ITAS 241 Project 1: Enterprise Anti-Malware

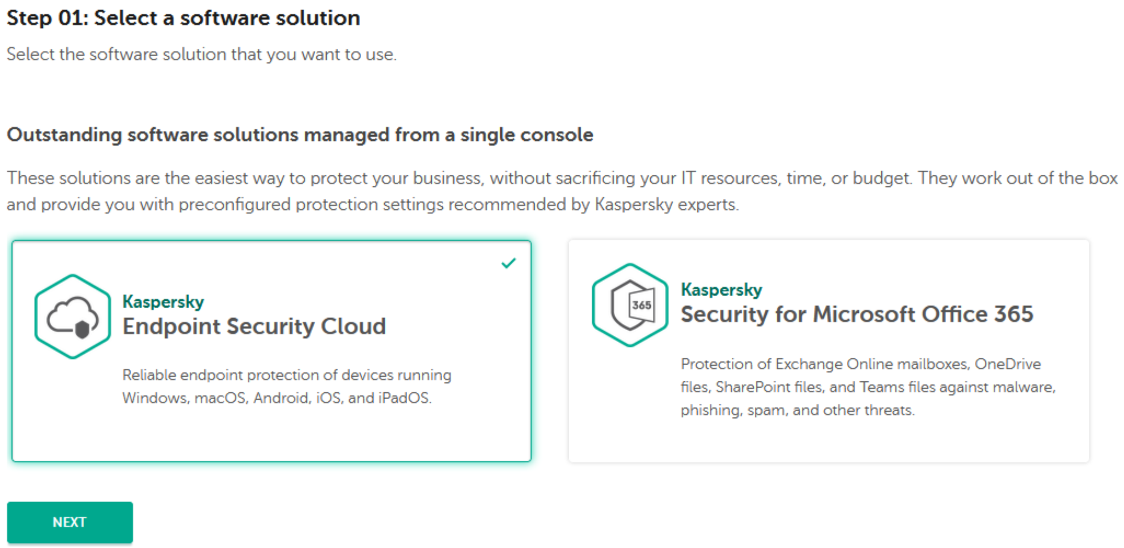
By: Ethan Holmes

Table of Contents

Anti-Malware of Choice and Features

For testing of anti-malware products, I have chosen to use Kaspersky Endpoint Security for Business. The reason for choosing Kaspersky was based on the 4 products that I had chosen to test, 2 did not get back to me in my acceptable timeframe, which was around 2 days. The other options that I had requested a trial from were Crowdstrike and Elastic, with Sohos being my 4th option however ultimately, I decided to go with Kaspersky.

Upon signing up for the Kaspersky Endpoint Trial, you are given the option to choose a software solution that you would like to use on the cloud platform, Endpoint Security Cloud, which is the basic option with all standard options that are included by Kaspersky, or Security for Microsoft Office 365 which offers the same features, but with added protection for monitoring Exchange online , OneDrive, and Teams with advanced threat protection to scan these services for malware, phishing and spam protection.



Step 01: Select a software solution

Select the software solution that you want to use.

Outstanding software solutions managed from a single console

These solutions are the easiest way to protect your business, without sacrificing your IT resources, time, or budget. They work out of the box and provide you with preconfigured protection settings recommended by Kaspersky experts.

Kaspersky Endpoint Security Cloud ✓

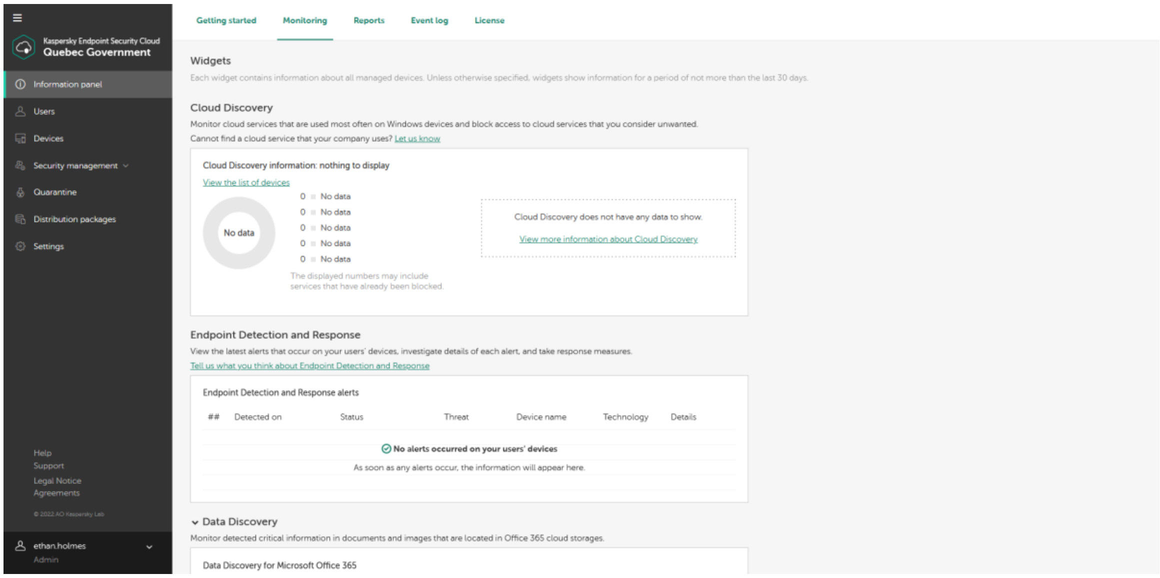
Reliable endpoint protection of devices running Windows, macOS, Android, iOS, and iPadOS.

