# CA Technologies Virtualization Security

## Vendor Report



Author: Martin Kuppinger

## 1 Executive Summary

Virtualization Security is not a single product category but comprises several different types of solutions from different categories, including IAM (Identity and Access Management), information protection, service automation, service assurance, service management, as well as system security solutions for hardening and monitoring resources. In order to be effective, Virtualization Security has to be well planned and requires a set of well-integrated products to provide the right balance between security and risk mitigation on one hand, and costs and complexity on the other.

CA Technologies offers a broad range of products which support customers in implementing Virtualization Security. CA Technologies specific strengths are not only that core security is provided but also IT service automation, assurance, management and other areas are covered as well. Furthermore, CA Technologies has clearly understood that Virtualization Security is not just about having yet another security tool but it is actually about enhancing the existing technologies and enabling them to seamlessly manage heterogeneous physical and virtual environments – in private and public environments ("clouds"). A specific strength for CA Technologies is what they call content-aware IAM, which is about enhancing the scope of IAM to extend to information protection and control through integrating IAM and DLP (Data Leakage Prevention) domains, thus ensuring that information access is well managed at any point of time.

To manage the complexity of virtualized environments and add Virtualization Security to these environments, the most effective approach is to reduce the number of vendors you rely upon and build on a strong portfolio of one vendor, which is able to integrate with your existing solutions and support your various heterogeneous environments. There are few companies out there which are able to cover all facets of virtualization in general and Virtualization Security in particular. From the KuppingerCole perspective, CA Technologies is extremely well positioned in this market not only from the product portfolio but also from the strategic perspective. CA Technologies provides a clear strategy encompassing the data center with physical and mainframe servers as well as virtualized environments and all facets of the Cloud – private, hybrid, public. CA Technologies product management process is clearly focused on enhancing the capabilities to support all of these environments. And with their acquisition of 4Base, a virtualization and cloud infrastructure consulting firm, CA Technologies is aiming to make it faster, easier, and cheaper to deploy and run their virtualization management and security solutions at customer sites. Because of this, CA Technologies is clearly amongst the leaders in the market of Virtualization Security.

CA Technologies existing portfolio covers all major challenges of Virtualization Security. Therefore we strongly recommend evaluating the CA Technologies solution portfolio when it comes to Virtualization Security. That portfolio has a strong potential to become the cornerstone of your future-proof Virtualization Security environment.



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

## 2 Core Findings Based on the Analysis

- ↗ Comprehensive portfolio of products for Virtualization Security.
- ↗ Seamless support for physical and virtualized environments.
- ↗ Content-aware IAM approach provides enhanced information protection and control for data moving around in virtualized environments.
- ↗ Strong PxM (Privileged User Management) solution, a cornerstone product for Virtualization Security.
- ↗ Supports not only security, but also service automation, assurance, and management.
- ↗ Strong vendor strategy of moving forward to enhanced virtualization and cloud support – for security and management.
- ↗ Strong professional services and partner ecosystem to support customers in implementing Virtualization Security.
- ➔ Virtualization Security requires (per se) the use of different products. Even solutions from a single vendor will require technical integration.
- ➔ The amount of conceptual work for well-planned virtualization security should not be underestimated - however CA Technologies and its partners can assist in defining these concepts.

## 3 Product Category

Virtualization Security is not a single product category but comprises several different types of solutions from different categories, including IAM (Identity and Access Management), information protection, service automation, service assurance, service management, as well as system security solutions for hardening and monitoring resources. In order to be effective, Virtualization Security has to be well planned and requires a set of well-integrated products to provide the right balance between security and risk mitigation on one hand, and costs and complexity on the other.

KuppingerCole currently is observing several approaches for addressing the needs for Virtualization Security. Point solutions provided by either startups or virtualization vendors which are focusing on some aspects of virtualization only are one of them. However, these approaches are by nature limited when it comes to a seamless, consistent management of both physical and virtual infrastructures. Nevertheless they might become an add-on within Virtualization Security strategies. From the KuppingerCole perspective, the other two approaches better suit the needs of organizations. One is the extension of security tools to support both types of environments, the other is the inclusion of virtualization security in overall IT and service management tools. In any case, KuppingerCole recommends using tools that support heterogeneous virtual and physical environments to avoid vendor lock-in.

The need to look specifically at Virtualization Security has increased with server and storage virtualization becoming standard technologies in today's data centers. These types of virtualization are a key enabler of a flexible IT environment and provide the foundation for private and public Cloud Computing approaches.

