processes when an unauthorized user attempts restricted activities. Furthermore, this is the space in which users can perform or schedule mass updates outside of work hours. But users can install software or update endpoints on an individual basis as well.

- ✔ Defining and Managing Configuration
- ✔ Editing
- ✔ Scalability
- ✔ Exception Management
- ✔ Application Control
- ✔ Automatic Client Updates
- ✔ Live Security Alerts
- ✔ Mass Updates
- ✔ Remote Software Installation and Updates

Device Control

This feature allows users to inspect external devices connected to the endpoint, typically through USB. However, many systems also have the capability to monitor local disk, CD and DVD drives, Bluetooth connection, and cloud storage. Moveover, users can pick and choose which devices to allow and which to block. For instance, you may choose to allow a USB connected mouse but not a USB connected hard drive. Exceptions can be applied using product information such as serial numbers.

Additionally, device control supports encryption of any data that does make it onto an external device. Unauthorized parties won't be able to access any of the stolen data without the encryption key. Further, device control can extend to offline endpoints or endpoints not connected to the company network. These systems will log all user activity offline, while continuing to enforce usual policies.

- ✔ Multiple Device Support
- ✔ USB Device Access Control and Monitoring
- ✔ Workstations
- ✔ Encryption Algorithms
- ✔ Offline Support and Forensics

Advanced Endpoint Protection

Even though the internal threat to corporations is large, it's still important to ward off outside attacks. Top endpoint security systems provide protection against known security threats as well as zero-day attacks. These systems can block attacks coming from email, social media, P2P applications (like Skype and Dropbox) and websites. This ensures that your devices and employees will be protected where they use the internet the most.

Endpoint Security Software Requirements & Features Checklist

Endpoint solutions protect against threats like viruses, rootkits, Spyware, Trojans, Worms and the like. Companies can utilize these systems to detect and automatically remove threats using heuristics and other advanced detection technologies.

- ✔ Blended Threats/Malware Protection
- ✔ Host-Based Intrusion Prevention System (HIPS)/Behavioral Analytics
- ✔ HTTP/Malicious Traffic Detection (MTD)
- ✔ HTTPS Malware Detection
- ✔ Automated Malware and Threat Removal
- ✔ Web Filtering
- ✔ Potentially Unwanted Application (PUA) Blocking
- ✔ Email Filtering and Attachment Scanning
- ✔ Botnet Protection
- ✔ Exploit Blocker
- ✔ Social Media Protection
- ✔ Peer-to-Peer (P2P) Applications

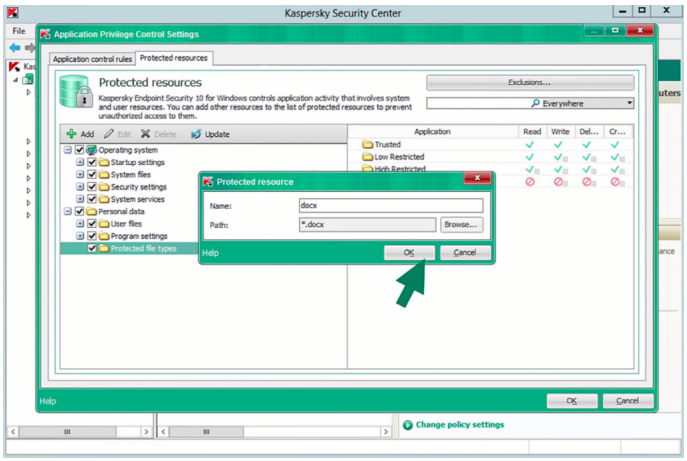
Server Security

When shopping for a new security solution, you'll want to make sure all your endpoints are protected. Servers are an especially sensitive endpoint, so it's important to choose a system that can protect them just as well as it would a desktop PC. Make sure your system can block threats to collaboration servers, data storage servers, internet gateways and your email servers. Some vendors apply existing features to protect your servers, while others use specialized tools for each type of server.

