Author: Paul Fisher

KuppingerCole ANALYSTS

Buyer's Compass

Identity Threat Detection and Response

ACALVIO AI-POWERED DECEPTION

Chapter 1

The Challenge

Identity-driven attacks are escalating, driven by the dissolution of traditional network perimeters due to cloud adoption, remote work, and the increasingly sophisticated tactics of adversaries. Over 80% of breaches involve compromised identities, as attackers leverage methods like Kerberoasting, password spraying, and the exploitation of misconfigurations in identity systems such as Active Directory. Traditional security measures are proving inadequate in differentiating between legitimate and malicious use of identities, leaving significant vulnerabilities.

The insidious nature of identity-based attacks is that the attacker can parade around your infrastructure using legitimate, highly trusted levels of authentication and encryption to commit crimes without any fear of being noticed. They're not the proverbial wolf in sheep's clothing—they manipulate the sheep, instead.

This dynamic is completely uprooting our current models for threat detection and response. To deal with this type of threat, a new runbook must be written. As an industry, we're still very early on in that process; but for the moment, we're cautiously referring to this new practice as Identity Threat Detection and Response (ITDR). But its arrival has posed some questions, such as who is responsible for this new tool.

The growing tension between identity and access management (IAM) and security operations center (SOC) teams further complicates the landscape. SOC teams handle threat detection and response, while IAM teams focus on managing digital identities, resulting in silos that inhibit effective identity threat response. This disconnect must be bridged to effectively defend against identity-driven threats, requiring a convergent approach.

The five pillars in the image below illustrate how neither IT administration nor SOC teams have control over the entire process, but that visibility is broadly available.

These pillars support activities that range from administration of identity systems (on the left) to shared responsibilities in the center, then SOC-related responsibilities to the right. Given that administration and SOC teams need to collaborate on this process, tools that provide integrated views will improve the success of ITDR projects.

Challenges

Identities can be stolen from identity repositories (such as Active Directory) or endpoints/workloads where identities are cached. Identities can also be unintentionally leaked in code repositories, log files etc.

These challenges highlight the complexity of managing and protecting digital identities, requiring ITDR solutions that are not only innovative but also comprehensive, interoperable and scalable for effective defense.

Complex Integration Across IAM and SOC
Bridging the gap between Identity and Access Management (IAM) and Security Operations Center (SOC) teams is difficult due to the differing focus and tools used by each. Effective

Protecting Identities both in the Identity Repositories (AD, IAM) and endpoints/workloads
Attacks can compromise identities in AD/cloud IAM repositories or steal cached identities across the network endpoints. Protecting only AD/IAM is only part of a comprehensive ITDR solution. Even with MFA enabled, identities cached on endpoints are valid for a certain duration. In addition, service accounts may not have MFA enabled. Many applications and browsers provide the ability to cache credentials. Identities / secrets are also cached in cloud and Kubernetes secret managers. Leaked secrets in configuration files, logs, code repositories are routinely used to compromise cloud workloads.

ITDR solutions should be comprehensive, covering identity repositories and identity caches, both on-premises and in cloud workloads.

Differentiating Legitimate vs. Malicious Identity Use
Accurately distinguishing between legitimate user activities and malicious behavior remains challenging, as attackers often exploit valid credentials. ITDR solutions need to be sophisticated enough to detect subtle anomalies without generating excessive false positives.