However, virtualization imposes new risks. First of all, there are more layers at a physical server and thus there is a larger attack surface. Instead of each physical machine having one operating system, in the virtualized environment a physical machine supports multiple guest operating systems controlled through a hypervisor. Moreover, the guest operating systems may be of different types with significant differences in their security requirements.



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

## Security Challenges in Virtualized Environments

Virtualization provides some security benefits as well as security challenges. Locating each application in its own virtual machine (VM) increases isolation and so reduces the risk of a security problem spreading. The ease with which a new VM can be set up by cloning makes it easier to standardize on a secure configuration and keep up to date with security related patches. However the ease with which VMs can be rolled out has led to the problems of 'sprawl'.

There are several specific security challenges in virtualized environments. There are also some security challenges which are more complex to deal with in virtualized environments than in physical ones. The most important virtualization-specific challenges might be named Virtual Entitlement Sprawl, VM Sprawl, and Data Sprawl. A further minor issue is that all security aspects which rely on specifics of physical systems like MAC addresses have to be changed to support the virtual environments.

Within the three types of sprawls, the VM sprawl is probably the most prominent one today. Smaller, disparate workloads lead to a situation where the number of virtual servers increases significantly. That makes sense – small workloads are easier to distribute and physical resources can be used optimally. However, there is the risk of non-standardized configurations as well as of an uncontrolled growth of such virtual machines which aren't required, together with the difficulty of controlling where the VMs are located. Organizations might end up with availability issues due to resource choking and other issues. However, from a security perspective the main issues are the security risks related to non-standardized configurations. Beyond that, VMs might be reverted back using snapshots, losing the current security settings. That adds to the risks around VM sprawl.

The issue of data sprawl is also widely discussed. Depending on the virtualization approach, data might move – and some data, which is local to the VM, always will. Therefore it is much harder to manage that data. That is an issue from a backup perspective, and also with respect to access control. As virtualization becomes the de facto platform and server workloads become more mobile, traditional perimeter security cannot offer enough information protection. The need to take an identity centric approach to information protection becomes paramount to enable a more collaborative environment that fosters information sharing while protecting the business from unnecessary risk.

From a KuppingerCole perspective the biggest issue is around virtual entitlement sprawl. There are several issues around this. The large numbers of VMs each have identity stores that need to be managed and the sheer scale makes centralizing this management essential. Hypervisors introduce a new privileged layer which needs to be managed. The hypervisor has direct access to the host system resources it can manage; and, for example, this makes it possible for the Hypervisor administrator to copy/clone virtual machines and to "misplace" the copy which can be installed elsewhere. There is a clear lack of SoD (Segregation of Duties) as well as well-defined, granular role management for users of the hypervisor. In fact, there is a lack of privileged access management especially with respect to the multi-layered environments with host, hypervisor, and guests.

Furthermore, there are issues with auditing these environments – monitoring and auditing the more complex environments is obviously a bigger task than it was previously in the physical environments. The privileged users: hypervisor administrator and OS administrators are fixed accounts and hence it is difficult to know which person performed which action that has been logged. The privileged users are also able to cover up their activities by starting and stopping monitoring processes and changing log files.

In addition, there is no fixed relation between the physical server, the logical instances of operating systems and applications, and the storage anymore. Applications might run on different servers at different points of time. Data might as well become stored in different locations, depending on the chosen approaches for server and storage virtualization.



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

Therefore, IT security needs to be enhanced to support these new types of environments and to address the additional and specific requirements they impose. That is where the field of *Virtualization Security* is –it is about integrating different types of security solutions to deliver on the benefits of virtualization in a secure manner.

It is important to note that Virtualization Security is not just about technology. It is about IT organization and IT processes as well. Virtualization Security requires enterprises to revisit their existing security guidelines, organizations, and processes and to adopt them in the new infrastructure. Ideally, security has to work the same for physical as for virtual environments and a primary target of implementing Virtualization Security is to support a consistent, seamless security approach across the entire IT environment.

From the process perspective, IT automation becomes the key. Managing the virtualized environments makes automation a must for virtualization. The increasing number of virtual machines with their disparate workloads all need to be created and managed in a standardized way to efficiently achieve consistency and robustness. Doing IT automation correctly is a cornerstone of Virtualization Security – for example: standardized configurations are a simple approach for consistent hardening and should form part of any risk mitigation approach.

