DRIVING DOWN

the Total Cost of Protection

CDW

KASPERSKY lab

TABLE OF CONTENT

Kaspersky Lab – Solid Business Protection BUILT THE RIGHT WAY

In 2009 we witnessed exponential growth in malware proliferation around the world. Over 30,000 new threats hit the wire each day requiring more than 3,500 new malware signatures being released daily by anti-malware companies. 2010 has been no different. In Q1 of 2010 there were over 327 million infection attempts from over 119 million malware hosting servers found on the Internet. According to IBM, the first half of 2010 saw a 36% spike in malware when compared to last year, with more than 10 million new pieces of malware released into "the wild."

Challenges to Every Organization

This rapidly escalating threat landscape, the pressures of ever-changing technology and the daily morphing of how business is done causes numerous problems for companies, regardless of size or industry:

- **Protection of a De-centralized Environment:** Data is the primary target for cybercrime today. Yet, data no longer resides solely in the mainframe or protected server farm. To respond, organizations must have premium protection wherever data resides, resulting normally in higher management overhead and resource strain. Protection is required for systems inside the protective confines of the corporate perimeter, but also for mobile devices, laptops and smart phones, that carry proprietary company data. In fact, Forrester Research's Survey found that the adoption of smart phones and Web-based applications and services represent the two greatest concerns for IT security today.
- **Management of a Heterogeneous Environment:** As the adoption rate of open-source or non-Microsoft operating systems continues to climb in the IT organization, Microsoft Windows systems are no longer the only target for cybercriminals. Organizations today must support and protect numerous platforms: Microsoft, Novell, Linux, Mac, and others. A recent survey by Forrester found that 73% of enterprises cite the complexity of their IT environment as a "major challenge" for their firm and 45% say that having too many security vendors to manage is also a challenge. This support and protection requirement can cause significant management overhead, particularly if multiple management consoles are required.
- **The High Cost of Poor Protection:** Companies are losing millions of dollars each year because their current anti-malware vendor is not able to identify and block threats to their environment. In 2009 those costs doubled to more than $560 million dollars, according to the FBI, and that was only the losses reported. A recent survey by RSA found that 88% of Fortune 500 companies have compromised PC's running Trojans. The cost of poor protection includes loss of data, damage to brand, continuous system reimaging to clean infections, lost employee productivity – and the list goes on.
- **Serious Support Deficiencies:** When there are problems with anti-malware solutions or breaches occur, getting time-sensitive support can be critical. Many companies are experiencing long hold times, call-back promises that are not fulfilled, and 3rd party, off-shore support teams do not have the expertise to solve problems. This strains limited resources, causes extreme frustration, and increases the cost of support and management of your anti-malware solution.

- **Lack of Security Expertise:** As the malware threat escalates, maintaining the number of adequately trained resources to manage the threat can become a real challenge for IT organizations. Companies often have too few resources and lack the security expertise required to maintain an optimum level of threat protection. Forrester Research found that 67% of firms say that their understaffed security department is a challenge for their business.
- **Shrinking Budgets:** IT organizations today are constantly being asked to do more with less as budgets get sliced. IT departments experience budgetary pressures with regard to proper staffing levels, while being asked to provide higher levels of network accessibility, business continuity, and most of all security, which cannot be compromised even under limited resources. It's no secret that effective security requires a multi-layered defense — but the resources required to manage multiple point products from different vendors can overwhelm an IT department. IT security spending has not increased proportionally with the malware threat. Organizations, therefore, must find the best protection possible for their budget and, in the process will sometimes sacrifice protection in certain areas to bolster other areas, often leaving themselves exposed.

IT Security Buying Considerations

Malware protection has long been considered a commodity, with price being the ultimate deciding factor. Some companies even use free malware protection software. Unfortunately, the malware that is often missed by these vendors is also free! "Aren't all AV vendors the same?" some IT managers have asked. Others say "All AV sucks. You pick the one that sucks the least!" While these mindsets are understandable, given the horrid experiences that some customers have had, they couldn't be further from the truth.