- ✔ Collaboration Servers
- ✔ File Servers
- ✔ Gateway Servers
- ✔ Email Servers

Data Loss Protection

Data loss protection (DLP) includes tools that allow system administrators to manage the network and prevent data loss and leaks across all company endpoints. DLP works through encryption, customized rules, remote access and user authentication. Encryption tools prevent files from being shared by employees through the internet via chat or email. Further, if the system administrator detects a user attempting to share privileged information, the admin can remotely wipe the hard drive to prevent any breaches.



Secure your files by extension to ensure protection of your most valuable documents.

- ✔ Endpoint Encryption
- ✔ DLP Configuration
- ✔ Remote DLP
- ✔ Secure Authentication

Endpoint Security Software Requirements & Features Checklist

Mobile and Virtual Environment

The same way you need server protection from your endpoint software, your company needs protection for mobile devices, too. Just like with a desktop, endpoint solutions allow restriction of application use. You can choose which apps a user will have access to and can monitor activity as well. For further security customization, admins can set lock screen timers, password requirements and block camera usage. And in the case of stolen or lost property, an administrator can erase all data from the device.

This feature also supports virtualized environment security. Virtualized environments are a great way to maximize capability from existing hardware, but you have to make sure each virtual machine (VM) is protected. Endpoint security solutions provide protection for your VMs even when they exist in the same physical equipment.

- ✔ **Mobile Device Management**
- ✔ **Mobile Security**
- ✔ **Virtualized Environments**
- ✔ **Full Disk Encryption**

Security Management Options

On-premise and cloud-based security both have their pros and cons. But since most of the top systems offer both management options, this requirement probably won't affect your software selection. But it's still good to look out for so you don't find the system of your dreams just to learn it's not offered in the cloud or vice versa.

Cloud systems offer security management from any internet connected device and can provide robust reports and real-time notifications. Cloud-based products also reduce the initial resource spend setting up the system. On-premise software isn't necessarily more expensive long-term, but it does require more investment up front.

It also gives companies more control and privacy, as all the data is hosted in-house. However, this privacy benefits hackers as well. With an on-premise system, they can launch "practice" attacks on their own servers without anyone knowing what they are working on. It's much harder to find vulnerabilities in cloud-based products, since they need to be connected to the vendor who would be able to see the attacks.

- ✔ **On-Premise**
- ✔ **Cloud-Based**
- ✔ **Hybrid**

Next Steps

After you've decided what features and other aspects of endpoint security software your business needs, it's time to compare vendors. In addition to our customizable template, we also offer a free comparison report detailing the top systems' features and how they compare to each other. Our analyst team scores each vendor based on how well they offer top requirements, like the ones listed above. Use the report along with your own requirements to see which vendor can offer you the perfect endpoint security solution for your business.

See the following pages for more information on SelectHub vendor evaluations, tools, and services.

Get Expert Selection Help

Flexible | Data-Driven | Affordable

Save time and get the best results at any stage of your selection project.

Let a trained SelectHub specialist guide you to success. Ask about our guided requirements gathering, standardized requirements lists, and end-to-end software selection packages.

Learn More About SelectHub Services

"Fantastic experience! I really like how SelectHub has your back - no pressure. They really understood the problems we were having and ultimately provided help that was professional, and efficient."

Operations Support Leader,
Global gauge manufacturer

"SelectHub has simplified our entire process—leading to better requirements understanding, better buy-in from all stakeholders, and better selection of technology."