Having said this it becomes obvious that Virtualization Security, as stated at the beginning, requires a set of technologies which all deliver enhanced security in virtualized environments:

- Identity and Access Management: Privileged User Management, Identity and Access Management including role management and SoD policies, access management to web-based and other management tools and other functionalities are part of Virtualization Security.
- Information/Data/System Security: Features like Data Leakage Prevention to mitigate the effects of data sprawl and distributed endpoint security are also necessary.
- Threat Management: To monitor and protect the complex, distributed virtualized environments against malware and mobile code.
- Service Automation/Assurance/Management: Provide the foundation for the efficient management of virtualized environments– for example with focus on standardized configuration and the hardening of system environments.

This report focuses on the security technologies and how they can help in Virtualization Security but it will also briefly cover other products in the field of virtualization as well as IT service automation, assurance, and management.

# 4 Product Descriptions

CA Technologies offers a broad range of products which help customers to implement Virtualization Security. CA Technologies specific strengths are not only in core security but also in IT service automation, assurance, and management, as well as other areas. Furthermore, CA Technologies has clearly understood that Virtualization Security is not just about having yet another security tool but that it is about enhancing the existing technologies and enabling them to seamlessly manage physical and virtual environments – in private and public environments ("clouds").

From a strategy aspect, it is interesting to observe that CA Technologies believes that to secure virtualization and cloud computing efforts, organizations need to adopt an identity-centric and content-aware security strategy from the very start. Content-aware IAM helps organizations to strengthen and automate their security controls by not only enabling them to control user identities and their access, but also managing their information usage Traditional IAM stops at the point of access of applications



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

and systems, being system-focused instead of information-focused. Content-aware IAM goes beyond this by providing management and control starting at the user all the way to the information and how it is used, for example by integrating IAM and DLP (Data Leakage Prevention). Thus it adds a level of functionality and another perspective to security – focusing on the information and not (only) the technology. This granular control helps prevent misuse of data, including improper disclosure or theft from the organization and thus adds to fulfilling compliance requirements and information protection across physical, virtual and cloud environments. It also enables the fine-grain controls of DLP to become user-centric instead of generic.

This section focuses on the core products of CA Technologies from the areas of IAM (Identity and Access Management) and IT Security in general. Other products are briefly covered in the later section. Within the CA Technologies portfolio, the solutions covered here are part of the *IT Security Solutions*. Virtualization Security is supported by different solutions within the IT Security Solutions part of the CA Technologies portfolio, e.g.

- Secure Identity
- Secure Access
- Secure Information
- Threat Management

This demonstrates that Virtualization Security is primarily about strategically expanding the existing IT Security portfolio – not about reinventing IT Security.

## 4.1 IAM-related products

As stated above, there are several products within the CA Technologies portfolio which play an important role in Virtualization Security. The most important one, from the KuppingerCole perspective, is CA Technologies Access Control, a leading-edge solution in the field of PxM (Privileged User/Identity/Access Management). But there are several other important tools as well. The following descriptions are listed in order of the relevance these tools have, from a KuppingerCole perspective, within an enterprise approach for Virtualization Security:

- CA Access Control: Privileged users and their access are even more critical in virtualized environments. Whilst the privileged users within a VM are comparable to what we have in physical server environments, privileged users at the host and hypervisor layer have control over all VMs and the applications and data residing on said VMs. There is a good reason that PxM is already a core issue for auditors– and it is even more important when it comes to virtualization. Unfortunately, the granularity of control provided by management tools for the hypervisors is typically very limited, and so the challenge isn't addressed. Advanced technologies for PxM are required to restrict administrative access to what is needed and to implement SoD rules for administrative access. CA Access Control is a leading-edge product in the PxM market, providing a broad set of features for physical as well as for virtualized environments. It supports a wide range of different environments, from Windows and UNIX/Linux up to mainframe environments. Therefore it can be effective to limit privileged access not only at the host level but also in the increasing number of VMs typically found in virtualized environments. Worth noting that CA Technologies has also made available a cut-down version of CA Access Control called CA VPM (Virtual Privileged Manager).



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

This product was specifically built to provide PxM capabilities for virtualized-only environments, but also offer an easy upgrade path to the full CA Access Control version, in case a customer needs to extend the PxM capabilities to physical environments in the future. From the KuppingerCole perspective, controlling privileged access is one of the mandatory cornerstones of Virtualization Security.