In reality, an ineffective anti-malware product can cost substantially more than the purchase price. Numerous factors can drive up the Total Cost of Protection (TCP), which accounts for both the easily-quantified 'hard costs,' as well as the 'soft costs' that are rarely considered when evaluating pricing proposals from vendors. These costs, some more easily quantifiable than others, begin to add up quickly as detection, performance and support issues increase. When considering the right security solution for the business, small, medium, or large, any organization should ask these questions to determine the real cost of protection, not just product price:

- How effective is the anti-malware solution in protecting you from malware? The cost of poor protection can result in significant costs to an organization:
  - lost company Intellectual Property due to stolen data
  - lost employee productivity when systems become unavailable due to malware infections
  - IT resource utilization in reimaging systems
  - lost money from corporate bank accounts due to cyber-theft
  - damage to company reputation
- **Do you sacrifice performance for protection?** Protection is of little use if it impedes the end users ability to perform their daily tasks. "Bloatware," as it's often called, uses systems resources to the point that the employee can no longer use the their computer system until it is finished scanning. Poor performance of your anti-malware solution, resulting in lost employee productivity, can dramatically increase your cost of protection.

- **How many resources and how much time is required to manage your anti-malware security?** The management console is a very important piece of the buying decision. If it is difficult to manage your security posture with a cumbersome, non-intuitive, resource intensive management console, your business will suffer from an increased cost of protection. Management should be simple, easy to use, yet granular and powerful enough to mitigate risk in your environment.
- **What is the real cost of Support?** Many vendors charge additional fees for support, whether standard or premium. Unfortunately, additional hidden costs are often not calculated when considering the overall value. Those costs include excessive hold times, long time-to-resolution, and the lost productivity tied to these common support problems.
- **How competitive is the pricing?** Competitors in the anti-malware space have become extremely aggressive in pricing their solutions. Some even offer it for free. When it comes to malware protection, the old adage rings true, "you get what you pay for." The cost of an anti-malware solution cannot be limited to the purchase price. You may choose the lowest price provider but pay high "soft costs". Or you can chose the highest price vendor and still not get the protection and performance that justifies your investment. Price, while very important, cannot be the ultimate decision criteria as it does not account for the hidden costs of protection.

Many companies are paying a much higher price for protection than they thought, and, in most cases, are not getting the protection they need.

Business Protection Built the Right Way

From its inception in 1997, Kaspersky Lab has been focused on one thing – protecting its customers from malware threat. Along the way, many of its competitors have shifted their focus beyond malware, often leading to a decline in their ability to provide the highest quality malware protection. Kaspersky Lab, with a dedicated world-class team of over 700 anti-malware researchers and engineers, and more than 2000 employees worldwide, has relentlessly maintained its focus, making Kaspersky Lab clearly one of the best in the world at protecting customers from these threats.

It is this focus that has engendered trust in our customers. Today, Kaspersky Lab has emerged as the 3rd largest anti-malware security company in the world and is growing more rapidly than all others, adding over 50,000 new customers a day, so that our products are protecting over 300 million systems worldwide.

Kaspersky Lab has consistently won numerous independent testing awards for our malware detection technologies and solutions:

- VB100: Kaspersky consistently receives one of the highest RAP Scores (Reactive and Proactive Detection Testing) of all its competitors, demonstrating the premium malware protection we provide.
- AV Comparatives: Kaspersky continues to receive the highest rating, Advanced+, because of our ability to detect and remove malware threat.
- Anti-Malware Test Lab: Kaspersky is the only vendor to receive a GOLD award in every category tested, demonstrating our high level of overall threat protection. We were also the only vendor that did not fail any test category.
- AV-Test.Org: According to AV-Test.Org, Kaspersky is the fastest to respond to new threats, responding in less than two hours, significantly reducing the window of exposure to our clients.