Kaspersky Security for Microsoft Office 365

Protection of Exchange Online mailboxes, OneDrive files, SharePoint files, and Teams files against malware, phishing, spam, and other threats.

Figure 1: Choices for Kaspersky Software solutions

Once you have created your business profile and have selected your choice of protection, you are then greeted with the Information Panel, which is an overview of all the devices and users that you have added to your cloud hub.



Widgets

Each widget contains information about all managed devices. Unless otherwise specified, widgets show information for a period of not more than the last 30 days.

Cloud Discovery

Monitor cloud services that are used most often on Windows devices and block access to cloud services that you consider unwanted.

Cannot find a cloud service that your company uses? Let us know

Cloud Discovery information: nothing to display

View the list of devices

0 No data
0 No data
0 No data
0 No data
0 No data

The displayed numbers may include services that have already been blocked.

Cloud Discovery does not have any data to show.

View more information about Cloud Discovery

Endpoint Detection and Response

View the latest alerts that occur on your users' devices, investigate details of each alert, and take response measures.

Tell us what you think about Endpoint Detection and Response

Endpoint Detection and Response alerts

##	Detected on	Status	Threat	Device name	Technology	Details

No alerts occurred on your users' devices

As soon as any alerts occur, the information will appear here.

Data Discovery

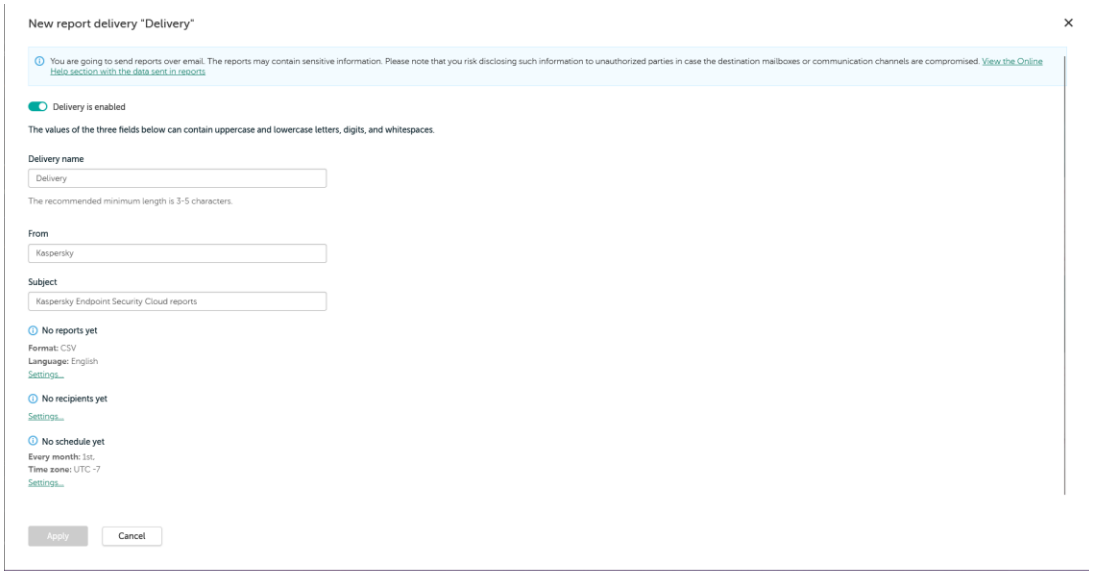
Monitor detected critical information in documents and images that are located in Office 365 cloud storages.

