Everything connected is protected

Technical Whitepaper

kaspersky

#bringonthefuture

Contents

Protection where you need it — securing your move to the cloud 3

Digital transformation — changing the face of corporate IT 3

When your infrastructure is suddenly not on your network 3

A single pane of glass for all your workloads — Kaspersky Security Center 4

Compliance 4

Public clouds — visibility and convenience with Kaspersky Hybrid Cloud Security 4

Integration through APIs 4

Auto-discovery and rollout 4

Kaspersky Hybrid Cloud Security — enabling dynamic environments and agility 4

Auto-scaling groups support 4

Container security 4

Virtualization — balancing security and efficiency in the datacenter 5

Enabling secure digital transformation 6

Physical machines and mobile devices — Kaspersky Endpoint Security for Business 6

Increased productivity: reduced risk 6

Streamlining inventory and patching 6

Endpoint protection integration 6

Data security 6

Remote and mobile scenario support 6

Regulating access to sensitive data and recording devices 6

Stopping web threats before they reach your endpoints 7

Fending off spam 7

Best-of-breed protection — on-premises and in the cloud 7

Enabling secure digital transformation 7

PROTECTION WHERE YOU NEED IT — SECURING YOUR MOVE TO THE CLOUD

Digital Transformation — Changing the Face of Corporate It

As enterprises embrace digital transformation and build their infrastructures out into the cloud, there are some very real fights to be had. Can you retain control over your corporate assets — or will it be wrested from you? How will you close integration gaps and eliminate boundaries, so you can harvest the benefits of the move? And how can you minimize performance impact during these changes, while being sure you're maximizing the return on your substantial investment?

Digital transformation takes many forms. Building new IT functions in the cloud from scratch. Migrating existing servers or applications. Facilitating the de-commissioning of old hardware by moving over to the cloud. Enabling service auto-scaling, enabling fast-changing work-styles — and so on and so forth. The reality is that we have only just begun to tap into what cloud adoption may mean for us all.

In most cases, the ongoing process of evolving with and into the cloud results in an intermediate stage, comprising a complex heterogeneous hybrid infrastructure spanning physical, virtual and cloud platforms — something that needs to be managed, fine-tuned and supported, all at the same time.

There was a time when we, as our own network builders and owners, could run a discovery tool that would create an inventory of our workstations, servers, services and applications. And that was relatively easy, because we had control over our own network. We could trace a cable. We could dig into hypervisor settings to figure out the extent of our software-defined network. In the world of IaaS, we don't have that luxury any more — and this is a good thing. We can relax — the hardware layer is no longer our responsibility. It's up to the IaaS provider now.

When Your Infrastructure is Suddenly not on Your Network

With all that responsibility gone, control and, alas, visibility are gone also. The old way of doing things is still possible — you can VPN-stitch different parts of infrastructures together and treat your cloud IT-assets in almost the same way as you treat your virtualized workloads. But the thing is — more often than not you don't really want that, because each time you choose the old way over the new, you also decline the benefits of the new approach.

And here's a dilemma. Old tools don't work well with hybrid infrastructures. And the new tools focus on migration aspects, too often treating workload security as a post-migration issue. The only option for most of us is just to use different security tools for the different parts of the infrastructure. The result — the sprawl of domains of responsibility, visibility gaps, control failures and eventually those security gaps that cybercriminals love so much.

To enable digital evolution, the tools you use need to change and adapt to the new realities and function usefully across numerous platforms, wherever these may be — on premises, physical or virtualized, or 'in the cloud' — a term we've got so used to, but which for most people still means 'on someone else's computer'.

Here at Kaspersky Lab, we think about security gaps almost as much as about the threats that utilize them. Arguably, the inability to control, enforce policy and ensure configuration uniformity across all of your infrastructure is a bigger danger than a vulnerability in your operating system or line of business application. Vulnerabilities in software can be fixed by the software vendor or your security vendor. But who's going to spot a difference in settings on multiple security management consoles, that's created a convenient entry-point for an interested attacker?

A Single Pane of Glass For All Your Workloads — Kaspersky Security Center

We believe that a 'single pane of glass' management console best addresses this problem. When you can seamlessly control security for all physical, virtualized, mobile and cloud elements of your environment, the chances of human error leading to a security gap are so much lower.