KASPERSKY lab

Kaspersky consistently scores higher than the competition in overall protection due to our focus on all malware threat vectors, including:

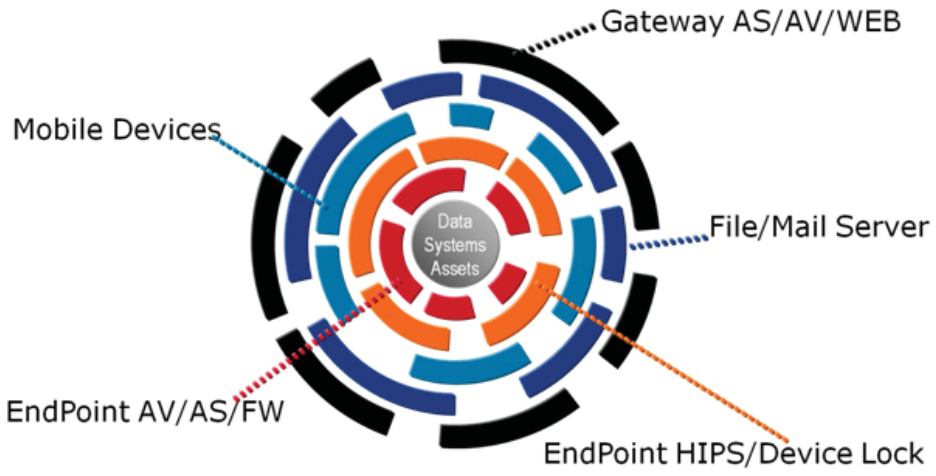
- Anti-Malware Protection
- Anti-SPAM Protection
- Anti-Phishing Protection
- Zero-Day Heuristics
- Rootkit Protection
- Worms/Bots/Trojans/Polymorphic Virus Protection
- Host Intrusion Protection
- Strong Personal Firewall Protection
- Email & Web Malware Protection
- Application and Device Control

It is this extraordinary protection foundation on which Kaspersky builds all its products and it is the core of the layered protection methodology that protects both small and large businesses alike. **We call it The Kaspersky Anti-Malware Protection System.**

The Kaspersky Anti-Malware Protection System

The escalating threat landscape and the need to protect an increasing complex environment are causing real problems for IT organizations across the board. Kaspersky Lab is responding with highly advanced solutions to combat these problems. Our vision and strategy transcends organizational size to provide a unique blend of the finest and broadest malware protection.

Cybercriminal expansion is leveraging every possible vector today to spread malicious content: email, web content, social media, 3rd party application vulnerabilities, among many others. As a result, companies must consider all threat vectors and provide real protection at every layer of the enterprise. A layered malware protection strategy is rarely considered. Many companies today consider malware protection to be simply a commoditized purchase, a security technology required for compliance purposes and, at best, procured for the lowest possible price.