- CA Identity Manager: With an increasing number of separate virtual machines, the need grows to manage users, including administrators and operators. Identities, their lifecycle and their access privileges have to be managed across a large number of systems. More complex relationships with managed service providers when moving from private to hybrid and public cloud environments add to the challenge. Advanced Identity Lifecycle Management and management of acess controls is mandatory to efficiently keep all identities (beyond the privileged ones) and their privileges under control across all the servers and VMs, regardless of where they are running. CA Identity Manager is amongst the leading-edge solutions in the area of Identity Lifecycle Management and provisioning and thus provides support for the implementation of Virtualization Security concepts.
- CA SiteMinder: Another interesting field with respect to Virtualization Security is Web Access Management (WAM). On one hand, WAM benefits from virtualized environments due to the improved scalability they provide. On the other hand, WAM plays an important role in securing applications in virtualized environments – web applications as well as other applications which are integrated with WAM tools using their specific APIs. WAM can play an important role as a centralized access management layer for distributed applications, regardless of where the VM is currently running. Beyond that - and from a Kuppinger Cole perspective, the most important aspect – WAM is essential to secure the virtualization management tools (which are commonly web applications). Given that these tools typically have a very limited security model, WAM enables organizations to build an additional security layer around these tools and thus mitigate risks. CA SiteMinder is the market leading product in the area of WAM and provides a very broad feature set to support the specific requirements of Virtualization Security as far as WAM is concerned.
- WebFort and RiskFort: These are additions to the CA Technologies portfolio from the recent Arcot acquisition. RiskFort provides strong, context-sensitive authentication and RiskFort detects and blocks suspicious behavior in real-time. These technologies can be used to better control and manage privileged access to virtualized environments, as well as for securing remote access to any type of virtualized environment.
- CA Role & Compliance Manager: Finally the CA Role & Compliance Manager can assist in the construction of roles, SoD policies and Compliance Management in combination with the other tools mentioned above. Again, CA provides a leading-edge solution in that field with a particular strength in role construction and management.

A key point to note is that there are no elements missing from that portfolio – CA Technologies provides a comprehensive set of solutions to address the Virtualization Security challenges from an IAM point-of-view. In addition to the tools mentioned above, other solutions like CA Federation Manager and CA SOA Security Manager are important when it comes to developing optimized solutions for virtualized environments – these tools are key elements for supporting distributed security concepts.



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

## 4.2 Other security-related products

Managing the identities and access, especially (but not only) of privileged users is one important part. But Virtualization Security goes well beyond that – think about data being on many more (virtual) servers than before – and thinks also about the increased attack surface of a virtualized server.

Virtualization Security requires additional elements and CA Technologies provides several important tools to support these requirements. These are, in the order of importance:

- CA DLP: DLP (Data Loss/Leakage Prevention) becomes more important when the number of servers grows and more administrators and operators for different types of systems are involved. The risk of data loss increases as the data becomes more distributed and potentially more people have access to it. Using DLP solutions to enforce consistent policies for data protection adds to the security of virtualized environments. CA Technologies supports this with its CA DLP product, a comprehensive solution in the field of DLP. Notably, the DLP product is fully integrated with the IAM solutions. At the time of writing this report, CA Technologies is the only vendor in the market providing that type of integrated portfolio.
- CA Enterprise Log Manager: As mentioned above, auditing becomes more complex in virtualized environments. Applications are running on different physical machines and in many cases the number of instances of an application increases significantly. Also worth mentioning is that log files are widely distributed across multiple systems. The life of most VMs is much shorter than of their physical counterparts. And as VMs comes online and goes offline possibly after a few minutes, organizations naturally need to keep track of the logs of these VMs after going offline again. Enterprise Log Management, which aggregates log information from different servers and provides analytics and actions based on these logs, is therefore a critical element of Virtualization Security. For this, CA Technologies provides CA Enterprise Log Manager, which delivers the full set of features required to manage logs centrally in distributed, virtualized environments.
- CA Total Defense: Finally, CA Total Defense as an endpoint security solution also adds to Virtualization Security by better protecting the multitude of servers.

Combined with the other solutions, CA Technologies can cover the challenges of Virtualization Security with a comprehensive and well integrated portfolio of products.

# 5 Additional products and solutions

Above and beyond the IAM and Security related products, CA Technologies is one of the market leaders in IT Service and Systems Management, covering all aspects from service automation to service assurance and service management.

From the KuppingerCole perspective, covering this area is a key success factor for the successful migration of data centers from physical environments to virtualized environments and further to private and hybrid cloud infrastructures.