Data Discovery for Microsoft Office 365

Figure 2: Overview for Kaspersky Cloud Hub

The left panel on the cloud hub also offers tabs for Users and Devices, which let you add and manage all users and devices that you have added to your cloud hub. Quarantine, which holds any files that have been deemed a potential threat and can then be restored via the Cloud Hub if it is safe to use. Near the bottom we have Distribution Packages, which lets you download a client version of Kaspersky that can be installed locally and includes some additional features such as Network Monitoring, as well as the ability to link a logon script to a GPO to install across the domain or email the executable to others in your domain and have them download it which I think is an easy feature to help deploy your anti-malware.

The Reports tab at the top also allows an Administrator the ability to schedule reports to be sent to an email on a scheduled basis. This will let you select which type of reports that you would like to be sent, and you can when you receive them on a daily, weekly or monthly basis, a helpful feature for Administrators who need to see security reports on the fly while being able to set and forget.



New report delivery "Delivery"

You are going to send reports over email. The reports may contain sensitive information. Please note that you risk disclosing such information to unauthorized parties in case the destination mailboxes or communication channels are compromised. View the Online Help section with the data sent in reports

Delivery is enabled

The values of the three fields below can contain uppercase and lowercase letters, digits, and whitespaces.

Delivery name: Delivery

The recommended minimum length is 3-5 characters.

From: Kaspersky

Subject: Kaspersky Endpoint Security Cloud reports

No reports yet

Format: CSV
Language: English

No recipients yet

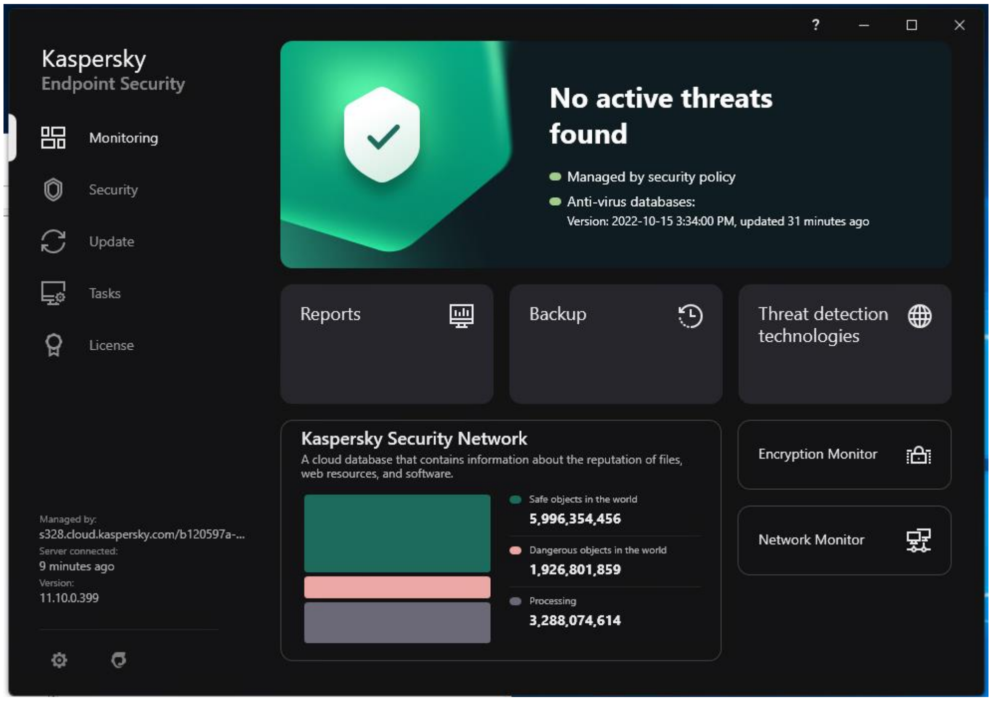
No schedule yet

Every month: 1st.
Time zone: UTC -7

Figure 3: Generating Reports

The Security Management tab on the left, is where many features that a user would care about are stored. Disk Encryption provided through, which is used to protect against ransomware, as well as Endpoint Detection which alerts you to any issues on a device, and Vulnerability report which will look at the current version of any applications or Operating Systems that you are using and will report any known security issues with them.

Moving to the Server side of Kaspersky, we can see the interface that it uses in the figure below. I found the server interface to have less functionality compared to the Cloud client. However, the reporting on the client is much more detailed with better graphs to show recent information about the services you want to see details on.



