

access management gartner magic quadrant

Access Management Gartner Magic Quadrant: A Deep Dive into 2024 Leaders and Challengers

Author: Dr. Anya Sharma, PhD, CISSP, CISM. Dr. Sharma is a leading cybersecurity researcher with over 15 years of experience in identity and access management (IAM). She has published extensively on access management solutions and has consulted for numerous Fortune 500 companies on IAM strategy and implementation. Her expertise directly informs her analysis of the Access Management Gartner Magic Quadrant.

Publisher: Gartner, Inc. Gartner is a globally recognized research and advisory firm specializing in information technology. Their Magic Quadrant reports are highly regarded within the IT industry for their rigorous methodology and insightful analysis, providing a valuable benchmark for evaluating vendors in specific technology markets. Their credibility in the realm of the Access Management Gartner Magic Quadrant is unparalleled.

Editor: Mr. David Chen, a seasoned editor with over 10 years of experience at Gartner, specializing in cybersecurity reports. Mr. Chen possesses a deep understanding of the methodologies used in creating the Access Management Gartner Magic Quadrant and ensures the report's accuracy and clarity.

Keywords: Access Management Gartner Magic Quadrant, IAM, Identity and Access Management, Cybersecurity, Access Management Solutions, Gartner Magic Quadrant 2024, Access Governance, Privileged Access Management, Identity Governance and Administration (IGA), Cloud Access Security Broker (CASB), Zero Trust, MFA

Introduction: Navigating the Access Management Gartner Magic Quadrant

The Access Management Gartner Magic Quadrant is a crucial resource for organizations seeking to understand the competitive landscape of Identity and Access Management (IAM) solutions. This report provides an in-depth analysis of the 2024 Magic Quadrant, examining the key factors that contribute to vendor placement, highlighting leaders and challengers, and discussing the implications for businesses seeking to enhance their security posture. Understanding the Access Management Gartner Magic Quadrant is crucial for making informed decisions about access management strategies.

Methodology of the Access Management Gartner Magic Quadrant

Gartner's methodology for creating the Access Management Gartner Magic Quadrant is rigorous and multi-faceted. It involves a comprehensive assessment of vendors based on two primary axes: Completeness of Vision and Ability to Execute. Completeness of Vision evaluates a vendor's market understanding, strategy, and innovative capabilities. Ability to Execute assesses a vendor's product or service capabilities, its customer base, its financial performance, and its operational effectiveness.

Data for the Access Management Gartner Magic Quadrant is collected through various channels, including:

Vendor submissions: Detailed questionnaires and presentations from participating vendors.

Customer references: Interviews with customers using the vendors' solutions to gather feedback on their experiences.

Gartner's own research: Analysis of market trends, technological advancements, and competitive dynamics.

This data is then rigorously analyzed to create a detailed profile for each vendor, ultimately resulting in their placement within the Access Management Gartner Magic Quadrant.

2024 Leaders in the Access Management Gartner Magic Quadrant

The Access Management Gartner Magic Quadrant 2024 identifies several vendors as leaders, demonstrating both strong vision and execution capabilities. These leaders typically offer comprehensive IAM solutions encompassing a wide range of functionalities, including:

Identity Governance and Administration (IGA): Managing user identities, access rights, and compliance.

Privileged Access Management (PAM): Securing access to sensitive systems and data for privileged users.

Cloud Access Security Broker (CASB): Controlling and monitoring access to cloud applications.

Multi-Factor Authentication (MFA): Adding layers of security to user authentication.

(Note: Specific vendor names and detailed analysis would be included here, referencing directly from the Gartner report. Due to the dynamic nature of the Magic Quadrant and the need to avoid outdated information, specific vendor names are omitted in this example.) The report would delve into the strengths and weaknesses of each leader, providing actionable insights for potential customers.

Challengers and Visionaries in the Access Management Gartner Magic Quadrant

Beyond the leaders, the Access Management Gartner Magic Quadrant also identifies vendors categorized as Challengers and Visionaries. Challengers possess a strong ability to execute but may have a less comprehensive vision or a narrower focus. Visionaries, on the other hand, exhibit a strong vision but may still be developing their execution capabilities. Analyzing these categories within the Access Management Gartner Magic Quadrant provides a nuanced perspective on the market, allowing organizations to identify vendors that align with their specific needs and risk tolerance.

Impact of Zero Trust and Cloud Adoption on the Access Management Gartner Magic Quadrant

The increasing adoption of Zero Trust security models and cloud-based applications significantly impacts the Access Management Gartner Magic Quadrant. Vendors that effectively integrate Zero Trust principles into their solutions and provide robust cloud access management capabilities are likely to be positioned more favorably. The Access Management Gartner Magic Quadrant reflects this trend, highlighting vendors that prioritize these critical aspects of modern security.

Choosing the Right Access Management Solution Based on the Gartner Magic Quadrant

The Access Management Gartner Magic Quadrant is a valuable tool, but it's not the sole determinant in selecting an access management solution. Organizations should consider their specific requirements, such as:

Industry regulations and compliance: Meeting industry-specific compliance standards (e.g., HIPAA, GDPR).

Integration with existing systems: Seamless integration with existing IT infrastructure.

Scalability and flexibility: Ability to adapt to changing business needs.

Budget and cost considerations: Evaluating the total cost of ownership.

By carefully considering these factors in conjunction with the insights provided by the Access Management Gartner Magic Quadrant, organizations can make informed decisions to select the most appropriate access management solution.

Conclusion

The Access Management Gartner Magic Quadrant provides a crucial framework for

understanding the competitive landscape of IAM solutions. By carefully analyzing the vendors' strengths and weaknesses, their vision, and their ability to execute, organizations can identify solutions that best align with their security objectives and business needs. The report's rigorous methodology and in-depth analysis make it an indispensable resource for making informed decisions in the complex world of access management. Understanding the implications of the Access Management Gartner Magic Quadrant is critical for maintaining a robust and secure IT environment in today's rapidly evolving threat landscape.

FAQs

1. What is the Access Management Gartner Magic Quadrant? It's a Gartner report that assesses and ranks vendors of Identity and Access Management (IAM) solutions based on their completeness of vision and ability to execute.
1. How often is the Access Management Gartner Magic Quadrant updated? Typically, it's updated annually.
1. What are the key criteria used in the Access Management Gartner Magic Quadrant? Key criteria include completeness of vision, ability to execute, market responsiveness, customer experience, and more.
1. How can I access the Access Management Gartner Magic Quadrant report? You typically need to purchase a subscription to Gartner's research services.
1. Are there any free resources summarizing the Access Management Gartner Magic Quadrant? Some analyst firms and technology blogs might offer summaries, but the full report is proprietary.
1. What does it mean if a vendor is positioned as a Leader in the Access Management Gartner Magic Quadrant? It signifies they have both a strong vision for the future of IAM and a proven ability to deliver on their promises.

1. What are the implications of being positioned as a Niche Player? Niche players excel in a specific area of IAM but may not offer as comprehensive a solution as Leaders.
1. How can I use the Access Management Gartner Magic Quadrant to inform my vendor selection? Use it as one data point among many; consider your specific needs and evaluate vendors based on those requirements.
1. Is the Access Management Gartner Magic Quadrant the only resource I should consider when choosing an IAM solution? No; conduct thorough due diligence, including reference checks and product demos, to inform your decision.

Related Articles

1. "Decoding the Access Management Gartner Magic Quadrant: A Guide for CIOs": This article focuses on the practical implications of the Magic Quadrant for Chief Information Officers.
1. "Top 5 Trends Shaping the Access Management Gartner Magic Quadrant": This piece explores emerging trends that influence vendor positioning in the Magic Quadrant.
1. "A Comparative Analysis of Leaders in the Access Management Gartner Magic Quadrant": A detailed comparison of the top-ranked vendors and their strengths.
1. "Navigating the Challengers Quadrant: Finding Hidden Gems in the Access Management Gartner Magic Quadrant": Focuses on under-the-radar vendors with potential.