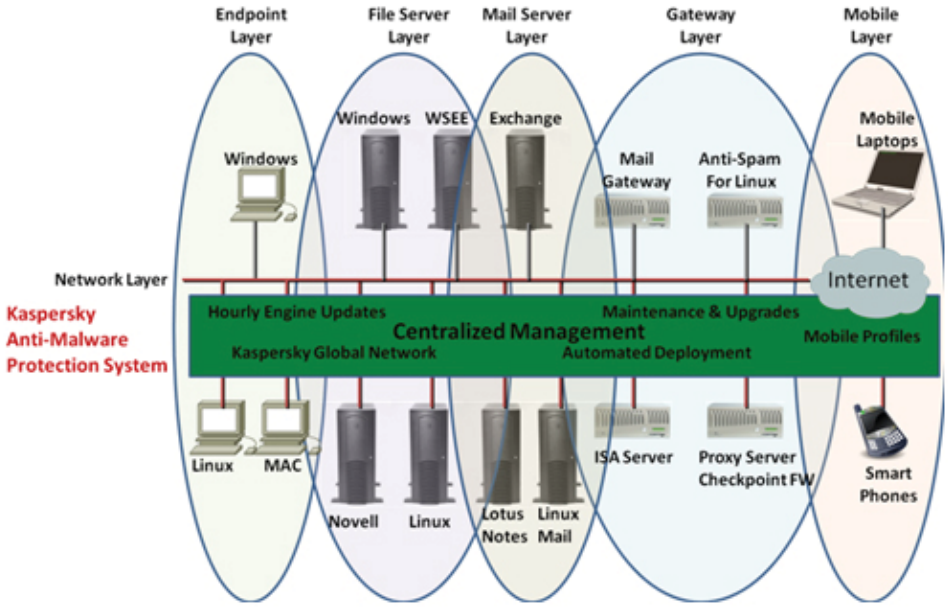


Keeping cybercrime at bay requires vigilance at every layer, not simply at the endpoint or the perimeter. The chart above illustrates the increased protection created by a layered malware protection strategy. While there is no such thing as 100% secure, from a holistic standpoint, layering security gets an organization as close to 100% protection as possible.

The question then is what is the best approach to delivered layered security throughout your organization? Loosely integrated layered security components create a disadvantage from the start. Solutions like these limit your visibility of the malware risks across the entire enterprise, making protection more difficult to manage and, ultimately, even more difficult to respond rapidly to threats as they appear.

The Kaspersky Anti-Malware Protection System is an award-winning, proprietary set of integrated protection technologies which form the backbone to the success of true layered malware protection. This Protection System extends from every endpoint (laptop, workstation, mobile device) to the cloud, and beyond, ensuring the best possible protection at every layer of the enterprise.

Each product within the system uses the identical proprietary, award-winning anti-malware technology, unifying best-of-breed protection across all network nodes. A centralized management console gives a complete view into any and all malware risks across the enterprise and allows for automated deployment, simplified maintenance and upgrading of protection system's components. All of these anti-malware components work seamlessly together to ensure the tightest end-to-end protection possible, as illustrated below.



Kaspersky's Anti-Malware Protection Layer provides the best protection value to businesses, with immediate visibility to all corners of the enterprise and a level of responsiveness not seen in other anti-malware approaches.

Premium Protection from Malware

Kaspersky Lab's strategy is to offer a unified set of products built upon a single, world-class anti-malware engine that extends across every layer of the enterprise, from the endpoint to the cloud. Ours is not a inadequately integrated set of disparate products requiring multiple agents and multiple management consoles. A single, proprietary, best of breed engine will power all of our technology solutions, workstation, laptop, smart mobile device, file server, mail server, gateway and into the cloud. Since 2009 and again in late 2010, Kaspersky has moved significantly closer to delivering a single core of premium anti-malware protection technologies to secure heterogeneous IT environments of all sizes.

- Kaspersky's single engine across the entire enterprise means the best protection available at every attack vector, ensuring premium malware protection.
- Kaspersky's single engine across all products simplifies management and updating, providing consistency at every layer of the enterprise.
- Kaspersky's anti-malware engine, due to its small footprint and minimal use of system resources, ensures the best in performance on all platforms across the enterprise.

Stanley Mierzwa, Director of IT Technology at The Population Council, has witnessed the difference Kaspersky makes when it come to protection:

"We immediately saw the impact of loading Kaspersky. We saw fewer infections which had a very positive operational impact, making our business much more efficient."