No active threats found

- Managed by security policy
- Anti-virus databases:
  Version: 2022-10-15 3:34:00 PM, updated 31 minutes ago

Kaspersky Security Network

A cloud database that contains information about the reputation of files, web resources, and software.

- Safe objects in the world: 5,996,354,456
- Dangerous objects in the world: 1,926,801,859
- Processing: 3,288,074,614

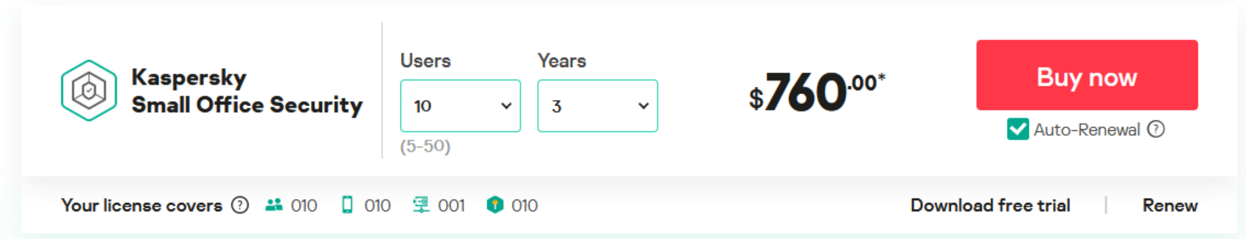
Managed by:
s328.cloud.kaspersky.com/b120597a-...
Server connected:
9 minutes ago
Version:
11.10.0.399

Figure 4: Kaspersky Local Agent

There's also the ability to actively update the databases for better protection against zero-day attacks and up-to-date protection against malware and ransomware in general.

Pricing and Recommendation

Kaspersky has various pricing models for their enterprise services depending on the size of your business. For small office solutions, Kaspersky Small Office Security comes in at $760.00 USD for 10 users over 3 years, up to $3,600 for 50 Users over 3 years.