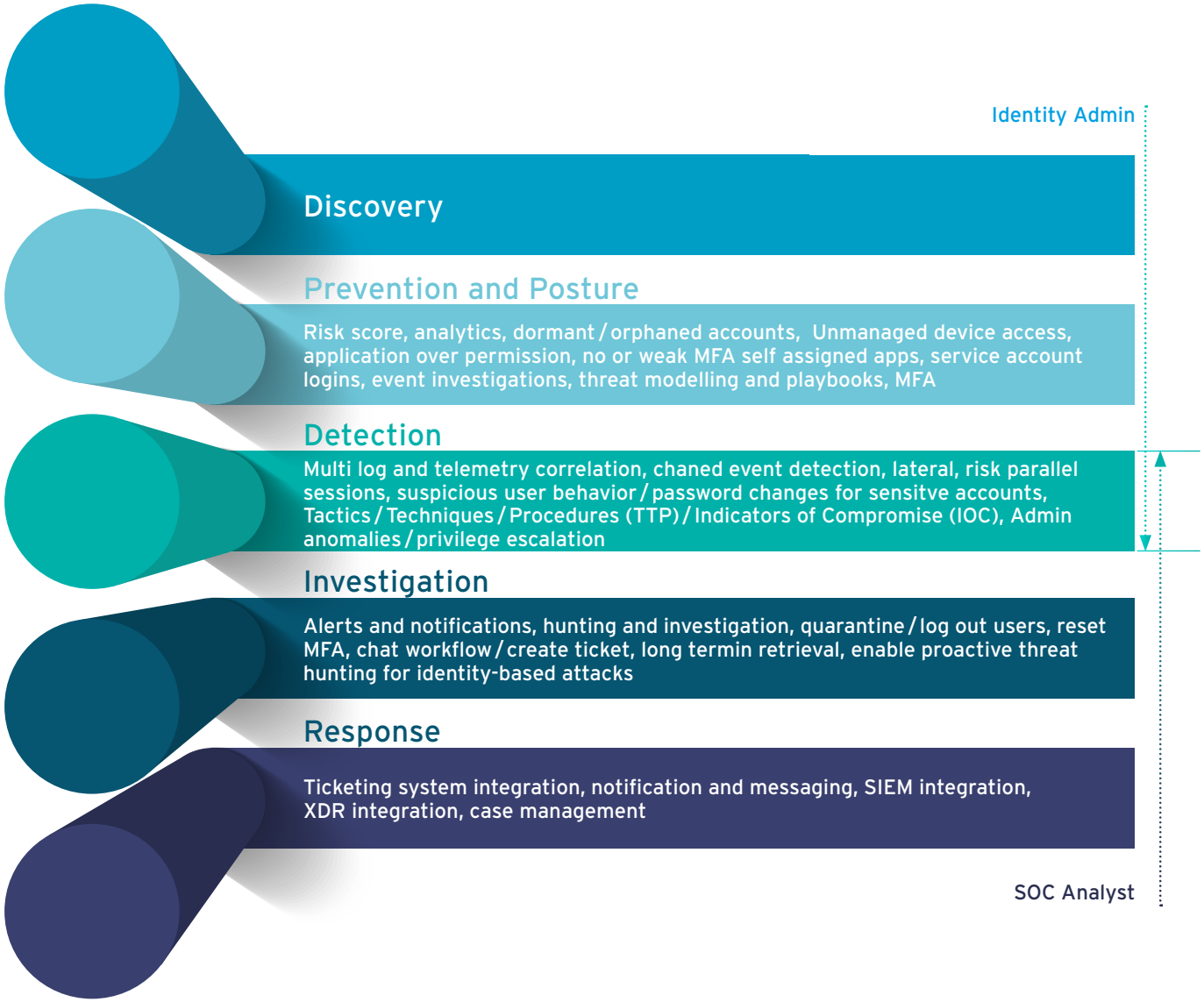
Managing Hybrid and Multi-Cloud Environments
As more organizations adopt hybrid and multi-cloud models, ITDR solutions must effectively monitor identity activities across diverse environments, including on-premises, cloud, and containerized infrastructure, while maintaining scalability.

Handling Identity Misconfigurations and Legacy Systems
Identifying and addressing identity misconfigurations, such as excessive privileges or poor password hygiene, is crucial. Legacy systems that lack modern security features further complicate ITDR implementations.

Scalability for Large Enterprises
Large organizations have complex identity environments with many users, devices, and services. ITDR solutions must scale effectively to handle vast amounts of data and provide actionable insights without overwhelming security teams.

Sophisticated Attacker Techniques
Attackers are increasingly leveraging advanced methods like Kerberoasting, DCSync, and Silver Ticket attacks to exploit identity vulnerabilities. ITDR solutions must stay ahead by detecting and mitigating these evolving threats.