Superior Performance

Kaspersky consistently provides the highest levels of performance to ensure employees remain productive while they are protected. Kaspersky's Anti-Malware Protection System assists this high performance rate by providing constant signature updates. Some other anti-malware products update their signature database once per day. Kaspersky keeps its premium malware engine updated hourly, providing the most immediate protection available. This is extremely important for two reasons:

- More updates means smaller updates, minimizing impact on system resources and keeping your employees productive. With over 3,500 signatures being created each day, a single update can dramatically impact system performance.
- Faster updates means you are getting protection to you machine as it's available, not at the end of the day. Kaspersky updates 22 times per day, compared to 2 or 3 times per day or less from other systems, significantly reducing the window of exposure for our clients.

At Great Batch, Inc., Mike Ciura, Security and Oracle Analyst, immediately saw a difference when loading Kaspersky:

"Those using CAD and system-intensive products have had no problems. In many cases I have received compliments that it is faster and works in the background without bothering them."

Comprehensive Coverage

Kaspersky provides comprehensive coverage for heterogeneous, multi-platform environments. Our support includes all versions of Microsoft Windows endpoint and server products. Kaspersky also supports Novell networks, both legacy Netware, which many competitors have dropped, as well current Novell server products. Additionally, Kaspersky provides support for Linux and MAC operating systems which have grown in market share to the point that they are now a target for cybercrime. Kaspersky also supports email applications, both Microsoft Exchange and Lotus Notes. All of these environments are managed centrally, through a single management console with a single view.

The boundaries between consumer and corporate environments are blurring. Corporate users expect faster and easy access to their corporate network and business applications from any device. They are increasingly demanding smaller, more mobile devices or even consumer-grade devices, which they expect the IT organization to support. In addition, consumer social networking sites, such as Facebook and Twitter, have quickly moved into the enterprise environment, creating both a risk of data loss and a new channel for malware distribution. The growing number of mobile and remote users is creating a complex distributed workplace. The proliferation of consumer devices that can access and store corporate data presents clear dangers for firms that must comply with regulatory statutes and secure sensitive corporate data. In fact, Forrester's survey found that the adoption of smartphones and Web-based applications and services represent the two greatest concerns for IT security.

Support for several versions of smartphones is included in the Kaspersky portfolio, with additional smartphone coverage and support coming in the next year.

According to Jeff Smith, Manager of Computing Experience Services at the University of Northern Brunswick, the breadth of Kaspersky's product support made all the difference:

"Novell support was a key factor. Our current vendor did not support legacy Netware, though they claimed to support it. We also needed one solution for multiple endpoint OS's, including Windows, MAC and Linux."

Kaspersky truly provides the most comprehensive coverage for malware protection in these diverse IT environments.

Deployment Made Easy

Often customers realize they need better protection and performance in their environments but, due to the pain of changing anti-malware vendors, often decide not to change. This places them in the position of maintaining an inadequate security environment and accepting the risk to avoid the pain of change.

Kaspersky has dramatically reduced the pain of change by completely automating the process of removal, installation and configuration. Kaspersky's management "wizards", built into its management console, will automatically find all incompatible software, remove it, install Kaspersky, including the granular policy configuration. Then, with one configurable reboot at the end, the process is done. Remote installation has never been easier, making rollout in a complex, dispersed environment, a SNAP.

Tim Pemberton, Director of IT at Markham Stouffville Hospital, describes his Kaspersky deployment onto 1,200 systems in just two days this way:

"We deployed on the PC side first. With the help of our partner, the installation went surprisingly well. It was easier to upgrade to Kaspersky than to update to the newer version of our current vendor. It was a non-event!"

Simplified Management

Multiple agents and multiple management consoles can over-tax already strained resources and reduce the effectiveness of managing your overall anti-malware strategy. Kaspersky's vision is to minimize resource utilization and maximize malware risk management by providing a management console that manages every Kaspersky product, from the endpoint to the cloud, including remote and mobile devices. Our products are manageable from one central view, the Kaspersky Security Center. Regardless of platform, regardless of complexity, you have one view into your malware security to identify and mitigate malware risk.