Users: 10 (5-50)
Years: 3

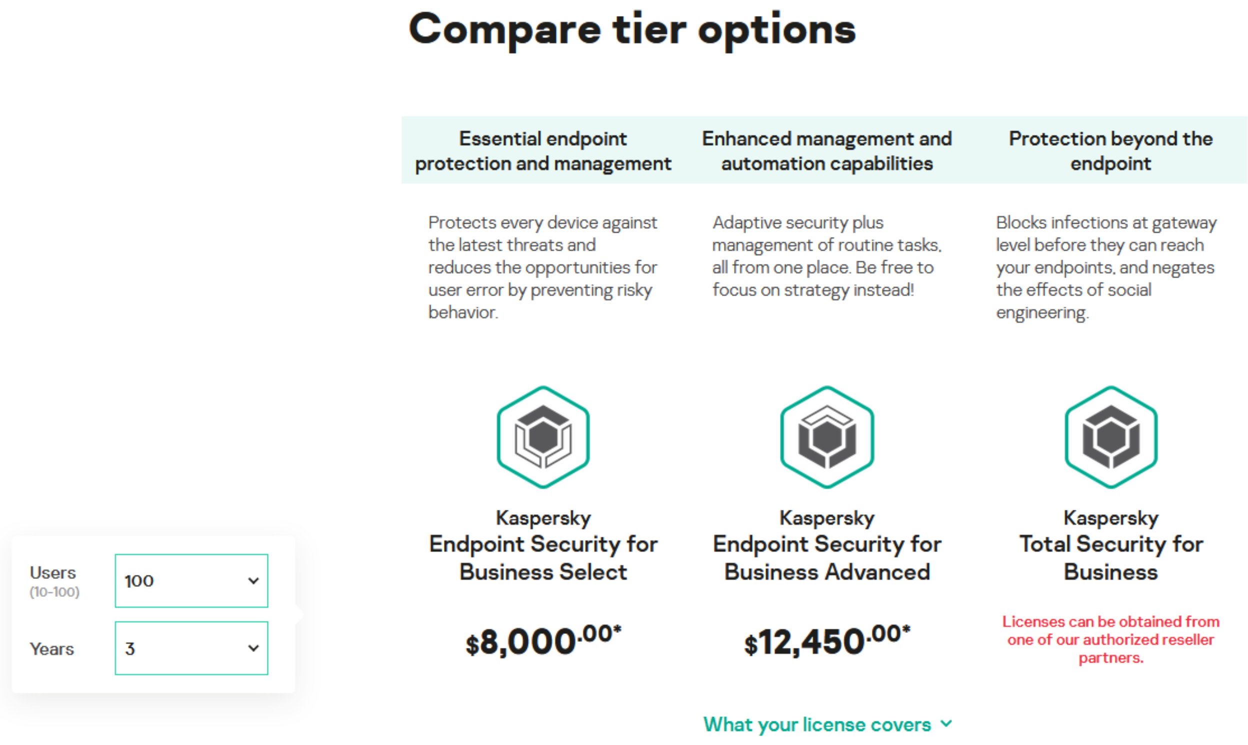
$760.00*

☑ Auto-Renewal

Your license covers 010 010 001 010

Figure 5: Price for Kaspersky Small Office

While medium-sized businesses who maybe looking for more protection with more enterprise features, we can see the various pricing for 100 users over 3 years.



Compare tier options

Essential endpoint protection and management	Enhanced management and automation capabilities	Protection beyond the endpoint
Protects every device against the latest threats and reduces the opportunities for user error by preventing risky behavior.	Adaptive security plus management of routine tasks, all from one place. Be free to focus on strategy instead!	Blocks infections at gateway level before they can reach your endpoints, and negates the effects of social engineering.
Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business
$8,000.00*	$12,450.00*	Licenses can be obtained from one of our authorized reseller partners.

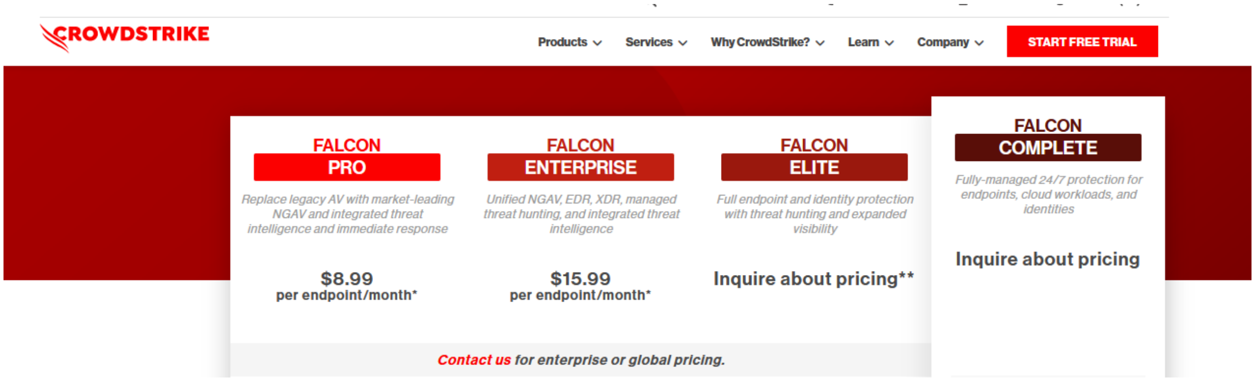
Users (10-100) 100

Years 3

What your license covers

Figure 6: Kaspersky Enterprise Pricing

We can compare this to a leading competitor such as CrowdStrike, who charges per endpoint per month.



FALCON PRO	FALCON ENTERPRISE	FALCON ELITE	FALCON COMPLETE
Replace legacy AV with market-leading NGAV and integrated threat intelligence and immediate response	Unified NGAV, EDR, XDR, managed threat hunting, and integrated threat intelligence	Full endpoint and identity protection with threat hunting and expanded visibility	Fully-managed 24/7 protection for endpoints, cloud workloads, and identities
$8.99 per endpoint/month*	$15.99 per endpoint/month*	Inquire about pricing**	Inquire about pricing

Contact us for enterprise or global pricing.

Figure 7: Crowdstrike pricing for reference

At $15.99 per user per month, to cover 100 users for one year comes out to around $19,200 USD, a near $6,500 dollar difference that could be used to allocate funds elsewhere in the business.

After using and testing Kaspersky Endpoint Security, I would recommend this product for a business that is looking for a reliable product while looking for a cheaper price than what another competitor in the enterprise malware protection industry could give you.

References

Kasperskysecurity for MicrosoftOffice 365. Kaspersky. (n.d.). Retrieved October 17, 2022, from https://www.kaspersky.com/small-to-medium-business-security/microsoft-office-365-security

Enterprise-grade endpoint protection. Kaspersky. (n.d.). Retrieved October 17, 2022, from https://www.kaspersky.ca/business/endpoint-security

Endpoint Security & Protection Products: CrowdStrike. crowdstrike.com. (2022, October 11). Retrieved October 17, 2022, from https://www.crowdstrike.com/products/

Link to Video Submission

https://youtu.be/XAR4e780hic