Operational Overheads and Deployment Complexity
The need for agentless and minimal-effort deployment is crucial, especially for hybrid models. Solutions must avoid introducing significant operational burdens or requiring extensive configuration and management.



Chapter 2

The Solution

Identity Threat Detection and Response (ITDR) solutions are designed to proactively detect, investigate, and respond to identity-related threats and vulnerabilities. ITDR introduces mechanisms that target identity-driven attacks, using techniques such as honeytokens and deception technology to detect lateral movement and identity misuse, and enhance protection against credential-based attacks.

ITDR is a crucial component of a comprehensive cybersecurity strategy, as identities have become the primary targets of attackers looking to gain unauthorized access to sensitive systems and information. By focusing on the security of identities, ITDR helps organizations protect against a range of threats, including credential theft, account takeovers, and insider threats.

How ITDR Works

ITDR works by monitoring identity activities across all environments, both identity repositories and identity caches, providing visibility into risks and anomalies. Generally, this begins with a dashboard that provides an overall status of the identity fabric, an ability to drill into identified risks or events (usually based on specific user accounts affected), and to begin investigations into the nature of the risk or attack.

These administrative portals differ in how many play-books are available, their use of AI and ML in assisting with discovery and explanations, and their depth of knowledge of identity products. So, selection of an administrative portal relies heavily on the needs of your organization.

ITDR products connect to IAM platforms and capture critical information in a database or data lake. The first step is to review all known accounts, identify their owners, and perform risk assessments on them. This process is repeated over time to ensure the identity posture is maintained.

The process also watches for events or threats that arise through log files and network traffic. However, this may result both in false positives and false negatives as log analytics needs to deal with large volumes of data, that can be especially dynamic in cloud workloads. Once an incident is detected, the ITDR product alerts administrators and security analysts through a variety of channels.

ITDR brings IAM and SOC teams together, supporting visibility, identity posture management, and threat hunting activities. It also aligns with Zero Trust principles by focusing on the identity as the new security perimeter. With multi-cloud and hybrid deployments, the solution covers Kubernetes clusters, IAM accounts, and cloud storage.

Chapter 3

Top Use Cases

Detecting Lateral Movement

Lateral movement is a common tactic used by adversaries who have gained initial access to a network. Using stolen credentials, attackers can navigate across the network to identify and compromise valuable assets. Detecting lateral movement is challenging because attackers often use legitimate credentials and protocols, making their activities appear benign.

Preventing Privilege Escalation

Privilege escalation is a key objective for attackers seeking to gain elevated permissions within a network. Techniques like Kerberoasting and password spraying are commonly used to obtain privileged credentials. ITDR helps prevent privilege escalation by closely monitoring privileged accounts and using decoy privileged accounts to detect malicious activity. By deploying honeytokens that mimic high-value accounts, ITDR can lure attackers into interacting with these fake accounts, triggering alerts before they can gain real elevated permissions. This approach not only detects privilege escalation attempts but also provides valuable insights into the methods attackers are using.

Defending Active Directory

Microsoft Active Directory (AD) is a critical component of many enterprise environments, making it a prime target for attackers. Detecting Active Directory attacks through traditional methods of monitoring network traffic or log analytics is challenging and time consuming, with attacks resulting in the same events and logs as normal traffic. Deception technology is an effective approach to detect AD attacks, the approach is not dependant on the availability of logs or a priori knowledge of threats, The NSA has written a valuable document on this – see Related Research.

ITDR can enhance AD security by detecting misconfigurations and monitoring for specific attacks such as AS-REP Roasting and DCSync. AS-REP Roasting involves extracting encrypted credentials from AD, while DCSync allows attackers to impersonate domain controllers and extract password hashes. ITDR deploys decoy objects within AD to detect unauthorized access attempts and provides detailed insights into AD vulnerabilities. By identifying and mitigating these threats early, ITDR helps protect the integrity of AD and prevents attackers from gaining domain-wide access.