George Thornton, Network Operations Manager of Montgomery Independent School District, experienced the "soft cost" savings Kaspersky Lab brings:

"Our previous vendor required multiple consoles. With Kaspersky, management is centralized on one console. It's nicely automated. We were spending one to two days per week managing our AV solution. Now we spend minutes per week."

World-Class Support

Because Kaspersky developed all technologies within The Kaspersky Anti-Malware Protection System, the company can provide the best in rapid response support. Kaspersky believes that support should be local, highly responsive, and exceptionally effective. All support teams are in-country, providing support in your language and understanding your local issues. Kaspersky has the shortest hold times in the industry, less than 5 minutes, reducing the time-to-resolution. Its support teams are highly trained resulting in over 90% first-call resolution. All of this means that you receive fast and effective support when you need it.

Victor Andreev, Systems Administrator for Centre for Education & Training, was having a different experience with his current vendor:

"Calling the vendor helpdesk was a nightmare. After holding forever, they would say they would call back but never did. When we called back we would get a new support technician that had no records of our previous call so we would have to go through the issues all over again. What really stood out was the support we received from Kaspersky. We had a few problems and had to call the Kaspersky Help Desk. Our experience was very good. The Help Desk had a great communications line to the development group and within a day we received the DLL's that solved our problem."

Minimized Total Cost of Protection (TCP)

Real protection, like that provided by the Kaspersky Anti-Malware Protection System, does not have to break your budget. Nor do you have to sacrifice performance and manageability. Earlier we described the buying considerations required to make sure that you are getting the best Total Cost of Protection. As you've heard from Kaspersky's customers above, the company has made every effort to provide the best overall Total Cost of Protection in the industry today, in every category:

- **Premium Malware Detection:** Kaspersky provides premium malware protection, dramatically reducing the Total Cost of Protection by minimizing the threat.
- **Superior Performance:** Kaspersky's proprietary technology dramatically reduces impact on system resources and system footprint, keeping employees productive while they are being protected. Poor performance can increase your cost of protection. Kaspersky minimizes performance impact, reducing your Total Cost of Protection.
- **Simplified Management:** Kaspersky's strategy is to have all products managed under one simple, intuitive yet powerful management console, reducing the time and resources required to manage even the largest enterprises, while providing the power to identify and manage risk across the entire enterprise, including remote and mobile devices. This dramatically reduces your Total Cost of Protection.
- **World-Class Support:** Kaspersky's standard support is free and comes with the shortest hold times in the industry, less than 5 minutes. Our first call resolution rates are over 90% meaning your problems are solved faster, with minimum time spent by IT resources. Kaspersky reduces the overall Total Cost of Protection by providing local, timely and effective standard support that is provided at no additional cost.
- **Competitive Pricing:** While Kaspersky provides the best Total Cost of Protection available, we do so at a very competitive price.

Organizations often equate value to price. As we've demonstrated above, the real value can be found in protecting the cost of the investment in security solutions by delivering real protection, performance that keeps you productive, management that reduces resource utilization and support that is fast and free. The Kaspersky Anti-Malware Protection System provides the best in malware protection while delivering the lowest Total Cost of Protection available today.

Kaspersky Lab – Always Ahead

Kaspersky Lab is planning for the future by continuously improving the performance and functionality of our products. We are also adding new features that aid in the protection and management of data so that we can provide a more holistic data protection strategy.
It is the core business of Kaspersky Lab to understand the key industry trends, the opportunities and risks they present, and to provide solutions not only to today's threats but also anticipating tomorrow's likely threats. Kaspersky Lab's virus laboratory, which stretches around the global with hundreds of virus research experts, is the core of up-to-the-minute expertise on developments in malware threats. This global network of international specialists provide constant input on regional developments and trends to ensure that the more than 300 million systems protected by Kaspersky remain always safe.

