Acronis Cyber Protect vs. Kaspersky Endpoint Security for Business

PRODUCTS COMPARED

ACRONIS	Kaspersky
Acronis Cyber Protect	Kaspersky Endpoint Security for Business

SOLUTION OVERVIEW

Kaspersky Endpoint Security for Business offers an advanced endpoint protection solution but it lacks data protection and recovery features, critical when dealing with modern cyber threats. Moreover, thorough visibility over data protection and endpoint remote management capabilities are limited, increasing IT management burden.

With **Acronis Cyber Protect,** businesses avoid downtime, data loss and security breaches with a complete cyber protection solution that offers backup, next-generation cybersecurity, and security management functions all in a single agent. Modernize your cybersecurity and data protection with integrated cyber protection delivering unique capabilities, better performance, compatibility, and the shortest recovery times – plus multi-layered anti-malware technology minimizes the need for recovery itself.

QUICK DEPOSITION STATEMENTS

- **Recovery and backup protection:** Kaspersky can't recover data and doesn't scan the backup repositories of 3rd party tools for malware, increasing the risk of recovery of infected data, while Acronis enables fast, easy, and safe recoveries with built-in antimalware scan of backups and patching and anti-virus updates.
- **Investigations:** Kaspersky can't aid breach investigations, while with Acronis Cyber Protect you have ready access to revealing forensics data, stored in backups.
- **Visibility:** Kaspersky has limited risk visibility with no broad view over the protection status of all data, leaving a high risk of data loss due to unprotected assets, while Acronis uses automatic data classification to track the protection status of all important files and provide quick remediation actions for protecting them..
- **Remote assistance:** With Kaspersky administrators are unable to remotely manage endpoints, while Acronis provides built-in capabilities for secure, remote access to endpoints.

AREAS WHERE ACRONIS CAN'T COMPETE WITH KASPERSKY

- **Independent product evaluations (3rd party tests)** – *Kaspersky might be a leader in historic evaluations, however latest tests are the ones that provide relevant information based on last product versions. Since 2020, Acronis Cyber Protect has been tested by some of the most credible testing laboratories, including AV-TEST, AV-Comparatives, ICSA Labs, and Virus Bulletin, being among the frontrunners in the category, along with Kaspersky.*
- **Cybersecurity for mobile devices** – *Acronis provides data protection for mobile devices' data.*
- **Email security**
- **EDR** (Kasersky's EDR comes as an add-on at an additional cost)
- **Device control**
- **Application control**

HOW TO DEPOSITION KASPERSKY – DETAILED PITCH

KASPERSKY ENDPOINT SECURITY FOR BUSINESS	ACRONIS CYBER PROTECT
RECOVERY	
Limited tools to recover from cyberattacks ✔ Remediation engine - rollbacks actions that have been performed by malware in the operating system (e.g. deleting executable files, partitions, and registry keys created by malware) – No data protection – can't recover affected data – No backup protection – if you rely on a third-party backup, Kaspersky can't scan backup repositories off-site, targeted by modern cyber threats (e.g. Maze, DopplePaymer, Sodinokibi ransomware; rootkit, bootkit). This increases the risk of recovering infected data.	**Enables safe, fast, and easy recoveries, ensuring no data loss** ✔ Integrated data protection – uses backups to recover affected data ✔ Anti-malware scan of backups ✔ Automatic ransomware recovery – Acronis Active Protection ✔ Safe recovery – anti-malware backup scans, installation of latest security patches and anti-virus definitions updates as part of recovery process ✔ Absolutely no data loss – ability to backup changes to critical apps between schedules backups (CDP)
GOLDEN QUESTIONS: 1. **Do you have a security tool in place to recover data in case its affected (deleted/encrypted) by malware?** – *refer to integrated data protection - backup* • **Are this tool's off-site repositories (Backup/VSS), from which you recover data, protected against storing and recovering malware in any way?** – *refer to antimalware scans in backups* • If backup is used: **Does the recovery you depend on, ensure absolutely no data loss: can it recover critical assets to the last known good state, even if changes were made between scheduled backups?** - *refer to Continuous Data Protection* **2. Have you ever been a victim to ransomware attack?** • **Are you aware that more advanced ransomware families such as Maze, Sodinokibi, DopplePaymer, target not only data on the endpoint, but VSS and backup repositories as well?** – *refer to antimalware protection of backups + Active Protection's ransomware rollback* 3. **Have you been a victim to a reoccurring cyber threat after recovery?** – *refer to safe recovery*	
INVESTIGATIONS: FORENSICS	
Can't support data breach investigations – No ability to investigate what happened in the event of cyberattack – doesn't collect forensic data – Increased cost - you need to license a separate solution (Kaspersky Incident Response) in order to access the functionality	**Ready-access to revealing forensic data** ✔ Eases investigations – collects forensics data (snapshots of full memory dumps, unused disk space, and running processes) ✔ Forensics data stored in backups for better security ✔ Makes investigations and legal representation less costly
GOLDEN QUESTIONS: 1. **Have you ever been a victim to an incident (cyber attack/internal data loss) you had to investigate internally?** – *refer to built-in Forensics*	