1. "The Impact of Zero Trust on the Access Management Gartner Magic Quadrant": This analysis delves into how the Zero Trust movement is reshaping the landscape.
1. "Cost Considerations and ROI in the Access Management Gartner Magic Quadrant": This article explores the financial aspects of different vendors.
1. "Access Management Gartner Magic Quadrant and Compliance Requirements": A look at how compliance affects vendor choices.
1. "Case Study: How One Company Used the Access Management Gartner Magic Quadrant to Choose an IAM Solution": A practical example of how the report is used.
1. "Future Predictions: The Next Generation of Access Management as Seen in the Gartner Magic Quadrant": This article speculates on future trends based on current Magic Quadrant positioning.

access management gartner magic quadrant: *Contemporary Identity and Access*

Management Architectures: Emerging Research and Opportunities Ng, Alex Chi Keung, 2018-01-26
 Due to the proliferation of distributed mobile technologies and heavy usage of social media, identity and access management has become a very challenging area. Businesses are facing new demands in implementing solutions, however, there is a lack of information and direction. Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities is a critical scholarly resource that explores management of an organization's identities, credentials, and attributes which assures the identity of a user in an extensible manner set for identity and access administration. Featuring coverage on a broad range of topics, such as biometric application programming interfaces, telecommunication security, and role-based access control, this book is geared towards academicians, practitioners, and researchers seeking current research on identity and access management.

access management gartner magic quadrant: *Cloud Identity Patterns and Strategies*

Giuseppe Di Federico, Fabrizio Barcaroli, 2022-12-23 Get to grips with identity patterns and design a structured enterprise identity model for cloud applications Key Features Learn all you need to know about different identity patterns and implementing them in real-world scenarios Handle multi-IDP-related common situations no matter how big your organization Gain practical insights into OAuth implementation patterns and flows Book Description Identity is paramount for every

architecture design, making it crucial for enterprise and solutions architects to understand the benefits and pitfalls of implementing identity patterns. However, information on cloud identity patterns is generally scattered across different sources and rarely approached from an architect's perspective, and this is what *Cloud Identity Patterns and Strategies* aims to solve, empowering solutions architects to take an active part in implementing identity solutions. Throughout this book, you'll cover various theoretical topics along with practical examples that follow the implementation of a standard de facto identity provider (IdP) in an enterprise, such as Azure Active Directory. As you progress through the chapters, you'll explore the different factors that contribute to an enterprise's current status quo around identities and harness modern authentication approaches to meet specific requirements of an enterprise. You'll also be able to make sense of how modern application designs are impacted by the company's choices and move on to recognize how a healthy organization tackles identity and critical tasks that the development teams pivot on. By the end of this book, you'll be able to breeze through creating portable, robust, and reliable applications that can interact with each other. What you will learn

Understand the evolution of identity in the enterprise
Discover basic to advanced OAuth patterns and implementations
Find out how OAuth standards are usually adopted in the enterprise
Explore proven solutions for modern identity challenges
Use Azure AD for implementing identity solutions
Comprehend how company structure and strategies influence design decisions

Who this book is for
This book is for cloud security engineers and identity experts. Enterprise architects, tech leads, developers, and anyone who wants to learn how to use identity patterns and strategies to build identity models for the modern cloud era will find this book useful. This book covers many DevOps and Agile principles; although not a pre-requisite, familiarity with these topics would be helpful.

access management gartner magic quadrant: [*Azure Architecture Explained*](#) David Rendón, Brett Hargreaves, 2023-09-22 Enhance your career as an Azure architect with cutting-edge tools, expert guidance, and resources from industry leaders

Key Features

- Develop your business case for the cloud with technical guidance from industry experts
- Address critical business challenges effectively by leveraging proven combinations of Azure services
- Tackle real-world scenarios by applying practical knowledge of reference architectures

Purchase of the print or Kindle book includes a free PDF eBook

Book Description

Azure is a sophisticated technology that requires a detailed understanding to reap its full potential and employ its advanced features. This book provides you with a clear path to designing optimal cloud-based solutions in Azure, by delving into the platform's intricacies. You'll begin by understanding the effective and efficient security management and operation techniques in Azure to implement the appropriate configurations in Microsoft Entra ID. Next, you'll explore how to modernize your applications for the cloud, examining the different computation and storage options, as well as using Azure data solutions to help migrate and monitor workloads. You'll also find out how to build your solutions, including containers, networking components, security principles, governance, and advanced observability. With practical examples and step-by-step instructions, you'll be empowered to work on infrastructure-as-code to effectively deploy and manage resources in your environment. By the end of this book, you'll be well-equipped to navigate the world of cloud computing confidently.

What you will learn

- Implement and monitor cloud ecosystem including, computing, storage, networking, and security
- Recommend optimal services for performance and scale
- Provide, monitor, and adjust capacity for optimal results
- Craft custom Azure solution architectures
- Design computation, networking, storage, and security aspects in Azure
- Implement and maintain Azure resources effectively

Who this book is for

This book is an indispensable resource for Azure architects looking to develop cloud-based services along with deploying and managing applications within the Microsoft Azure ecosystem. It caters to professionals responsible for crucial IT operations, encompassing budgeting, business continuity, governance, identity management, networking, security, and automation. If you have prior experience in operating systems, virtualization, infrastructure, storage structures, or networking, and aspire to master the implementation of best practices in the Azure cloud, then this book will become your go-to guide.

access management gartner magic quadrant: The Connector Manager Jaime Roca, Sari Wilde, 2019-09-19 The best managers work smarter, not harder After conducting a unique global study of over 9,000 people, analysts at the world-leading sales research firm Gartner identified four distinct types of manager. Incredibly, they found one type consistently performs far better than the rest, and it wasn't the one they were expecting. Connector Managers understand that it's not enough for managers to just encourage and teach employees themselves, and that providing constant coaching to employees can actually be detrimental to their independent development. Instead, by connecting employees to others in the team or organisation, Connector Managers can help their employees develop a range of skills beyond their own areas of expertise. Although the four types of managers are more or less evenly distributed, employees with Connector Managers perform significantly better than others. Employees with Always-on Managers who provide constant feedback and coaching perform significantly worse. Drawing on their ground-breaking data-driven research, as well as in-depth case studies and extensive interviews with thousands of managers, you'll discover what behaviours define Connector Managers and how you can use them yourself to build brilliant, powerhouse teams.

access management gartner magic quadrant: Engineering and Management of Data Centers Jorge Marx Gómez, Manuel Mora, Mahesh S. Raisinghani, Wolfgang Nebel, Rory V. O'Connor, 2017-11-10 This edited volume covers essential and recent development in the engineering and management of data centers. Data centers are complex systems requiring ongoing support, and their high value for keeping business continuity operations is crucial. The book presents core topics on the planning, design, implementation, operation and control, and sustainability of a data center from a didactical and practitioner viewpoint. Chapters include: · Foundations of data centers: Key Concepts and Taxonomies · ITSDM: A Methodology for IT Services Design · Managing Risks on Data Centers through Dashboards · Risk Analysis in Data Center Disaster Recovery Plans · Best practices in Data Center Management Case: KIO Networks · QoS in NaaS (Network as a Service) using Software Defined Networking · Optimization of Data Center Fault-Tolerance Design · Energetic Data Centre Design Considering Energy Efficiency Improvements During Operation · Demand-side Flexibility and Supply-side Management: The Use Case of Data Centers and Energy Utilities · DevOps: Foundations and its Utilization in Data Centers · Sustainable and Resilient Network Infrastructure Design for Cloud Data Centres · Application Software in Cloud-Ready Data Centers This book bridges the gap between academia and the industry, offering essential reading for practitioners in data centers, researchers in the area, and faculty teaching related courses on data centers. The book can be used as a complementary text for traditional courses on Computer Networks, as well as innovative courses on IT Architecture, IT Service Management, IT Operations, and Data Centers.

