Everything connected is protected

Unity, balance and total protection come from Kaspersky's perfect combination of esndpoint and hybrid security

kaspersky

#bringonthefuture

SECURITY SYNERGY FOR FEARLESS TRANSFORMATION

"You will never be transformed. You will always be transforming."

Forrester, The Sorry State of Digital Transformation in 2018

From Maverick To Mundane? New Trends Breathe New Life into Digital Transformation

The term 'digital transformation' has been so overused that it's gradually losing meaning and impact. Like all disruptive technologies or methodologies, digital transformation has travelled the same well-trodden arc, from maverick to mundane.

However, recent trends have emerged, breathing new life into the concept of digital transformation. In this paper, we've selected four to look at in turn, and addressed the threats they bring with them.

1. Instantaneous flexibility
2. Business Intelligence (BI) and analytics
3. Smart workplaces and the IoT
4. Intelligent automation

TREND #1: INSTANTANEOUS FLEXIBILITY

Instantaneous Flexibility – Threat Spotlight: Dangerous Security Gaps

One of the key limits to interoperability is the lack of alignment between security standards and capabilities offered by different vendors, or different solutions. Data may be as safe as houses in one solution, but become exposed while migrating (or after migrating) to another, which might operate according to a less rigorous security protocol. In this sense, the migration journey itself becomes as risky as a young bird leaving the nest for the first time: it's suddenly exposed, and at the mercy of the elements – including cyber-predators.

Protection, therefore, needs to be total and seamless, with an agnostic approach that secures all data, everywhere, no matter where it rests, or where it migrates to and from. Without it, businesses won't be able to migrate their data and processes freely, flexibly and proactively, in precise accordance with rapidly changing horizons. Their IT infrastructures will remain static, ponderous and inefficient; chained inexorably to the redundant world of yesterday.

"It's no longer about hardware or software — it's about delivering services that accomplish business needs. The future of infrastructure everywhere and anywhere, and will be business-driven by nature."

Gartner

Increased use of hybrid and multicloudarchitecture alongside on-premise solutions has accelerated thanks to improved interoperability between offerings from a wide range of vendors. This enhanced interoperability has led to a level of instantaneous flexibility that was unthinkable, even a few years ago.

Migration between the very many different components of contemporary IT infrastructures is now highly responsive and instant, with businesses leveraging the elasticity and instant scalability of the cloud to procure exactly what they need, as soon as they need it; and, later, to scale back if necessary, when requirements change.

Business optimization depends wholesale on having the power to implement the best possible configuration of IT resources, and to be able to change that at any moment, in response to a changing reality.

TREND #2: BUSINESS INTELLIGENCE AND ANALYTICS

Threat spotlight – Business Intelligence and analytics: data security stakes are raised

The more valuable your business' data becomes to you, the more attractive it is to cyber criminals. Knowing that BI is in wide use in companies across the globe is like a red flag to malicious actors, who may think: "Just by stealing or interfering with this data, I can cause this business to alter its course in a devastating way." This is compounded by the risk of internal actors (either through deliberate or accidental action), particularly in the context of BYOD (Bring Your Own Device), and ill thought-out data access policies. Sensitive data leaks or attacks can be catastrophic in any scenario; so much more so when such data forms the absolute bedrock of business optimization strategy.

To paraphrase Uncle Ben, with great digitization comes great data: the further your business progresses along the path of digital transformation, the more data you accrue. Storage challenges aside, the good news is that the more data your business holds, the more intelligence you can glean from it. This is where Business Intelligence applications come in. Rather than leave data riches lying 'fallow,' businesses now have access to software applications that automate the process of analytics to guide process optimization with an astounding level of acuity, based on solid facts about past events. According to Gartner, the worldwide BI and analytics market is set to grow to $22.8 billion by 2020.

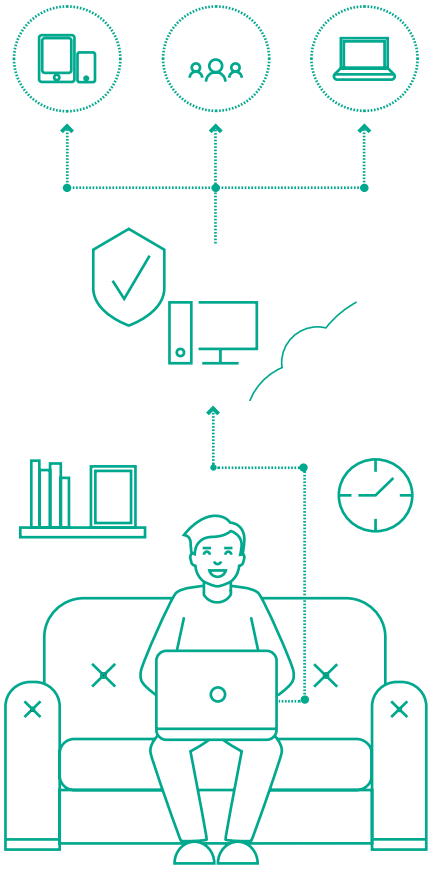
TREND #3: SMART WORKPLACES AND THE IOT

Threat spotlight – smart workplaces: the multiplication of attack interfaces

Smart workplaces, like all hyper-connected networked IoT systems, naturally entail a phenomenal multiplication in the number of possible attack interfaces. Businesses may yearn for the simple days when all they had to protectwere servers, endpoints and maybe a discretely used cloud resource or data center. Cybercriminals now have a huge menu of entry points at which to pitch their malicious attacks, including mobile devices, wearables, and a growing range of sensors and feedback systems. The movement towards Edge Computing, whereby data is processed close to where it's collected (i.e. the IoT sensors themselves), instead of centrally, makes this vulnerability even more acute.