Compliance

Compliance is an important requirement for every organization. Kaspersky Lab products enable compliance through multiple controls and features, such as:

- Management server hierarchy provides flexibility to support infrastructure complexity
- Different deployment options — on-premises or in the cloud
- Comprehensive and highly configurable reporting and log inspection to simplify audits
- Role-Based Access Control (RBAC) to ensure the segregation of control rights between different groups of administrators according to the organizational structure and IT policies
- Agent password protection and self-defense, to prevent security systems tampering
- Secure communications between all the components of the solution
- Encryption for the protection of data at rest
- System hardening — executable lock-down with Default Deny and the prevention of substitution attacks though File Integrity Monitoring (FIM)
- Device Control for the granular control of attached storage, camera, microphone and other hardware in use
- Configurable anti-malware protection and personal firewalls for enhanced server and workstation security

There are also features and mechanisms to ensure full visibility, sufficient granularity and high levels of control, as well as continuous improvement and adaptation to the risk landscape.

Public Clouds — Visibility and Convenience with Kaspersky Hybrid Cloud Security

Integration through APIs

Kaspersky Hybrid Cloud security simplifies orchestration for public cloud deployments, through things like:

- Native API integration with AWS and Microsoft Azure clouds
- Very straightforward cloud infrastructure inventory, and automated security provisioning of your AWS EC2 instances, regardless of their location
- Pay-Per-Use (PPU), enabling security procurement and billing directly through the cloud provider's marketplace

Auto-discovery and rollout

Integration with cloud APIs provides automation and administrative flexibility. The management console can see all the instances running under the specified accounts, and use that information to deploy security agents, as well as applying security policies to them. When a new instance is created, an IAM role or a script deployment mechanism can be used to ensure the instance is fully protected the moment it's created.

Kaspersky Hybrid Cloud Security — Enabling Dynamic Environments and Agility

Auto-scaling groups support

Configurable elasticity is an important cloud benefit. So the security solution used must be able to be able to respond to each instance that's automatically created and run by the cloud in response to the increasing load. Kaspersky Hybrid Cloud Security uses the integration with API and auto-scaling policies to ensure that every new instance in each auto-scaling group has security deployed to it, and conforms to the policy set by the organization.

Container security

One of the important use cases for public cloud is the enablement of DevOps[1]. But the adoption and wide (often loosely controlled) use of container technologies, such as Docker, creates a persistent challenge for security managers. We secure Docker and Windows Containers to prevent an attacker from using a vulnerable or malicious container component as a steppingstone into the organization's internals.

1 According to Gartner, by the year 2020, more than 50% of companies will use container technology, up from less than 20% in 2017.

Virtualization — Balancing Security and Efficiency in The Datacenter

While public clouds maybe be changing the fact of IT, on-premises virtualization and private clouds remain here to stay. Managing corporate risk means securing every Virtual Machine (VM) and virtualization storage, but while the goals for public and private clouds security are the same (reduce and manage cyber-risk), the challenges on the way are different.

Virtualization and public cloud technologies manage a lot of computing power on a dedicated set of hardware, and while hypervisor and virtualization orchestration tools maintain the required level of performance expected of VMs, the traditional approach to security tends to hamstring virtual systems performance. This 'security tax' on performance, as it's often known, can compromise your return on investment in virtualization. In short, you can only place so many VMs on a hardware server before they start competing for resources, and strangling each other in the process.

Effective virtualization security must find ways to centralize security tasks, reuse available information and eliminate redundancy, balance the load between VMs, and utilize the possibilities provided by virtualization platforms to maximize protection with the lowest possible performance impact.

Recognizing the importance of virtual systems security, and its unique features, VMware opened an API that enabled agentless file-level security mechanism for its vSphere virtualization platform.

This layer creates an integrated security space for third-party solutions, natively integrated with VMware APIs such as vShield Endpoint and NSX Guest Introspection, enveloping all virtualized assets and allowing easy and efficient access by appropriately designed security solutions. Only one Security Virtual Machine (SVM) — a specialized VM carrying an anti-malware scanning engine and signature databases — is needed per host, removing this burden from individual VMs and so greatly reducing resource consumption. The biggest benefit of this approach for enterprise businesses is smooth and native integration with the VMware ecosystem.