access management gartner magic quadrant: Handbook of Research on Big Data Storage and Visualization Techniques Segall, Richard S., Cook, Jeffrey S., 2018-01-05 The digital age has presented an exponential growth in the amount of data available to individuals looking to draw conclusions based on given or collected information across industries. Challenges associated with the analysis, security, sharing, storage, and visualization of large and complex data sets continue to plague data scientists and analysts alike as traditional data processing applications struggle to adequately manage big data. The Handbook of Research on Big Data Storage and Visualization Techniques is a critical scholarly resource that explores big data analytics and technologies and their role in developing a broad understanding of issues pertaining to the use of big data in multidisciplinary fields. Featuring coverage on a broad range of topics, such as architecture patterns, programing systems, and computational energy, this publication is geared towards professionals, researchers, and students seeking current research and application topics on the subject.

access management gartner magic quadrant: Privileged Attack Vectors Morey J. Haber, 2020-06-13 See how privileges, insecure passwords, administrative rights, and remote access can be combined as an attack vector to breach any organization. Cyber attacks continue to increase in

volume and sophistication. It is not a matter of if, but when, your organization will be breached. Threat actors target the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today's environmental complexity has seen an explosion of privileged credentials for many different account types such as domain and local administrators, operating systems (Windows, Unix, Linux, macOS, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and so many more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. We are experiencing an expanding universe of privileged accounts almost everywhere. There is no one solution or strategy to provide the protection you need against all vectors and stages of an attack. And while some new and innovative products will help protect against or detect against a privilege attack, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. *Privileged Attack Vectors* details the risks associated with poor privilege management, the techniques that threat actors leverage, and the defensive measures that organizations should adopt to protect against an incident, protect against lateral movement, and improve the ability to detect malicious activity due to the inappropriate usage of privileged credentials. This revised and expanded second edition covers new attack vectors, has updated definitions for privileged access management (PAM), new strategies for defense, tested empirical steps for a successful implementation, and includes new disciplines for least privilege endpoint management and privileged remote access. What You Will Learn Know how identities, accounts, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and monitoring strategies to mitigate privilege threats and risk Understand a 10-step universal privilege management implementation plan to guide you through a successful privilege access management journey Develop a comprehensive model for documenting risk, compliance, and reporting based on privilege session activity Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privilege access management problems

access management gartner magic quadrant: *Real Business of IT* Richard Hunter, George Westerman, 2009-10-20 If you're a general manager or CFO, do you feel you're spending too much on IT or wishing you could get better returns from your IT investments? If so, it's time to examine what's behind this IT-as-cost mind-set. In *The Real Business of IT*, Richard Hunter and George Westerman reveal that the cost mind-set stems from IT leaders' inability to communicate about the business value they create-so CIOs get stuck discussing budgets rather than their contributions to the organization. The authors explain how IT leaders can combat this mind-set by first using information technology to generate three forms of value important to leaders throughout the organization: -Value for money when your IT department operates efficiently and effectively -An investment in business performance evidenced when IT helps divisions, units, and departments boost profitability -Personal value of CIOs as leaders whose contributions to their enterprise go well beyond their area of specialization The authors show how to communicate about these forms of value with non-IT leaders-so they understand how your firm is benefiting and see IT as the strategic powerhouse it truly is.

access management gartner magic quadrant: *Infonomics* Douglas B. Laney, 2017-09-05 Many senior executives talk about information as one of their most important assets, but few behave as if it is. They report to the board on the health of their workforce, their financials, their customers, and their partnerships, but rarely the health of their information assets. Corporations typically exhibit greater discipline in tracking and accounting for their office furniture than their data. Infonomics is the theory, study, and discipline of asserting economic significance to information. It strives to apply both economic and asset management principles and practices to the valuation, handling, and deployment of information assets. This book specifically shows: CEOs and business leaders how to more fully wield information as a corporate asset CIOs how to improve the flow and

accessibility of information CFOs how to help their organizations measure the actual and latent value in their information assets. More directly, this book is for the burgeoning force of chief data officers (CDOs) and other information and analytics leaders in their valiant struggle to help their organizations become more infosavvy. Author Douglas Laney has spent years researching and developing Infonomics and advising organizations on the infinite opportunities to monetize, manage, and measure information. This book delivers a set of new ideas, frameworks, evidence, and even approaches adapted from other disciplines on how to administer, wield, and understand the value of information. Infonomics can help organizations not only to better develop, sell, and market their offerings, but to transform their organizations altogether. Doug Laney masterfully weaves together a collection of great examples with a solid framework to guide readers on how to gain competitive advantage through what he labels the unruly asset – data. The framework is comprehensive, the advice practical and the success stories global and across industries and applications. Liz Rowe, Chief Data Officer, State of New Jersey A must read for anybody who wants to survive in a data centric world. Shaun Adams, Head of Data Science, Betterbathrooms.com Phenomenal! An absolute must read for data practitioners, business leaders and technology strategists. Doug's lucid style has a set a new standard in providing intelligible material in the field of information economics. His passion and knowledge on the subject exudes thru his literature and inspires individuals like me. Ruchi Rajasekhar, Principal Data Architect, MISO Energy I highly recommend Infonomics to all aspiring analytics leaders. Doug Laney's work gives readers a deeper understanding of how and why information should be monetized and managed as an enterprise asset. Laney's assertion that accounting should recognize information as a capital asset is quite convincing and one I agree with. Infonomics enjoyably echoes that sentiment! Matt Green, independent business analytics consultant, Atlanta area If you care about the digital economy, and you should, read this book. Tanya Shuckhart, Analyst Relations Lead, IRI Worldwide

access management gartner magic quadrant: Identity Attack Vectors Morey J. Haber, Darran Rolls, 2019-12-17 Discover how poor identity and privilege management can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments

access management gartner magic quadrant: Research Directions in Data and Applications

Security Ehud Gudes, Sujeet Shenoi, 2013-03-19 Research Directions in Data and Applications Security describes original research results and innovative practical developments, all focused on maintaining security and privacy in database systems and applications that pervade cyberspace. The areas of coverage include: -Role-Based Access Control; -Database Security; -XML Security; -Data Mining and Inference; -Multimedia System Security; -Network Security; -Public Key Infrastructure; -Formal Methods and Protocols; -Security and Privacy.

access management gartner magic quadrant: *Trust and Privacy in Digital Business* Sokratis Katsikas, Günther Pernul, 2004-11-02 Sincerely welcome to proceedings of the 1st International Conference on Trust and Privacy in Digital Business, Zaragoza, Spain, held from August 30th to September 1st, 2004. This conference was an outgrowth of the two successful TrustBus international workshops, held in 2002 and 2003 in conjunction with the DEXA conferences in Aix-en-Provence and in Prague. Being the first of a planned series of successful conferences it was our goal that this event would initiate a forum to bring together researchers from academia and commercial developers from industry to discuss the state of the art of technology for establishing trust and privacy in digital business. We thank you all the attendees for coming to Zaragoza to participate and debate the new emerging advances in this area. The conference program consisted of one invited talk and nine regular technical papers sessions. The invited talk and keynote speech was delivered by Ahmed Patel from the Computer Networks and Distributed Systems Research Group, University College Dublin, Ireland on "Developing Secure, Trusted and Auditable Services for E-Business: An Autonomic Computing Approach". A paper covering his talk is also contained in this book. The regular paper sessions covered a broad range of topics, from access control - sues to electronic voting, from trust and protocols to digital rights management. The conference attracted close to 100 submissions of which the program committee - cepted 29 papers for presentation and inclusion in the conference proceedings.