Kaspersky Lab's strategies to address key industry trends are as follows:

1. **A Move to Cloud Computing Models**
   - Kaspersky Security Network (KSN) Cloud-based detection benefits all Kaspersky Lab products today. Malware information is collected in the Kaspersky cloud from many millions of consumer installations. The virus laboratory creates malware signature updates for both Corporate and Consumer users as frequently as twice per hour based on this enormous cloud resource that is the companies eyes and ears into the immediate global threat landscape.
   - Kaspersky is launching Hosted Mail & Web e-mail filtering services where we provide companies with in-the-cloud anti-malware and anti-spam filtering before the traffic reaches client mail system.
   - Kaspersky is launching Managed Services where Kaspersky's Management Security Center resides on the Service Provider premises and manages security of their clients.
   - Future developments: Kaspersky's Endpoint 8.0 scheduled for late 2011 release will include the option to connect to the KSN cloud. KSN cloud detection/reputation will be added to future versions of Kaspersky's Messaging and Web products to block links, for instance, where malware resides, all in real time.

2. **A Move to Virtualization**
   - Kaspersky already has VMWare Ready certification for its key products. This is stage one, to enable anti-malware protection across Virtualized architectures.
     - There is no need to protect the VMWare Host OS (virtualization platform itself), in case of ESXi, as the hypervisor and host OS is tiny, monolithic, and digitally signed.
     - In the case of Hyper-V, the host OS is the standard Windows OS, so a Kaspersky anti-malware product would be installed on the host OS as well as on all guest machines. Kaspersky Lab's WSEE product supports Core mode (recommended by Microsoft for Hyper-V implementations) and provides perfect Hyper-V protection.
     - Microsoft Hyper-V compatibility tests are part of the Certified for Windows Server 2008 R2 logo certification program. Kaspersky Lab is planning to receive this logo for WSEE 8.0.
   - Kaspersky will create smart products aware of the Virtualized environment, i.e., Offline Image AV DB updates, Offline Image scans, Reporting, Interoperability with systems like VMWare (vCenter/ vSphere) and Microsoft System Center Virtual Machine Manager, Performance and intelligent load distribution, Virtual NAC and Virtual Appliances

3. **Kaspersky will increase attention to Data Loss Prevention (DLP)**
   - Kaspersky Lab plans to include advanced device control policies in its Endpoint product in 2011 to reduce risk of data loss via USB sticks, for example.
   - Kaspersky plans to launch Encryption data protection in 2011
   - Kaspersky Lab plans to add DLP functionality to its Microsoft Exchange protection product in 2011/12

4. **Kaspersky Lab will develop a new Endpoint Client, including:**
   - Vulnerability Assessment
   - Patch Management
   - Advanced Application Control
   - Advanced Device Control
   - Other technologies: Encryption, DLP, NAC, Cloud-based reputation services

5. **Kaspersky will develop additional technologies for mobile platforms**
   - Adding Blackberry and Android support in addition to Symbian, Windows Mobile.

6. Kaspersky will increase attention to Identity Access Management
   - The Kaspersky Lab Administration Kit reports not only by hostnames and IP addresses, but also with the domain\user information in virus detection events - which adds the "user" dimension. We plan to extend Kaspersky Lab Management Security Center to resolve logins to real names via integration with Microsoft Active Directory

Summary

Kaspersky truly provides premium malware protection, for today and tomorrow! Our Kaspersky Anti-Malware Protection Systems provides the best overall protection and performance for all businesses, small and large, and does so with the best Total Cost of Protection available today. Yet we aren't satisfied with protection for today's threats. We're planning for tomorrow, expanding our portfolio, and investing in technology that will protect customers from the threat of tomorrow.

That's Kaspersky Lab – Solid Business Protection Built the Right Way!

That's Kaspersky Lab –

Solid Business Protection Built the Right Way!

500 Unicorn Park
Woburn, MA 01801
866.563.3099
smbsales@kaspersky.com

www.kaspersky.com
www.threatpost.com

KASPERSKY lab