Another approach is an API-independent or, rather, a platform-independent solution, which utilizes a lightweight agent optimized to operate inside the OS of each VM being protected. With the file scanning engine and databases still held centrally on the SVM, 'light agent' technology delivers a dramatically smaller resource footprint than a traditional full agent solution. The solution sits between 'agentless' and traditional full agent solutions in terms of resource consumption, but is not tied to or limited by VMware technologies and can also be used on popular platforms, including Microsoft Hyper-V, Citrix Hypervisor and KVM.

These approaches allow efficient deployment of secure virtualization, and solve the issues of:

Excessive resource consumption

This is due to the replication of signature databases and active anti-malware engines on each protected VM. By centralizing most security tasks, we can balance the load and use a single instance of a database, as well as caching verdicts.

'Storms'

These result from simultaneous database updates and/or anti-malware scanning processes on each VM, leading to an avalanche-like increase in resource consumption, causing drastic loss of performance and even denial of service. Attempts to mitigate the problem by scheduling these processes generates 'vulnerability windows' — time periods when postponed malware scans leave the VM vulnerable to attack. Smart queueing, balancing and caching of verdicts on the SVM eliminate these storms.

'Instant-on gaps'

Databases and modules can't be updated on inactive VMs. So from the moment a VM starts up until the update process completes, the VM's vulnerable to attack. This is resolved by using an always-on always-updated SVM.

Incompatibilities

Because standard solutions aren't built to handle virtualization-specific features, like migrating VMs or non-persistent storage, their use can cause instabilities and even system lockups. Using a virtualization platform native API or our own patented Light-Agent technology solves the problem, allowing for easy VM control and life cycle management.

Enabling Secure Digital Transformation

Digital transformation is, by definition, a process, and should perhaps be seen as a continuous one, rather than a march towards a specific glorious end — arrival the shiny golden dawn of the digitally transformed business.

So your security needs to flex, in harness with your evolving IT systems — embracing change, moving adeptly into new spheres of operation, accompanying workloads beyond the corporate perimeter and into the cloud. You need security that promotes rather than impedes performance, and reduces rather than adds to complexity and costs. Seamless, centrally managed, all-encompassing and adaptive security for today's transforming hybrid environments is fully attainable. And pretty well essential, if IT Security professionals are to retain their sanity in the face of current business expectations.

Digital transformation produces a whole spectrum of new opportunities — for you, and for the cybercriminals targeting you. Make the very most of your own business opportunities, while firmly removing all those of your attackers, with Kaspersky Lab's integrated best-of-breed security solutions for hybrid environments.

Physical Machines and Mobile Devices — Kaspersky Endpoint Security For Business

Let's not forget however about physical servers and most importantly — physical workstations and mobile devices. Employees usually have a laptop or computer that they use for work while in the office or travelling, as well as a mobile device. An employee machine is arguable the easiest way for an attacker to circumvent corporate security. Not all employees are IT experts, and some social engineering attacks are so clever (and not necessarily complex!) that even an experienced security researcher might be tricked. So machines that assist us in our everyday activities must enable us work safely and focus on our responsibilities. Creating this safe environment is the role of Kaspersky Endpoint Security for Business.

Increased productivity: reduced risk

Specialized threat protection layers safeguard the user against the dangers of malicious websites and compromised 'watering hole' resources. Web Control filters which websites your end-users can access, increasing productivity while reducing the risk of webbased attacks such as drive-by infections.

Streamlining inventory and patching

Inventorying and managing the timely patching of vulnerabilities in hardware and software is tedious and time-consuming. Exploiting unpatched vulnerabilities is one of the most common ways for cybercriminals to attack IT infrastructures through a single endpoint. Automated vulnerability assessment and patch management goes well beyond simple remote deployment of new third-party software. Based on round-the-clock intelligence into exploited vulnerabilities, Kaspersky Vulnerability and Patch Management keeps potentially vulnerable software up to date, leaving your IT administrators with more time to spend on other tasks.

Endpoint protection integration

Customers and partners can natively integrate their systems with our security management console using a standardized application programming interface — OpenAPI.

Data security

User-transparent FIPS 140-2 certified encryption fully secures confidential data on portable devices and on-site. Integrated technology means you can centrally enforce the encryption of corporate data at file, disk or device level.