access management gartner magic quadrant: *The Challenge of Sustainability in Agricultural Systems* Aleksei V. Bogoviz, 2021-06-05 This book brings together segmental knowledge and creates new insights on the sustainability of agricultural systems, critically analyzing not only individual system components, but also focusing on interactions between them and external environments. This book is primarily devoted to (1) agricultural agribusiness, (2) policies and institutions, and (3) farming systems. The compelling collection of chapters presents critical, comparative, and balanced perspectives on what changes are needed to achieve and maintain sustainability in agricultural systems, actively leading to new ways of thinking about these complex issues. The research presented relies on an array of methods developed within complex systems science, addresses the existing gaps in the scholarship, and uses original data collected on the development of agricultural systems. Finally, the authors provide robust conclusions and recommendations for both scholars and practitioners in the field of studying, constructing, and maintaining sustainable agricultural systems. The special focus of the book is on technologies, policies, and management systems enabling sustainable agricultural development. A rich collection of practical cases could be used to move from theories to reality. The book appeals to both academics and professionals working in the field.

access management gartner magic quadrant: *Mastering Cloud Security Posture Management (CSPM)* Qamar Nomani, 2024-01-31 Strengthen your security posture in all aspects of CSPM technology, from security infrastructure design to implementation strategies, automation, and remedial actions using operational best practices across your cloud environment Key Features Choose the right CSPM tool to rectify cloud security misconfigurations based on organizational requirements Optimize your security posture with expert techniques for in-depth cloud security insights Improve your security compliance score by adopting a secure-by-design approach and implementing security automation Purchase of the print or Kindle book includes a free PDF eBook Book Description This book will help you secure your cloud infrastructure confidently with cloud security posture management (CSPM) through expert guidance that'll enable you to implement CSPM effectively, ensuring an optimal security posture across multi-cloud infrastructures. The book begins by unraveling the fundamentals of cloud security, debunking myths about the shared

responsibility model, and introducing key concepts such as defense-in-depth, the Zero Trust model, and compliance. Next, you'll explore CSPM's core components, tools, selection criteria, deployment strategies, and environment settings, which will be followed by chapters on onboarding cloud accounts, dashboard customization, cloud assets inventory, configuration risks, and cyber threat hunting. As you progress, you'll get to grips with operational practices, vulnerability and patch management, compliance benchmarks, and security alerts. You'll also gain insights into cloud workload protection platforms (CWPPs). The concluding chapters focus on Infrastructure as Code (IaC) scanning, DevSecOps, and workflow automation, providing a thorough understanding of securing multi-cloud environments. By the end of this book, you'll have honed the skills to make informed decisions and contribute effectively at every level, from strategic planning to day-to-day operations.

What you will learn

- Find out how to deploy and onboard cloud accounts using CSPM tools
- Understand security posture aspects such as the dashboard, asset inventory, and risks
- Explore the Kusto Query Language (KQL) and write threat hunting queries
- Explore security recommendations and operational best practices
- Get to grips with vulnerability, patch, and compliance management, and governance
- Familiarize yourself with security alerts, monitoring, and workload protection best practices
- Manage IaC scan policies and learn how to handle exceptions

Who this book is for

If you're a cloud security administrator, security engineer, or DevSecOps engineer, you'll find this book useful every step of the way—from proof of concept to the secured, automated implementation of CSPM with proper auto-remediation configuration. This book will also help cybersecurity managers, security leads, and cloud security architects looking to explore the decision matrix and key requirements for choosing the right product. Cloud security enthusiasts who want to enhance their knowledge to bolster the security posture of multi-cloud infrastructure will also benefit from this book.

access management gartner magic quadrant: Mastering IAM Kris Hermans, In today's interconnected digital landscape, effective Identity and Access Management (IAM) is vital for organizations to secure their systems, protect sensitive data, and enable seamless collaboration. In *Mastering IAM*, acclaimed author Kris Hermans provides a comprehensive guide that demystifies the complexities of IAM, empowering readers to establish robust identity management practices and optimize access controls. With years of experience in the cybersecurity field, Hermans understands the critical role IAM plays in ensuring the confidentiality, integrity, and availability of digital resources. In this book, he shares his expertise, providing a practical roadmap for implementing and managing IAM solutions that align with business goals and industry best practices. Inside *Mastering IAM*, you will:

1. Explore the IAM landscape: Gain a deep understanding of the core concepts, components, and frameworks that form the foundation of IAM. From authentication and authorization to identity governance and federation, master the essential building blocks of a successful IAM strategy.
2. Design and implement IAM solutions: Learn how to design an IAM architecture tailored to your organization's needs, considering factors such as scalability, compliance, and user experience. Follow step-by-step guidelines for deploying IAM solutions, including user provisioning, access controls, single sign-on (SSO), and multi-factor authentication (MFA).
3. Enhance security and compliance: Discover strategies for mitigating security risks and ensuring compliance with relevant regulations. Explore identity lifecycle management, privileged access management (PAM), and security incident response to safeguard against threats and unauthorized access.
4. Leverage IAM for business efficiency: Uncover how IAM can streamline business processes, improve productivity, and enhance user experiences. Explore topics such as self-service portals, role-based access control (RBAC), and integration with other systems to optimize IAM functionality.
5. Address emerging challenges: Stay up to date with the latest trends and emerging technologies shaping the IAM landscape. Learn about cloud-based IAM solutions, IoT device management, and the impact of artificial intelligence and machine learning in enhancing IAM capabilities.

With real-world examples, practical tips, and insightful case studies, *Mastering IAM* equips readers with the knowledge and skills needed to effectively implement and manage IAM solutions. Whether you are an IAM professional, IT manager, or security practitioner, this book will

guide you toward harnessing the full potential of IAM to protect your organization's assets and drive business success. Don't let identity and access management be a barrier to productivity and security. Unleash the power of IAM with Kris Hermans as your trusted guide.

access management gartner magic quadrant: The Effortless Experience Matthew Dixon, Nicholas Toman, Rick DeLisi, 2013-09-12 A new breakthrough idea about how to win customer loyalty from Matthew Dixon, the bestselling author of *The Challenger Sale* Everyone knows that the best way to create customer loyalty is with service so good, so over the top, that it surprises and delights. But what if everyone is wrong? In their acclaimed bestseller *The Challenger Sale*, Matthew Dixon and his colleagues at CEB busted longstanding myths about sales. Now they've turned to a new vital business subject - customer loyalty - with a book that turns conventional wisdom on its head. Companies devote untold time and resources trying to dazzle customers. Yet CEB's careful research proves that is wildly overrated: loyalty has a lot more to do with how well companies deliver on their basic promises than on how dazzling the service experience might be. Forget bells and whistles and just solve your customer's problems. *The Effortless Experience* lays out the four pillars of a low-effort customer experience, with robust data, insights and profiles. Here are tools and templates you can start applying right away to improve service, reduce costs, and ultimately generate the elusive loyalty that the 'dazzle factor' fails to deliver. The rewards are there for the taking, and the pathway to achieving them is now clearly marked. 'A business detective story, in which cherished truths are systematically investigated-and frequently debunked' -Dan Heath, coauthor of *Decisive*, *Switch*, and *Made to Stick* Matt Dixon is Executive Director of the Sales & Service Practice at CEB. He is a frequent contributor to the Harvard Business Review, and his previous book, *The Challenger Sale*, was a Wall Street Journal bestseller. Nick Toman is Senior Director of Research for CEB's Sales & Services Practice and is a frequent contributor to the Harvard Business Review. Rick DeLisi is Senior Director of Advisory Services for CEB's Sales & Service Practice and a noted public speaker and facilitator.