Cloud Identity Protection

As organizations increasingly adopt cloud services, protecting cloud identities has become a critical challenge. ITDR extends its identity threat detection capabilities to multi-cloud environments, including AWS, Azure, and Google Cloud. It monitors cloud IAM roles, service accounts, and user activities to detect suspicious behavior that could indicate a potential attack. By deploying honeytokens within cloud environments, ITDR can detect unauthorized attempts to access cloud resources. This approach ensures that cloud identities and roles are continuously monitored for anomalies, providing comprehensive protection against identity threats in the cloud.

Proactive Threat Hunting

Proactive threat hunting is an essential part of modern cybersecurity, allowing SOC teams to identify threats before they can cause significant damage. ITDR facilitates proactive threat hunting by providing enriched log data and leveraging deception-based identity activity monitoring. By generating detailed logs of all interactions with decoy assets, ITDR gives SOC teams the context they need to identify potential threats and understand attacker behavior. This enriched data, combined with the use of honeytokens and decoy accounts, enables SOC teams to proactively search for signs of compromise and take action before an incident escalates. ITDR's integration with SIEM platforms further enhances threat hunting capabilities by providing a centralized view of all identity-related activities.

Chapter 4

Top Functional Selection Criteria

Platform

The infrastructure supporting ITDR features and connectivity to IAM and other services.

Discovery and Visibility

Surveying the organization's identity assets by connecting to authoritative systems and linking accounts to the responsible owners. The ITDR solution then provides continuous visibility into the state of the organization's identity assets.

Prevention and Posture Management

Proactively identifies risks to an organization's identities and surfaces them to the administrative team. Also provides decoy accounts that test for intrusion.

Detection

Identifying abnormal behavior or suspicious activities that could indicate a threat to an identity, such as unauthorized access attempts, anomalous login patterns, or exploitation of vulnerabilities related to identity services and protocols.

Investigation

Analyzing detected activities to understand the scope, method, and impact of a potential identity threat. This involves correlating data from various sources to gain insights into the nature of the threat and identifying the affected systems or data.

Response

Taking appropriate actions to mitigate identified threats and prevent future occurrences. This could involve adjusting security policies, implementing stronger authentication measures, revoking compromised credentials, or deploying patches to address vulnerabilities.

Chapter 5

Vendor Spotlight

Acalvio ShadowPlex

Acalvio Technologies has positioned itself as a leader in the field of deception-based cybersecurity solutions with its flagship product, ShadowPlex. As a comprehensive Identity Threat Detection and Response (ITDR) platform, ShadowPlex leverages deception technology to detect, investigate, and respond to identity-related threats across hybrid and cloud environments. By seamlessly integrating with existing security infrastructure, Acalvio aims to strengthen enterprise defenses against increasingly sophisticated identity-driven attacks, including identity attacks originating from external threat actors and insider threats.

Acalvio's ShadowPlex is an ITDR platform that focuses on using deception techniques to detect identity threats early in their attack lifecycle. Unlike traditional security tools that rely on signature or log-based detection, ShadowPlex employs deceptive elements such as honeytokens and honey accounts —fake credentials — to lure and identify malicious actors attempting to misuse identity assets. This proactive approach is instrumental in detecting threats that may evade conventional endpoint detection solutions. The solution also provides visibility to identity threats originating from unmanaged endpoints, this is an important attack surface not protected through traditional security tools.

ShadowPlex is built to seamlessly integrate with identity and access management (IAM) systems, as well as security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms. This integration helps to unify the efforts of both security operations center (SOC) and IAM teams, facilitating a more coordinated defense against identity threats. With support for both on-premises and cloud environments, including Kubernetes and multi-cloud deployments, ShadowPlex provides comprehensive coverage for enterprise identity infrastructure.

A notable feature of ShadowPlex is its emphasis on agentless deployment, which simplifies the adoption process for organizations by eliminating the need for extensive endpoint software installations. This is particularly beneficial for enterprises with diverse environments, where maintaining endpoint agents can become cumbersome and expensive. ShadowPlex's cloud-native architecture also allows for scalability, enabling it to adapt to the growing needs of enterprises as they expand their identity ecosystems.