CA Technologies IT management solutions include:

- CA Service Automation plays a key role in enhancing security in virtualized environments by ensuring that systems are configured consistently and according to centralized policies. For example, through the integration of CA Access Control with CA Spectrum Automation Manag-



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

er, administrators can control VM sprawl and automate the deployment of privileged user policies in their environments: when a VM comes online, it is automatically detected by CA Spectrum Automation Manager and joined to a "host group" in CA Access Control, which automatically applies a policy based on the attributes of the host group. When the VM moves from QA (Quality Assurance) to a Production environment, the policy is automatically changed by CA Access Control so that QA personnel cannot log into the VM.

- CA Service Assurance helps by identifying performance and availability issues in virtualized environments and thus complements enterprise log management and other monitoring approaches. Incidents can be related to security issues, thus adding to the capabilities for successfully managing a secure virtualized IT infrastructure. Service assurance is also essential to improve performance management and capacity planning for the security infrastructure itself. The security infrastructure is a business critical infrastructure (think about web access management and log management) and thus performance has to be maintained at optimum levels. This becomes particularly critical in virtual and cloud environments.
- Finally, CA Service Management is a key technology especially when it comes to private clouds. Cloud Computing is in fact a service-oriented approach – it is about being able to consume the most appropriate services from different clouds and thus, from the internal perspective, to produce these services efficiently. Thus, virtualization and service management are tightly related. Again, from a security perspective, service management is highly important – think about change and configuration management to ensure consistent, well-planned management of the services which are provided by virtualized IT infrastructures. Service Management is also important to:
  - Achieve higher levels of security automation through self-service capabilities (e.g., Service Catalog) – an essential component for building a cloud-enabled data center.
  - Improve the value of security by utilizing a pay-as-you-go model through service accounting (also another essential component for building a cloud-enabled data center).
  - Better align security with the business requirement through service level management.

And in order to make some of these management solutions more easily accessible to organizations adopting virtualization and cloud computing, CA Technologies has introduced CA Virtual, a portfolio of products to manage heterogeneous virtualized-only environments. And to protect virtualization management investments in the long run, these products are designed to easily provide on-ramps into physical plus virtual management if needed.

In short, with its leading-edge portfolio fully covering all these areas, CA Technologies is well positioned to provide an integrated approach to virtualize and cloud-enable data centers with Virtualization Security in mind.

# 6 Services

To successfully make the transition from a physical environment to Virtualization Security requires rethinking existing security concepts and expanding the IAM, security, and management solutions in place. To make this transition, careful planning and preparation is required.

CA Technologies can provide support for this through its own professional services as well as its partners. Given that CA Technologies has a long experience in the different technical solution areas involved in Virtualization Security, and especially with the acquisition of 4Base the company appears to be well positioned to support customers in moving forward to secure virtualized and cloud-enabled environments.



KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon

# 7 Kuppinger Cole's Conclusion

When looking at Virtualization Security, it becomes obvious that it is not about a single tool but about a set of solutions which have to work together and be integrated to provide the required level of security in what is a significantly more complex IT environment. Virtualization Security will typically be implemented based on existing tools plus solutions which haven't yet been implemented – or have only been implemented as non-strategic point solutions, as is often the case with PxM. To manage the complexity of virtualized environments and add Virtualization Security, it is mandatory to reduce the number of vendors and exploit the strong portfolio of one vendor, which can integrate with your existing solutions.

There are few companies out there which are capable of covering all facets of virtualization in general and Virtualization Security in particular. From the KuppingerCole perspective, CA Technologies with its content-aware IAM approach is extremely well positioned in this market not only in terms of the product portfolio but also from the strategic perspective. CA Technologies provides a clear strategy, whether it's for the data center with physical and mainframe servers or virtualized environments and all facets of the cloud – private, hybrid, public. CA Technologies product management process is clearly focused on enhancing the capabilities to support all of these environments. Because of this, CA Technologies is clearly amongst the leaders in the market of Virtualization Security.

The existing portfolio covers all major challenges of Virtualization Security. Therefore we recommend evaluating the CA Technologies solution portfolio when it comes to Virtualization Security. That portfolio has a strong potential to become the cornerstone of your future-proof Virtualization Security environment.





KuppingerCole Arnheimer Str. 46 40489 Duesseldorf
Tel. +49 211/2370770 Fax +49 211/23707711 service@kuppingercole.com www.kuppingercole.com
Martin Kuppinger, Tim Cole, Jörg Resch, Dr. Horst Walther, Sebastian Rohr, Felix Gaehtgens, Prof. Dr. Sachar Paulus
Düsseldorf – Stuttgart – München – Darmstadt – Hamburg – Lissabon