2. **Are you legally obliged to report breaches, involving customer data, to the authorities?** – *refer to ability to use forensics in reporting*
3. **Do you store sensitive data of other prospects – e.g. partners/customers? Are you under risk of being sued by such prospects in case their sensitive data gets leaked?** – *Increases the risk/need;* Refer to *Forensics stored in backup (secure) to ensure evidence in court and limit damage*

VISIBILITY

No ability to track the protection status of all data	Visibility into the protection status of all data
– Limited risk visibility – no broad view over protected assets – Critical data can be exposed for attacks	✔ Data protection maps – discover all data important for your organization and display detailed information about its protection status ✔ Protection for exposed data – get alerts about exposed critical data, and protect it with a few clicks ✔ Visibility over data distribution across endpoints ✔ Reporting – detailed report to serve as a basis for compliance reporting.

GOLDEN QUESTIONS:

1. **Are you aware of all the places critical data resides in your organization?** – *Data protection map*
2. **Do you have visibility over the protection status of each asset in your organization?** – *Data protection map*
3. **Have you ever come by exposed critical data on endpoints? / Have you ever lost data after a breach because it was not backed up?** – *Data protection map for visibility of unprotected sensitive content*
4. **Do you need to generate compliance reports regarding the protection status of all data in your organization?** – *Data protection map serving as basis for compliance reporting*

REMOTE MANAGEMENT

Limited remote management capabilities.	Powerful remote management capabilities with built-in remote desktop
✔ Remote deployment - automatic discovery of machines and remote agent installation ✔ Remote device wipe ✔ Disk health monitoring – Can't manage endpoints remotely	✔ Centralized management for cybersecurity and data protection (cyber protection) ✔ Remote deployment - automatic discovery of machines and remote agent installation ✔ Remote device wipe ✔ Disk health monitoring ✔ Eases remote endpoint management – built-in remote access to machines via RDP; remote bootable media controls for more extreme cases

GOLDEN QUESTIONS:

1. **How regularly do you need to provide IT assistance internally or manage protected endpoints?** – Built-in *Remote Desktop and assistance*
    - **Does this process require a lot of efforts? How can it be made more effortless?** – *Remote assistance eases administrative efforts*
    - **Do you have the tools to make this remotely?** *Eases administrative burden*

2. **Do you find the number of tools you're using for data protection and cybersecurity burdensome?** – *Refer to Integration of data protection, cybersecurity and multiple security management capabilities*
    - **Do you think security efficiency could be increased if IT administrators spend less time managing security tools and more time focusing on optimizing the security strategy?** – *Centralized management of data protection and cybersecurity*

FEATURE-BY-FEATURE COMPARISON

	KASPERSKY ENDPOINT SECURITY FOR BUSINESS	ACRONIS CYBER PROTECT
Supported languages	22 languages	25 languages
DEPLOYMENT OPTIONS		
Vendor's cloud (SaaS)	✓	✓
On-premises (software)	✓	✓
SUPPORTED OPERATING SYSTEMS		
Windows	✓	✓
Mac	✓	✓
Linux	✓	✓
SUPPORTED MOBILE DEVICES		
Android	✓	X
iOS	✓	X
ANTI-MALWARE FEATURES		
Real-time anti-malware and anti-ransomware protection	✓	✓
On-demand scanning and malware removal	✓	✓
Pre-execution AI-based analyzer	✓	✓
Behavioral analysis and dynamic detection rules	✓	✓
Exploit prevention	✓	✓
Protection against zero-day attacks	✓	✓
Disk and master boot record protection	✓	✓
Real-time malicious cryptominer protection	✓	✓
Automatic file recovery after a ransomware attack	Limited Rollbacks changes with remediation engine	✓
Self-protection	✓	✓
Malware scanning of backups	X	✓
Anti-virus updates of OS images before recovery	X	✓
Installation of the latest security patches before recovery	X	✓
Email security	✓	X
Firewall	✓	X
Protection against emerging threats (threat intelligence)	✓	✓
Auto adjust protection plans based on threat intelligence	X	✓
OTHER CYBER PROTECTION FEATURES		
Integrated vulnerability assessments of systems	✓	✓
Integrated patch management	✓	✓
Automatic backups of endpoints before patching	X	✓
Continuous data protection	X	✓
Data protection maps	X	✓
Compliance reporting	✓	✓
Forensic data collection	X	✓
URL filtering	✓	✓
Network shares and mapped drives protection	✓	✓
Ability to manage Microsoft Windows Defender	X	✓

	KASPERSKY ENDPOINT SECURITY FOR BUSINESS	ACRONIS CYBER PROTECT
Two-factor authentication	✓	✓
Endpoint Detection & Response (EDR)	X Add-on: Kaspersky EDR Optimum	X
Device control	✓	X
Application control	✓	X
MANAGEMENT		
Unified portal for all workloads	✓	✓
Unified policies for data protection and cybersecurity	X	✓
Auto-discovery of machines	✓	✓
Remote agent installation	✓	✓
Remote access to machines via integrated RDP	X	✓
Remote device wipe	✓	✓
Remote bootable media control	X	✓
Hard drive health monitoring	✓	✓