access management gartner magic quadrant: Losing the Cybersecurity War Steve King, 2022-12-07 This book explains the five pillars or battlefields of cybersecurity and how a Zero Trust approach can change the advantage on each battlefield. We have taken a deep dive into each of five battlefields where we have a decided disadvantage due to constitutional structure and moral behavioral guidelines, where we provide examples of how we got here, what we can do about it, why we got here, and how we can avoid these traps in the future. This is a unique viewpoint that has never been explored - the five battlefields include Economics, Technology, Information, Education, and Leadership - and how each has contributed to our current disadvantage on the global stage. We go on to discuss how Zero Trust can change the game to create an advantage for us going forward. The credibility of Zero Trust stems directly from the father of Zero Trust, John Kindervag, who says, "And now, Steve has written a new book on Zero Trust called *Losing the Cybersecurity War: And What We Can Do to Stop It*. It is undeniably the best Zero Trust book yet written. While other writers have focused on implementing Zero Trust from their perspectives, Steve focuses on why Zero Trust is so important on the modern cybersecurity battlefield. His concept of the five cyber battlefields is a great insight that will help us win the cyberwar. By weaving Zero Trust principles throughout these five concepts, Steve demonstrates how the ideas and efforts involved in building Zero Trust environments will lead to a profound shift in terrain advantage. No longer will attackers own the high ground. As defenders and protectors, we can leverage modern technology in a Zero Trust way to keep our data and assets safe from infiltration and exploitation."

access management gartner magic quadrant: Machine Learning Techniques and Analytics for Cloud Security Rajdeep Chakraborty, Anupam Ghosh, Jyotsna Kumar Mandal, 2021-12-21 MACHINE LEARNING TECHNIQUES AND ANALYTICS FOR CLOUD SECURITY This book covers new methods, surveys, case studies, and policy with almost all machine learning techniques and analytics for cloud security solutions The aim of *Machine Learning Techniques and Analytics for Cloud Security* is to integrate machine learning approaches to meet various analytical issues in cloud security. Cloud security with ML has long-standing challenges that require

methodological and theoretical handling. The conventional cryptography approach is less applied in resource-constrained devices. To solve these issues, the machine learning approach may be effectively used in providing security to the vast growing cloud environment. Machine learning algorithms can also be used to meet various cloud security issues, such as effective intrusion detection systems, zero-knowledge authentication systems, measures for passive attacks, protocols design, privacy system designs, applications, and many more. The book also contains case studies/projects outlining how to implement various security features using machine learning algorithms and analytics on existing cloud-based products in public, private and hybrid cloud respectively. Audience Research scholars and industry engineers in computer sciences, electrical and electronics engineering, machine learning, computer security, information technology, and cryptography.

access management gartner magic quadrant: Gartner and the Magic Quadrant Shaun Snapp, 2013-10 If you want to get more out of your Gartner research subscription, this book is for you! Whether you are a software buyer, a large or small vendor, or are wondering how Gartner can help you make better investment decisions, this book will give you new insights to Gartner's research. By studying the methodology behind such popular analytical tools as the Magic Quadrant, you will understand how a vendor earned its rating and whether or not the ratings are justified! Starting with the history of Gartner and how it compares to other IT analyst firms, this book gives a realistic assessment of the value of Gartner research to a company and provides ideas about other resources that could complement Gartner's analysis. You will also have the tools to level the playing field between large, medium and small vendors when using Gartner's analysis in selecting software. By reading this book, you will: Evaluate whether or not a Gartner subscription is of value to your company Adjust the Magic Quadrant to get a more realistic assessment of large and small vendors and their products Increase the value of your interactions with Gartner analysts Understand Gartner's biases and how Gartner makes money, and how this impacts its research results Appreciate the effects of cloud computing on Gartner, and why it matters to you Choose consulting services with confidence Assess the value of Gartner's other analytical products to your business

access management gartner magic quadrant: *CSO*, 2009-07 The business to business trade publication for information and physical Security professionals.

access management gartner magic quadrant: *Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing* Yang, Xiaoyu, 2013-01-31 Innovations in cloud and service-oriented architectures continue to attract attention by offering interesting opportunities for research in scientific communities. Although advancements such as computational power, storage, networking, and infrastructure have aided in making major progress in the implementation and realization of cloud-based systems, there are still significant concerns that need to be taken into account. Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing aims to present insight into Cloud principles, examine associated methods and technologies, and investigate the use of service-oriented computing technologies. In addressing supporting infrastructure of the Cloud, including associated challenges and pressing issues, this reference source aims to present researchers, engineers, and IT professionals with various approaches in Cloud computing.

access management gartner magic quadrant: **Cybersecurity Blue Team Strategies** Kunal Sehgal, Nikolaos Thymianis, 2023-02-28 Build a blue team for efficient cyber threat management in your organization Key Features Explore blue team operations and understand how to detect, prevent, and respond to threats Dive deep into the intricacies of risk assessment and threat management Learn about governance, compliance, regulations, and other best practices for blue team implementation Book Description We've reached a point where all organizational data is connected through some network. With advancements and connectivity comes ever-evolving cyber threats - compromising sensitive data and access to vulnerable systems. Cybersecurity Blue Team Strategies is a comprehensive guide that will help you extend your cybersecurity knowledge and teach you to implement blue teams in your organization from scratch. Through the course of this book, you'll learn defensive cybersecurity measures while thinking from an attacker's perspective.

With this book, you'll be able to test and assess the effectiveness of your organization's cybersecurity posture. No matter the medium your organization has chosen- cloud, on-premises, or hybrid, this book will provide an in-depth understanding of how cyber attackers can penetrate your systems and gain access to sensitive information. Beginning with a brief overview of the importance of a blue team, you'll learn important techniques and best practices a cybersecurity operator or a blue team practitioner should be aware of. By understanding tools, processes, and operations, you'll be equipped with evolving solutions and strategies to overcome cybersecurity challenges and successfully manage cyber threats to avoid adversaries. By the end of this book, you'll have enough exposure to blue team operations and be able to successfully set up a blue team in your organization. What you will learn

- Understand blue team operations and its role in safeguarding businesses
- Explore everyday blue team functions and tools used by them
- Become acquainted with risk assessment and management from a blue team perspective
- Discover the making of effective defense strategies and their operations
- Find out what makes a good governance program
- Become familiar with preventive and detective controls for minimizing risk

Who this book is for This book is for cybersecurity professionals involved in defending an organization's systems and assets against attacks. Penetration testers, cybersecurity analysts, security leaders, security strategists, and blue team members will find this book helpful. Chief Information Security Officers (CISOs) looking at securing their organizations from adversaries will also benefit from this book. To get the most out of this book, basic knowledge of IT security is recommended.

access management gartner magic quadrant: Wolf in Cio's Clothing Tina Nunno, 2016-09-19 Machiavellians are few in number in IT. The massive pressure on CIOs continues to increase as the opportunities to use technology in business become more prevalent and more competitive. As CIOs often find themselves at the center of business conflict, they must not only familiarize themselves with Machiavellian tactics as a defensive weapon, but also learn to use them as an offensive weapon in extreme situations so that they can increase IT's contribution to their enterprises. As Italian political philosopher Niccolo Machiavelli implied, you're either predator or prey, and the animal you most resemble determines your position on the food chain. In *The Wolf in CIO's Clothing* Gartner analyst and author Tina Nunno expands on Machiavelli's metaphor, examining seven animal types and the leadership attributes of each. Nunno posits the wolf -- a social animal with strong predatory instincts -- as the ideal example of how a leader can adapt and thrive. Technology may be black and white, but successful leadership demands an ability to exist in the grey. Drawing on her experience with hundreds of CIOs, Nunno charts a viable way to master the Machiavellian principles of power, manipulation, love, and war. Through compelling case studies, her approach demonstrates how CIOs and IT leaders can adjust their leadership styles in extreme situations for their own success and that of their teams.