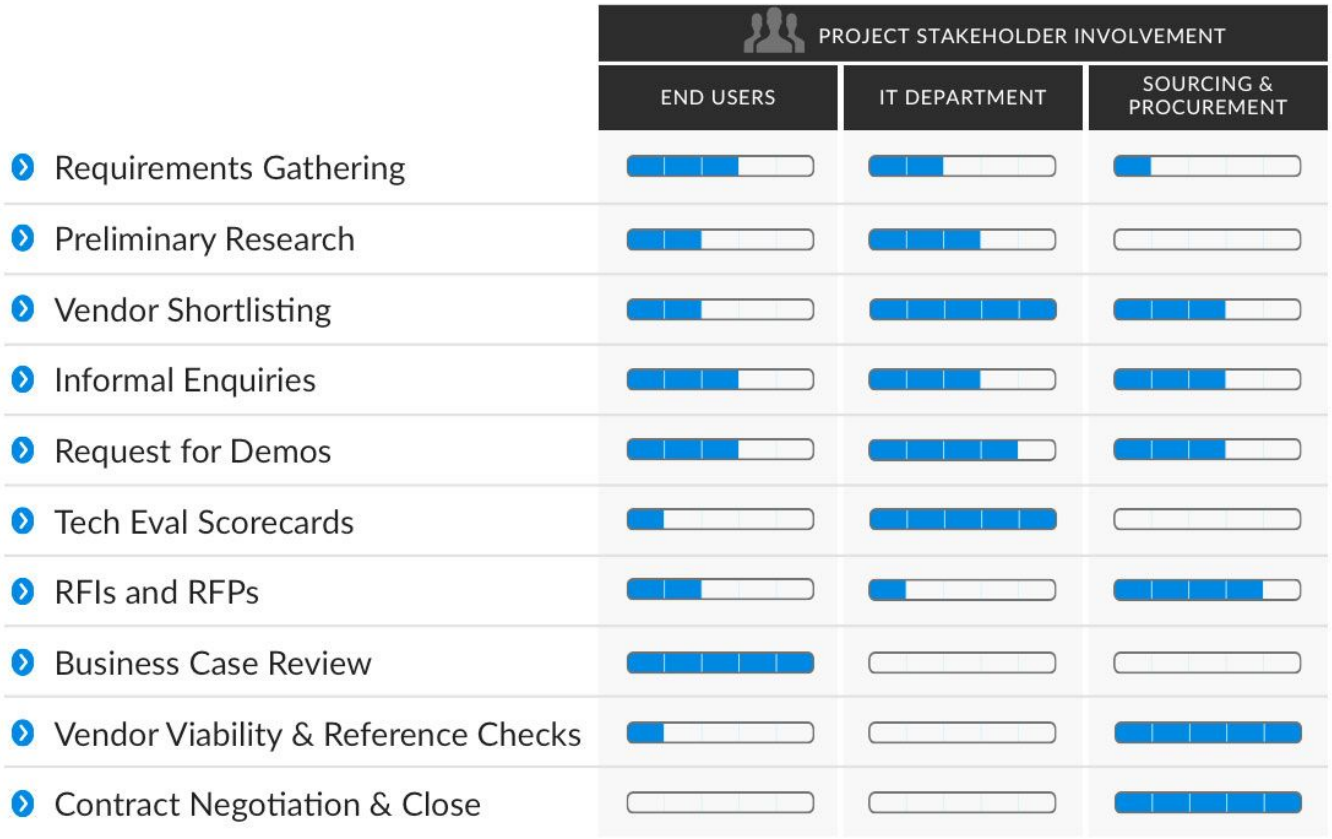
Rob Meilen, VP & CIO, Hunter Douglas

Find out More

Choosing enterprise software is a major business decision—why risk it?

Source: SelectHub

Technology Selection & Sourcing Process



SelectHub's bite-sized approach is easy to follow and provides the best results.

Regardless of whether an organization is making a small or a large IT purchase, our **Technology Selection Management (TSM)** platform enables relevant stakeholders to come together and follow bite-sized process steps to achieve an objective, informed and consensus-driven purchasing decision. The specific process steps can be based on criteria such as project budget size, scope and sponsorship or even broader aspects such as organizational policies and compliance needs.

Find out More

Find the Best Endpoint Security Software for Your Business

Free software selection assistance:
Call 855-850-3850

SelectHub