Businesses now have to oversee multiple interdependences and large, increasingly complex attack surfaces which, if attacked, may create devastating cascade effects. And, while doing this, they must keep track of device software security, data encryption, and stay on top of maintenance (particularly for devices that rely on legacy systems), and – which is key – focus on eliminating the potential for human error that comes with entrusting staff with a wide range of connected devices.

A shocking 14 people a day died while working in the US in 2017 alone, with one in four of those deaths in the construction industry. Alongside traditional risk reduction strategies, companies are now turning to IoT technology (including wearables), to turn machine (factory and computer) generated data into actionable safety guidance, and prevent accidents and death. This is a rather stark way to open a discussion of the smart workplace trend, and its place in digital transformation, but it's important to understand just how direct the relationship between machine-generated data and the lived environment has become for enterprises. Office-based smart workplace technology (a somewhat lighter topic) incorporates IoT technology, alongside other digital innovations, to boost collaboration, productivity, flexibility, efficiency, facilities management, and human wellness. The goal, as ever, is to liberate staff from laborious and exhausting work, by automating the analytical processes that inform business process optimization.

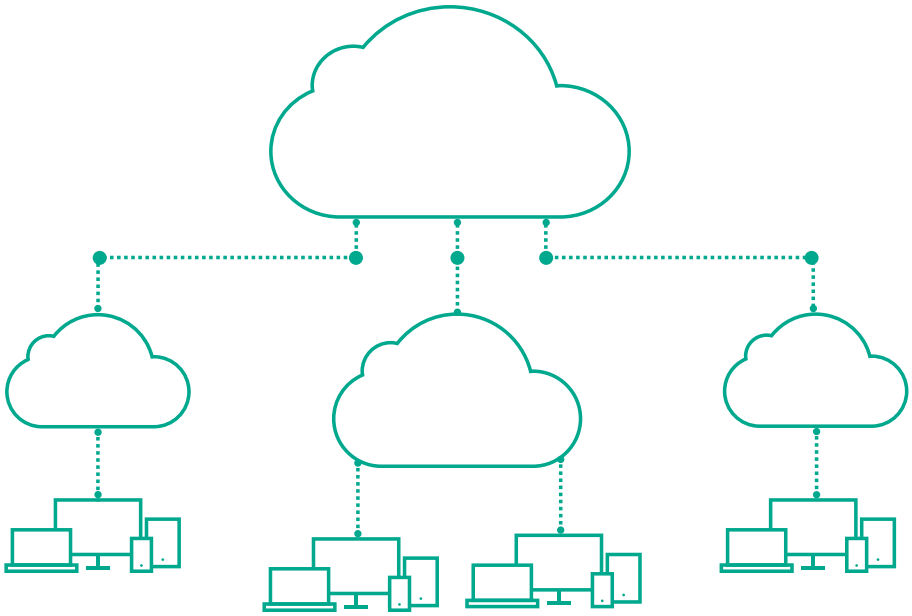


TREND #4: INTELLIGENT AUTOMATION

Threat spotlight – Intelligent Automation: who's the boss?

Technology that imbues digital connected systems with deep cognitive powers is risky enough but, in 2019, that's nothing new. Handing over the reins to those digital connected systems, however, brings risks to a frightening level. At some level, the removal of human error from the risk equation is compelling reason enough to adopt Intelligent Automation. Yet, even with Intelligent Automation, humans are still center stage: all technologies are only as good as the humans that code them, maintain them, control them, and make the right cybersecurity decisions to protect them.

According to Deloitte, Intelligent Automation is "the combination of artificial intelligence and automation — is already helping companies transcend conventional performance tradeoffs to achieve unprecedented levels of efficiency and quality." While Business Intelligence employs software to analyse data and guide process optimization, Intelligence Automation shoots direct to the action itself, by combining data, analytics, Machine Learning, and Artificial Intelligence, to put decisions into action automatically — guiding everything from driverless cars, to robots, drones, code, bots, key operational functions, and even healthcare.



"With a solid IT foundation in place, enterprises can forge ahead with new investments in next-generation resources like AI and machine learning."

Forbes

What Do Today's it Infrastructures Look Like?