access management gartner magic quadrant: Continuous API Management Mehdi Medjaoui, Erik Wilde, Ronnie Mitra, Mike Amundsen, 2018-11-14 A lot of work is required to release an API, but the effort doesn't always pay off. Overplanning before an API matures is a wasted investment, while underplanning can lead to disaster. This practical guide provides maturity models for individual APIs and multi-API landscapes to help you invest the right human and company resources for the right maturity level at the right time. How do you balance the desire for agility and speed with the need for robust and scalable operations? Four experts from the API Academy show software architects, program directors, and product owners how to maximize the value of their APIs by managing them as products through a continuous life cycle. Learn which API decisions you need to govern and how and where to do so Design, deploy, and manage APIs using an API-as-a-product (AaaP) approach Examine ten pillars that form the foundation of API product work Learn how the continuous improvement model governs changes throughout an API's lifetime Explore the five stages of a complete API product life cycle Delve into team roles needed to design, build, and maintain your APIs Learn how to manage your API landscape—the set of APIs published by your organization

access management gartner magic quadrant: IT-Governance in der Praxis Andreas Rüter, Jürgen Schröder, Axel Göldner, Jens Niebuhr, 2010-06-09 Die Autoren adressieren die

Sandwich-Position, in der sich die IT heute in vielen größeren Unternehmen befindet: Zum einen der Druck, Governance-Anforderungen wie Sarbanes-Oxley oder Compliance-Anforderungen abdecken zu müssen, und zugleich der Druck, die Kosten weiter reduzieren zu müssen. Zum anderen steht dem der eigene Anspruch entgegen, sich als innovativer Dienstleister aufzustellen, der im Verbund mit den Fachbereichen die Prozesskompetenz besitzt. Dieses Buch erläutert die Herausforderungen an die IT und zeigt anhand konkreter Praxisbeispiele effektive Wege auf, wie die IT Governance des Unternehmens ausgestaltet werden kann. Es richtet sich an die Lenker der IT, aber auch an das Management aus Finanzbereich oder Unternehmens- und Organisations-Entwicklung. In der zweiten Auflage wurden die Themen IT-Compliance und ihre Prüfung sowie Sicherheit in der IT ergänzt. Handlungsempfehlungen und eine Checkliste, erstellt für den Praktiker, runden dieses Fachbuch ab.

access management gartner magic quadrant: A CISO Guide to Cyber Resilience Debra Baker, 2024-04-30 Explore expert strategies to master cyber resilience as a CISO, ensuring your organization's security program stands strong against evolving threats Key Features Unlock expert insights into building robust cybersecurity programs Benefit from guidance tailored to CISOs and establish resilient security and compliance programs Stay ahead with the latest advancements in cyber defense and risk management including AI integration Purchase of the print or Kindle book includes a free PDF eBook Book Description This book, written by the CEO of TrustedCISO with 30+ years of experience, guides CISOs in fortifying organizational defenses and safeguarding sensitive data. Analyze a ransomware attack on a fictional company, BigCo, and learn fundamental security policies and controls. With its help, you'll gain actionable skills and insights suitable for various expertise levels, from basic to intermediate. You'll also explore advanced concepts such as zero-trust, managed detection and response, security baselines, data and asset classification, and the integration of AI and cybersecurity. By the end, you'll be equipped to build, manage, and improve a resilient cybersecurity program, ensuring your organization remains protected against evolving threats. What you will learn Defend against cybersecurity attacks and expedite the recovery process Protect your network from ransomware and phishing Understand products required to lower cyber risk Establish and maintain vital offline backups for ransomware recovery Understand the importance of regular patching and vulnerability prioritization Set up security awareness training Create and integrate security policies into organizational processes Who this book is for This book is for new CISOs, directors of cybersecurity, directors of information security, aspiring CISOs, and individuals who want to learn how to build a resilient cybersecurity program. A basic understanding of cybersecurity concepts is required.

access management gartner magic quadrant: The Social Organization Anthony J. Bradley, Mark P. McDonald, 2011-09-27 As a leader, it's your job to extract maximum talent, energy, knowledge, and innovation from your customers and employees. But how? In *The Social Organization*, two of Gartner's lead analysts strongly advocate exploiting social technology. The authors share insights from their study of successes and failures at more than four hundred organizations that have used social technologies to foster—and capitalize on—customers' and employees' collective efforts. But the new social technology landscape isn't about the technology. It's about building communities, fostering new ways of collaborating, and guiding these efforts to achieve a purpose. To that end, the authors identify the core disciplines managers must master to translate community collaboration into otherwise impossible results:

- Vision: defining a compelling vision of progress toward a highly collaborative organization.
- Strategy: taking community collaboration from risky and random success to measurable business value.
- Purpose: rallying people around a clear purpose, not just providing technology.
- Launch: creating a collaborative environment and gaining adoption.
- Guide: participating in and influencing communities without stifling collaboration.
- Adapt: responding creatively to change in order to better support community collaboration.

The Social Organization highlights the benefits and challenges of using social technology to tap the power of people, revealing what managers must do to make collaboration a source of enduring competitive advantage.

access management gartner magic quadrant: The New Normal in IT Gregory S. Smith,

2022-02-23 Learn how IT leaders are adapting to the new reality of life during and after COVID-19. COVID-19 has caused fundamental shifts in attitudes around remote and office work. And in *The New Normal in IT: How the Global Pandemic Changed Information Technology Forever*, internationally renowned IT executive Gregory S. Smith explains how and why companies today are shedding corporate office locations and reducing office footprints. You'll learn about how companies realized the value of information technology and a distributed workforce and what that means for IT professionals going forward. The book offers insightful lessons regarding: How to best take advantage of remote collaboration and hybrid remote/office workforces How to implement updated risk mitigation strategies and disaster recovery planning and testing to shield your organization from worst case scenarios How today's CIOs and CTOs adapt their IT governance frameworks to meet new challenges, including cybersecurity risks *The New Normal in IT* is an indispensable resource for IT professionals, executives, graduate technology management students, and managers in any industry. It's also a must-read for anyone interested in the impact that COVID-19 had, and continues to have, on the information technology industry.

access management gartner magic quadrant: Handbook of Research on Knowledge-Intensive Organizations Jemielniak, Dariusz, Kociatkiewicz, Jerzy, 2009-03-31 Provides an international collection of studies on knowledge-intensive organizations with insight into organizational realities as varied as universities, consulting agencies, corporations, and high-tech start-ups.

access management gartner magic quadrant: AWS for Solutions Architects Saurabh Shrivastava, Neelanjali Srivastav, Alberto Artasanchez, Imtiaz Sayed, Dr. Siddhartha Choubey Ph.D, 2023-04-28 Become a master Solutions Architect with this comprehensive guide, featuring cloud design patterns and real-world solutions for building scalable, secure, and highly available systems. Purchase of the print or Kindle book includes a free eBook in PDF format. Key Features Gain expertise in automating, networking, migrating, and adopting cloud technologies using AWS Use streaming analytics, big data, AI/ML, IoT, quantum computing, and blockchain to transform your business Upskill yourself as an AWS solutions architect and explore details of the new AWS certification Book Description Are you excited to harness the power of AWS and unlock endless possibilities for your business? Look no further than the second edition of *AWS for Solutions Architects*! Packed with all-new content, this book is a must-have guide for anyone looking to build scalable cloud solutions and drive digital transformation using AWS. This updated edition offers in-depth guidance for building cloud solutions using AWS. It provides detailed information on AWS well-architected design pillars and cloud-native design patterns. You'll learn about networking in AWS, big data and streaming data processing, CloudOps, and emerging technologies such as machine learning, IoT, and blockchain. Additionally, the book includes new sections on storage in AWS, containers with ECS and EKS, and data lake patterns, providing you with valuable insights into designing industry-standard AWS architectures that meet your organization's technological and business requirements. Whether you're an experienced solutions architect or just getting started with AWS, this book has everything you need to confidently build cloud-native workloads and enterprise solutions. What you will learn Optimize your Cloud Workload using the AWS Well-Architected Framework Learn methods to migrate your workload using the AWS Cloud Adoption Framework Apply cloud automation at various layers of application workload to increase efficiency Build a landing zone in AWS and hybrid cloud setups with deep networking techniques Select reference architectures for business scenarios, like data lakes, containers, and serverless apps Apply emerging technologies in your architecture, including AI/ML, IoT and blockchain Who this book is for This book is for application and enterprise architects, developers, and operations engineers who want to become well versed with AWS architectural patterns, best practices, and advanced techniques to build scalable, secure, highly available, highly tolerant, and cost-effective solutions in the cloud. Existing AWS users are bound to learn the most, but it will also help those curious about how leveraging AWS can benefit their organization. Prior knowledge of any computing language is not needed, and there's little to no code. Prior experience in software architecture

design will prove helpful.