Remote and mobile scenario support

Data has become accessible anytime, travelling freely through the perimeter. Mobile security protects against threats specifically targeting data on the move, as well as against attempts to use weaknesses in the device as a springboard for subsequent infrastructure infiltration. Device Control guards against the consequences of data loss on unapproved or unencrypted portable devices, and the uploading of infected data from the device.

Regulating access to sensitive data and recording devices

Our solution restricts application privileges according to assigned trust levels, limiting access to resources like encrypted data. Working in step with our local and cloud (KSN) reputations database, a Host Intrusion Prevention System (HIPS) controls applications and restricts access to critical system resources, as well as to audio and video recording devices.

Stopping web threats before they reach your endpoints

By stopping the majority of incoming threats at gateway level, before they reach your endpoints, we significantly reduce the security impact of human weakness and workstation vulnerabilities.

Our security technologies filter traffic flowing through gateways, automatically blocking incoming threats before they reach your endpoints and servers. This significantly reduces the risk of vulnerability exploitation and considerably reduces operational overheads for IT security staff.

Fending off spam

Kaspersky Lab's cloud-assisted, next generation anti-spam detects even the most sophisticated, unknown spam with minimal loss of valuable communications due to false positives.

Best-Of-Breed Protection — On-premises and in the Cloud

The application of security to hybrid infrastructures, with so many different demands and considerations, and so many potential pitfalls, is a wide-ranging subject, and the best approaches to different scenarios are not always obvious, or uncontested.

One thing remains true, however. The same rule applies, whether your security is running on a mobile phone, a physical server, an SVM or in the cloud — it needs to be up to the job.

Best of breed protection is at the heart of all Kaspersky Lab products and services, protecting against the latest threats, including ransomware.

Based on unparalleled sources of real-time threat intelligence and machine learning, our technologies continually evolve to protect your endpoints from the latest exploits, keeping your data, and shared folders safe and secure from advanced threats and ransomware.

- Our Award-winning anti-malware engine, providing automatic, real-time file level protection for every computer, VM and workload — on-access and on-demand.
- Cloud-based Intelligence rapidly identifying new threats and providing automatic updates.
- Behavior Detection, monitoring applications and processes, protecting against advanced threats and even bodiless malware and rolling back any malicious changes if needed.
- Exploit Prevention, controlling systems operation processes and applications behavior, helping block advanced threats including ransomware.
- Anti-Ransomware, protecting cloud workloads and their shared networks against attacks, rolling back any affected files to their pre-encrypted state.
- HIPS / HIDS, detecting and preventing network-based intrusions into cloud-based assets.
- Application Controls, enabling you to lock down all your hybrid cloud workloads in Default Deny mode for optimum systems hardening, as well as dictating what applications can run where, and what they can access.
- Device Control, specifying which virtualized devices can access individual cloud workloads, while.
- Web Control protects against internet-based cyber threats.
- Network Segmentation, providing visibility and automated protection of hybrid cloud infrastructure networks.
- Vulnerability Shielding, preventing advanced malware and zero-day threats from exploiting unpatched vulnerabilities.
- Mail Security including Anti-Spam, protecting email traffic in cloud workloads.
- Web Security including Anti-Phishing, protecting against threats from potentially dangerous websites and scripts.
- File Integrity Monitoring, protecting critical and system files, while Log Inspection scans internal log files to ensure operational hygiene.

Enabling Secure Digital Transformation

Digital transformation is, by definition, a process, and should perhaps be seen as a continuous one, rather than a march towards a specific glorious end — arrival the shiny golden dawn of the digitally transformed business.

So your security needs to flex, in harness with your evolving IT systems — embracing change, moving adeptly into new spheres of operation, accompanying workloads beyond the corporate perimeter and into the cloud. You need security that promotes rather than impedes performance, and reduces rather than adds to complexity and costs. Seamless, centrally managed, all-encompassing and adaptive security for today's transforming hybrid environments is fully attainable. And pretty well essential, if IT Security professionals are to retain their sanity in the face of current business expectations.

Digital transformation produces a whole spectrum of new opportunities — for you, and for the cybercriminals targeting you. Make the very most of your own business opportunities, while firmly removing all those of your attackers, with Kaspersky Lab's integrated best-of-breed security solutions for hybrid environments.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/
Enterprise Cybersecurity: www.kaspersky.com/enterprise

www.kaspersky.com

kaspersky **BRING ON THE FUTURE**