Made up of a bespoke selection of on-premise, cloud (private and public) and endpoint solutions, todays IT infrastructures are pluralistic, diverse and multi-faceted. Every single element has unique properties, and comes with its own unique cybersecurity risk profile. Juggling these divergent characteristics can be exhausting, like fighting a war on infinite fronts, or trying to assemble an endless fiendish jigsaw puzzle. Even where a cloud and on-premise solution might work well together in theory, security concerns can interrupt migration, either because of doubt and fear, or because of well-founded risk awareness. This is because diversified IT infrastructures often suffer from the problem of fragmentation.

An IT infrastructure built from a diverse combination of (hybrid/multicloud) cloud and on-premise solutions should be far more than a simple collection of different tools. Configured correctly (and securely), the unique amalgamation of diverse solutions is a powerful digital entity in and of itself. This is the power of synergy, which the Oxford English Dictionary defines as **"The interaction or cooperation of two or more organizations, substances, or other agents to produce a combined effect greater than the sum of their separate effects."**

Synergy, and not digital transformation alone, is the goal for IT leaders today. Synergy can only be achieved when borderless orchestration and seamless interaction between infrastructure components is not only logistically possible, but procedurally secure. Only under these conditions can businesses profit from the full promise of flexibility, elasticity, availability, scalability, responsiveness, and automation that new technologies now offer.

OUR SOLUTION

It's a cliché to say that business is moving faster than ever; but process automation, optimization and migration within a diversified IT infrastructure mean that it's never been more true. We know that businesses don't want their staff wasting time fretting about how to secure a proliferation of new attack interfaces, and we also know that they don't want to deal with the frustrating roadblocks that clunky mismatched security tools can present.

That's why we worked hard to increase the synergistic power of Kaspersky Endpoint Security for Business Advanced with Kaspersky Hybrid Cloud Security; so that businesses can put optimization first, once and for all.

These two solutions combine to deliver total assurance **that every single component of your changing IT infrastructure is protected**, freeing you to forge ahead with new tech adoption without fear, and allowing migration to flow fast and securely under every conceivable condition. Above all, this formidable cybersecurity duo will bring stunningly efficient synergy to your IT infrastructure, so that everything works as it should, and all the constituent parts (from any and all vendors) chime together with the intensity and power of a world-class orchestra.

Our guiding principle is that security must partner with infrastructure, rather than building barriers. To protect your diversified infrastructure, two powerful solutions produce an end result that is greater than the sum of its parts. Here's how it works:

Kaspersky Hybrid Security Cloud provides outstanding multi-layered protection for multicloud environments. Wherever you process and store critical business data — in a private or public cloud, or both — we deliver a perfectly balanced combination of agile, continuous security and superior efficiency, protecting your data against the most advanced current and future threats without compromising on systems performance.

Kaspersky Endpoint Security for Business Advanced does far more than just protect every endpoint your business runs. Patch Management helps eliminate security vulnerabilities, while encryption helps to prevent data being accessed by cybercriminals, and Next Gen protection defends your business against known and unknown threats. The solution hardens endpoints, automates OS and software deployment tasks, reduces attack entry points and prevents the loss or theft of confidential business data.

These four scenarios exemplify the synergistic power of this formidable security duo:
Business #1 was restricting itself to on-premise storage and, in spite of an urgent need for availability and elasticity, fears about data leakage and privacy were holding back their expansion to the public cloud. By adopting Kaspersky Endpoint Security for Business and Kaspersky Hybrid Cloud Security, the business now has the confidence it needs to adapt its infrastructure and business processes to meet the new digital reality, and grow exponentially.

Business #2 was using a combination of public cloud and endpoint devices, and was anxious about the limits of the shared responsibility model, as well as the potential potential shortcomings of vendors' native security offerings. Already using Kaspersky Endpoint Security for Business, the company added the power of Kaspersky Hybrid Cloud Security to provide total peace of mind that their entire infrastructure was protected from the full range of threats.

Business #3 was beginning the process of migrating to the public cloud, with full awareness that the migration journey itself is replete with challenges, vulnerabilities and weak points. By adopting the synergistic power duo of Kaspersky Endpoint Security for Business with Kaspersky Hybrid Cloud Security, the company was able to prioritize business optimization without having to stress about data made vulnerable during migration.

Business #4 has achieved a high level of digital transformation maturity, and is benefiting from a perfectly bespoke and responsive configuration of on-premise, public and private cloud solutions. The synergistic power duo of Kaspersky Endpoint Security for Business and Kaspersky Hybrid Cloud Security has supported the company throughout its evolution, liberating IT staff from agonizing over security risks, and enabling them to focus on business optimization alone.

CYBERSECURITY SYNERGY: We've engineered these two powerful cybersecurity solutions so that they work together flawlessly, resulting in total, utter, complete, comprehensive and synergistic protection for your entire IT infrastructure, no matter what the future holds.

By engaging this power duo, you won't have to give security a second thought. Whatever technology you adopt, whichever software or endpoint vendors you trust, and however and wherever you migrate data to and from, you'll know it's safe. The best part is that everything is controlled from one unified intuitive web-based console.

Total control, total security, totally at your fingertips.

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**