access management gartner magic quadrant: Information Technology for Management Efraim Turban, Carol Pollard, Gregory R. Wood, 2021 Information Technology for Management provides students with a comprehensive understanding of the latest technological developments in IT and the critical drivers of business performance, growth, and sustainability. Integrating feedback from IT managers and practitioners from top-level organizations worldwide, the International Adaptation of this well-regarded textbook features thoroughly revised content throughout to present students with a realistic, up-to-date view of IT management in the current business environment. This text covers the latest developments in the real world of IT management with the addition of new case studies that are contemporary and more relevant to the global scenario. It offers a flexible, student-friendly presentation of the material through a pedagogy that is designed to help students easily comprehend and retain information. There is new and expanded coverage of Artificial Intelligence, Robotics, Quantum Computing, Blockchain Technology, IP Intelligence, Big Data Analytics, IT Service Management, DevOps, etc. It helps readers learn how IT is leveraged to reshape enterprises, engage and retain customers, optimize systems and processes, manage business relationships and projects, and more.

access management gartner magic quadrant: ,

access management gartner magic quadrant: Enterprise Integration Patterns Gregor Hohpe, Bobby Woolf, 2012-03-09 Enterprise Integration Patterns provides an invaluable catalog of sixty-five patterns, with real-world solutions that demonstrate the formidable of messaging and help you to design effective messaging solutions for your enterprise. The authors also include examples covering a variety of different integration technologies, such as JMS, MSMQ, TIBCO ActiveEnterprise, Microsoft BizTalk, SOAP, and XSL. A case study describing a bond trading system illustrates the patterns in practice, and the book offers a look at emerging standards, as well as insights into what the future of enterprise integration might hold. This book provides a consistent vocabulary and visual notation framework to describe large-scale integration solutions across many technologies. It also explores in detail the advantages and limitations of asynchronous messaging architectures. The authors present practical advice on designing code that connects an application to a messaging system, and provide extensive information to help you determine when to send a message, how to route it to the proper destination, and how to monitor the health of a messaging system. If you want to know how to manage, monitor, and maintain a messaging system once it is in use, get this book.

access management gartner magic quadrant: Asset Management Excellence John D. Campbell, Andrew K.S. Jardine, Joel McGlynn, 2016-04-19 During the eight years since the publication of Maintenance Excellence: Optimizing Equipment Life-Cycle Decisions the business environment has changed drastically. Globalization, consolidation, and changes in technology challenge asset management and maintenance professionals to be more efficient. Globalization and consolidation have been particula

access management gartner magic quadrant: APM Best Practices Michael J. Sydor, Karen Sleeth, Jon Toigo, Ed Yourdon, Scott E. Donaldson, Stanley G. Siegel, Gary Donaldson, 2011-08-22 The objective of APM Best Practices: Realizing Application Performance Management is to establish reliable application performance management (APM) practices—to demonstrate value, to do it quickly, and to adapt to the client circumstances. It's important to balance long-term goals with short-term deliverables, but without compromising usefulness or correctness. The successful strategy is to establish a few reasonable goals, achieve them quickly, and then iterate over the same topics two more times, with each successive iteration expanding the skills and capabilities of the APM team. This strategy is referred to as "Good, Better, Best". The application performance monitoring marketplace is very focused on ease of installation, rapid time to usefulness, and overall ease of use. But these worthy platitudes do not really address the application performance management processes that ensure that you will deploy effectively, synergize on quality assurance test plans, triage accurately, and encourage collaboration across the application life cycle that

ultimately lowers overall application cost and ensures a quality user experience. These are also fine platitudes but these are the ones that are of interest to your application sponsors. These are the ones for which you need to show value. This CA Press book employs this iterative approach, adapted pragmatically for the realities of your organizational and operational constraints, to realize a future state that your sponsors will find useful, predictable and manageable—and something that they will want to fund. In the meantime, you will learn the useful techniques needed to set up and maintain a useful performance management system utilizing best practices regardless of the software provider(s).

access management gartner magic quadrant: Asset Attack Vectors Morey J. Haber, Brad Hibbert, 2018-06-15 Build an effective vulnerability management strategy to protect your organization's assets, applications, and data. Today's network environments are dynamic, requiring multiple defenses to mitigate vulnerabilities and stop data breaches. In the modern enterprise, everything connected to the network is a target. Attack surfaces are rapidly expanding to include not only traditional servers and desktops, but also routers, printers, cameras, and other IOT devices. It doesn't matter whether an organization uses LAN, WAN, wireless, or even a modern PAN—savvy criminals have more potential entry points than ever before. To stay ahead of these threats, IT and security leaders must be aware of exposures and understand their potential impact. Asset Attack Vectors will help you build a vulnerability management program designed to work in the modern threat environment. Drawing on years of combined experience, the authors detail the latest techniques for threat analysis, risk measurement, and regulatory reporting. They also outline practical service level agreements (SLAs) for vulnerability management and patch management. Vulnerability management needs to be more than a compliance check box; it should be the foundation of your organization's cybersecurity strategy. Read Asset Attack Vectors to get ahead of threats and protect your organization with an effective asset protection strategy. What You'll Learn Create comprehensive assessment and risk identification policies and procedures Implement a complete vulnerability management workflow in nine easy steps Understand the implications of active, dormant, and carrier vulnerability states Develop, deploy, and maintain custom and commercial vulnerability management programs Discover the best strategies for vulnerability remediation, mitigation, and removal Automate credentialed scans that leverage least-privilege access principles Read real-world case studies that share successful strategies and reveal potential pitfalls Who This Book Is For New and intermediate security management professionals, auditors, and information technology staff looking to build an effective vulnerability management program and defend against asset based cyberattacks

access management gartner magic quadrant: Integrating a Usable Security Protocol into User Authentication Services Design Process Christina Braz, Ahmed Seffah, Bilal Naqvi, 2018-11-08 There is an intrinsic conflict between creating secure systems and usable systems. But usability and security can be made synergistic by providing requirements and design tools with specific usable security principles earlier in the requirements and design phase. In certain situations, it is possible to increase usability and security by revisiting design decisions made in the past; in others, to align security and usability by changing the regulatory environment in which the computers operate. This book addresses creation of a usable security protocol for user authentication as a natural outcome of the requirements and design phase of the authentication method development life cycle.

access management gartner magic quadrant: Hyperautomation Matt Calkins, Neil Ward-Dutton, George Westerman, Lakshmi N, Sidney Fernandes, Alice Wei, Chris Skinner, Isaac Sacolick, John Rymer, Lisa Heneghan, Darren Blake, Rob Galbraith, Ron Tolido, Michael Beckley, 2020-11-20 HYPERAUTOMATION is a collection of expert essays on low-code development and the future of business process automation. In each chapter, an academic, analyst, implementer, or end-user examines different aspects of low-code and automation in the enterprise, clarifying both value and barriers through personal experiences and insights. With contributions from: Dr. George Westerman, MIT - Neil Ward-Dutton, IDC - Lakshmi N, Tata Consultancy Services - Sidney Fernandes & Alice Wei, University of South Florida - Lisa Heneghan, KPMG - Chris Skinner, FinTech

expert - John R. Rymer, Forrester (Emeritus) - Isaac Sacolick, StarCIO - Darren Blake, Bexley Neighbourhood Care - Rob Galbraith, InsureTech expert - Ron Tolido, Capgemini - Michael Beckley, Appian All proceeds from the sale of this book will be donated to Black Girls Code, an organization providing young girls of color opportunities to learn in-demand skills in technology and computer programming.

access management gartner magic quadrant: Supply Chain Management: Concepts, Methodologies, Tools, and Applications Management Association, Information Resources, 2012-12-31 In order to keep up with the constant changes in technology, business have adopted supply chain management to improve competitive strategies on a strategic and operational level. Supply Chain Management: Concepts, Methodologies, Tools, and Applications is a reference collection which highlights the major concepts and issues in the application and advancement of supply chain management. Including research from leading scholars, this resource will be useful for academics, students, and practitioners interested in the continuous study of supply chain management and its influences.

access management gartner magic quadrant: Product Information Management Jorij Abraham, 2014-05-05 Product Information Management is the latest topic that companies across the world are deliberating upon. As companies sell online, they are confronted with the fact that not all information necessary to sell their products is available. Where marketing, sales and finance have been core processes of the corporate world for a long time, PIM is a new business process with its own unique implementation and management challenges. The book describes the core PIM processes; their strategic, tactical and operational benefits and implementation challenges. The book has been written for managers, business users as well as students, and illustrates the different concepts with practical cases from companies like Coca Cola, Nikon and Thomas Cook.