How ShadowPlex Works

ShadowPlex employs advanced deception techniques, including honeytokens, honey accounts, and decoy systems, to create a layer of false information within the identity environment. These deceptive elements are strategically positioned to attract attackers, enabling early detection of malicious activity. When an attacker interacts with these decoys, ShadowPlex raises alerts, allowing security teams to initiate appropriate responses before the threat escalates.

In addition to deception-based detection, ShadowPlex provides deep insights into the identity attack surface. It monitors privileged accounts, service accounts, and non-person entities to assess vulnerabilities and detect potential threats. By integrating with SIEM and SOAR platforms, ShadowPlex can automate threat response, helping to reduce the mean time to repair (MTTR) and mitigate attacks in real time.

ShadowPlex's collaboration with CrowdStrike's Falcon Identity Protection and with Microsoft's Defender for Identity adds an extra layer of robustness to the solution. This integration enhances detection capabilities through joint use of deception and endpoint monitoring, providing a holistic view of identity threats that would be challenging to detect without the use of deception. The joint approach ensures that malicious activity is detected and contained quickly, limiting the potential damage that attackers can cause.

Acalvio ShadowPlex offers a robust ITDR solution that leverages deception technology to effectively detect and respond to identity threats. Its strengths lie in its proactive detection mechanisms, scalability, and seamless integration with existing security tools, making it a valuable addition to any enterprise's security stack. However, organizations should be mindful of the challenges associated with deploying deception at scale, the potential for false positives, and the need for comprehensive integration. By addressing these challenges, Acalvio ShadowPlex can provide significant value in the fight against sophisticated identity-driven attacks.

Strengths

ShadowPlex's use of deception technology, including honeytokens and honey accounts, is highly effective at detecting a wide variety of identity threats, many of which evade traditional security tools. This proactive detection method not only detects attacks against identity repositories using honey accounts, but also distributes honeytokens across the network endpoints and services to ensure that malicious actors are caught early in their attack lifecycle.

The agentless nature of ShadowPlex makes it easy to deploy across complex environments, reducing operational overhead and simplifying the adoption process. This is particularly beneficial for organizations with hybrid or multi-cloud architectures, where managing endpoint agents can be challenging.

ShadowPlex has extensive use of AI to automate the configuration and placement of the deceptions. Manual attempts to create deceptions are challenging, with a single user object in Active Directory having 100+ attributes, including bitmaps. Through the use of ML and AI, ShadowPlex automates the creation of realistic deceptions that are enticing for attackers to exploit, luring the attacker toward the deceptions and protecting the enterprise assets.

ShadowPlex integrates seamlessly with leading SIEM, SOAR, and IAM platforms, allowing security teams to leverage existing investments in their cybersecurity infrastructure. This integration supports coordinated threat detection and response, enhancing the overall security posture.

ShadowPlex's cloud-native architecture is designed for scalability, making it suitable for enterprises of all sizes. It provides coverage across on-premises, cloud, and Kubernetes environments, offering a comprehensive solution for modern identity security challenges.

The collaboration with CrowdStrike's Falcon Identity Protection and Microsoft Defender for Identity enhances the overall effectiveness of ShadowPlex by combining deception-based detection with end-point monitoring. This integration ensures a more comprehensive approach to identity threat detection and response, improving detection accuracy and response efficiency.

Challenges

ShadowPlex relies heavily on attacker interaction with deception elements to generate alerts. If attackers avoid interacting with honeytokens or decoy accounts, the solution's ability to detect threats may be limited, potentially leaving some attacks undetected. However, by comprehensive deployment of honeytokens across the network, Acalvio ensures that attackers will come across deception at every step.

The effectiveness of ShadowPlex is enhanced through integration with other security tools, such as SIEM, SOAR, and IAM systems. Organizations that do not have mature integrations in place may find it difficult to fully realize the benefits of ShadowPlex.

Although deception technologies are designed to reduce false positives, there remains a possibility that benign activities could trigger alerts, especially in environments with frequent legitimate scanning or testing activities. This may lead to alert fatigue if not managed properly.

ShadowPlex is primarily focused on identity threats and relies on deception as its main detection mechanism. It does not provide full endpoint protection capabilities, which means that it needs to be used in conjunction with other endpoint detection and response (EDR) tools for comprehensive security.

Chapter 6

Considerations

Deployment

ITDR solutions are mainly delivered as cloud-hosted software as a service (SaaS), with most vendors providing this deployment model. However, vendors also offer support for and integration with on-premises environments. Despite the continued relevance of on-premises deployments, organizations are requiring more agile multi-cloud and multi-hybrid deployments that provide a gradual migration to the cloud.

Pre-deployment Considerations

How modern is the solution's architecture?
Preference should be given to modern software architecture solutions that use microservices, container-based deployments, and APIs that provide more modular and flexible deployment, orchestration, and customization.

How well can your solution scale to meet future growth in terms of users and transaction volume?
The ability of an ITDR solution to scale effectively is crucial for accommodating future growth in both user base and transaction volume. This ensures that as your organization expands, the authentication system can manage increased demands without compromising performance or security.

Questions to Ask Vendors during RFPs

Do you specialize in serving specific industries?
Some vendors focus on the finance industry and/or payments fraud prevention. Others focus on ecommerce. Some provide services that work across multiple industries.

What are your key differentiators?
Understanding the key differentiators between the various vendors is essential. Determine how important or relevant these differentiators are to your ITDR journey. This information can help to shortlist vendors. For example, when selecting an ITDR vendor, inquire about their solution's security capabilities as detailed above.

What is the roadmap for future development and innovation of your solution?
If your organization has a good idea of future ITDR management requirements, find out what a prospective vendor's plans are for future versions of the solution to ensure that your organization's expected future needs will be met.

Chapter 6

Recommendations

These considerations are designed to help organizations navigate the complexities of adopting ITDR and ensure that they select a solution that not only enhances security but also improves the overall user experience.

Choosing a solution always requires a thorough analysis of specific customer requirements and a comparison with available product and/or service features. Therefore, this Buyer's Compass will help organizations identify those vendors that customers should look at more closely.

Identify Your Organization's Needs

Before selecting an ITDR solution, it's crucial to identify your organization's specific needs and challenges. Assess the current identity threat landscape, your existing cybersecurity capabilities, and any gaps that need to be addressed. Consider the scale of your environment—whether it includes on-premises, cloud, or hybrid components—and evaluate your security team's capabilities. Understanding the unique characteristics of your organization, such as the presence of legacy systems or specific regulatory requirements, will help in selecting an ITDR solution that aligns with your operational goals and addresses your most pressing security concerns.

Work with Your Incumbent System Vendors

Leveraging the relationships with your existing system vendors can significantly enhance the implementation of an ITDR solution. Collaborating with current vendors ensures better integration and interoperability between ITDR tools and your existing security stack, such as IAM, SIEM, and SOAR platforms. Vendors familiar with your environment can provide insights into how to best implement ITDR without causing disruptions. Working closely with them can also streamline the deployment process, reduce compatibility issues, and help optimize the use of existing investments to create a unified and effective cybersecurity strategy.

Choose an Appropriate Deployment Model

Choosing the right deployment model for an ITDR solution is essential to its success. Depending on your organization's infrastructure, you may opt for an on-premises, cloud-based, or hybrid deployment model. Cloud-based solutions offer scalability and lower upfront costs, while on-premises deployments provide greater control over data and compliance requirements. Hybrid models combine the best of both worlds, offering flexibility and resilience. Evaluate your organization's capabilities, such as cloud readiness, compliance requirements, and operational preferences, to determine the deployment model that will provide the most value while aligning with your security policies and resource availability.

Related Research

Leadership Compass

- Fraud Reduction Intelligence Platforms (2023)
- ITDR (2024)
- Fraud Reduction Intelligence Platforms (2021)
- CIAM Platforms (2022)

Others

- NSA Guidance for Mitigating Active Directory Compromises

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

For further information, please contact clients@kuppingercole.com.

KUPPINGERCOLE ANALYSTS AG
Wilhelmstraße 20 – 22
65185 Wiesbaden | GERMANY
P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 - 11
E: clients@kuppingercole.com.
KUPPINGERCOLE.COM