Additional Resources

Magic Quadrant for Privileged Access Management - MI2

Gartner defines privileged access management (PAM) as tools that manage and protect accounts, credentials and commands that offer an elevated level of technical access, that is, ...

Recognized in Gartner Peer Insights "Voice of the Customer": ...

Access management (AM) applies to technologies that use access control engines to provide centralized authentication, single sign-on (SSO), session management and authorization ...

Access Management Gartner Magic Quadrant (2024) - x ...

Access Management Gartner Magic Quadrant: Identity Attack Vectors Morey J. Haber,Darran Rolls,2019-12-17 Discover how poor identity and privilege management can be leveraged to ...

Devolutions Listed in Gartner's Magic Quadrant for Privileged ...

Gartner analysts state that "privileged access management is one of the most critical security controls, particularly in today's increasingly complex IT environment. Security and risk ...

Magic Quadrant for Privileged Access Management

Magic Quadrant for Privileged Access Management. ARCON is a Challenger in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Magic Quadrant for Identity Governance and Administration

This Magic Quadrant covers all the common use cases for IGA. It includes vendors that offer the basic functions listed above and have at least 1% of Gartner's estimated market share or ...

Gartner Magic Quadrant Access Management Leader

Access management has become the source of trust for identity-first security. Increased dependence on identities for access anywhere, anytime, requires AM to be more reliable and ...

Critical Capabilities for Identity and Access Management as a ...

Use this document alongside the companion Magic Quadrant to aid IDaaS selection decisions and identify key differentiators among services.

WALLIX NAMED A LEADER IN THE 2022 MAGIC QUADRANT ...

Jul 25, 2022 · 2022 Magic Quadrant™ for Privileged Access Management Magic Quadrant™ reports are a culmination of rigorous, fact-based research in specific markets, providing a wide ...

Magic Quadrant for Privileged Access Management

Gartner defines the privileged access management (PAM) market as a foundational security technology to protect accounts, credentials and operations that offer an elevated ("privileged") ...

Access Management Magic Quadrant (2024) - x-plane.com

The concept of an "access management magic quadrant" isn't a formally defined quadrant from a specific analyst firm like Gartner or Forrester. Instead, it's a metaphorical representation of the ...

2022 Gartner Magic Quadrant For Privileged Access ...

The 2022 Gartner Magic Quadrant for Privileged Access Management categorized vendors into four quadrants: Leaders, Challengers, Visionaries, and Niche Players. [Insert a table here ...

Magic Quadrant for Identity Governance and Administration

Feb 21, 2018 · Security and risk management leaders responsible for identity and access management (IAM) must ensure that only the right people get access to the right resources ...

Access Management Gartner Magic Quadrant (2024) - x ...

Gartner's methodology for creating the Access Management Gartner Magic Quadrant is rigorous and multi-faceted. It involves a comprehensive assessment of vendors based on two primary ...

Magic Quadrant for Identity and Access Management as a ...

This Magic Quadrant rates vendors on their abilities to be global, general purpose identity and access management (IAM) service providers for multiple use cases. The vendors in this Magic ...

Mag i c Quad rant f o r Manag e d N e two rk S e rv i c e s

Managed LAN services (MNS for LAN) must include the management of enterprise

LAN customer premises equipment (CPE), such as campus switches and wireless access points. It provides ...

Magic Quadrant for Privileged Access Management

ARCON is a Leader in this Magic Quadrant, ARCON was established in 2006 in London, and is now based out of Mumbai, India. ARCON's PASM functionality is provided by the ...

eMudhra is Recognized with an Honorable Mention in ...

Magic Quadrant for Access Management is market-specific research done by Gartner to provide industry experts with a wide-angle view of competitor positions. The research is based on ...

Magic Quadrant for Privileged Access Management

Dec 3, 2018 · By 2022, more than half of enterprises using privileged access management (PAM) tools will emphasize just-in-time privileged access over long-term privileged access, up from ...

Magic Quadrant for Privileged Access Management - MI2

Gartner defines privileged access management (PAM) as tools that manage and protect accounts, credentials and commands that offer an elevated level of technical access, that is, ...

Recognized in Gartner Peer Insights "Voice of the Customer": ...

Access management (AM) applies to technologies that use access control engines to provide centralized authentication, single sign-on (SSO), session management and authorization ...

2020 GARTNER MAGIC QUADRANT FOR PRIVILEGED ...

Gartner Magic Quadrants are among the most anticipated research findings of the year, released in different categories from the esteemed IT consulting firm Gartner. No matter the specific ...

Access Management Gartner Magic Quadrant (2024) - x ...

Access Management Gartner Magic Quadrant: Identity Attack Vectors Morey J. Haber,Darran Rolls,2019-12-17 Discover how poor identity and privilege management can be leveraged to ...

Devolutions Listed in Gartner's Magic Quadrant for ...

Gartner analysts state that "privileged access management is one of the most critical security controls, particularly in today's increasingly complex IT environment. Security and risk ...

Magic Quadrant for Privileged Access Management

Magic Quadrant for Privileged Access Management. ARCON is a Challenger in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Magic Quadrant for Identity Governance and Administration ...

This Magic Quadrant covers all the common use cases for IGA. It includes vendors that offer the basic functions listed above and have at least 1% of

Gartner's estimated market share or ...

Garnter Magic Quadrant Access Management Leader

Access management has become the source of trust for identity-first security. Increased dependence on identities for access anywhere, anytime, requires AM to be more reliable and ...

Critical Capabilities for Identity and Access Management ...

Use this document alongside the companion Magic Quadrant to aid IDaaS selection decisions and identify key differentiators among services.

WALLIX NAMED A LEADER IN THE 2022 MAGIC QUADRANT ...

Jul 25, 2022 · 2022 Magic Quadrant™ for Privileged Access Management Magic Quadrant™ reports are a culmination of rigorous, fact-based research in specific markets, providing a wide ...

Magic Quadrant for Privileged Access Management

Gartner defines the privileged access management (PAM) market as a foundational security technology to protect accounts, credentials and operations that offer an elevated ("privileged") ...

Access Management Magic Quadrant (2024) - x-plane.com

The concept of an "access management magic quadrant" isn't a formally defined quadrant from a specific analyst firm like Gartner or Forrester. Instead, it's a metaphorical representation of the ...

2022 Gartner Magic Quadrant For Privileged Access ...

The 2022 Gartner Magic Quadrant for Privileged Access Management categorized vendors into four quadrants: Leaders, Challengers, Visionaries, and Niche Players. [Insert a table here ...

Magic Quadrant for Identity Governance and ...

Feb 21, 2018 · Security and risk management leaders responsible for identity and access management (IAM) must ensure that only the right people get access to the right resources ...

Access Management Gartner Magic Quadrant (2024) - x ...

Gartner's methodology for creating the Access Management Gartner Magic Quadrant is rigorous and multi-faceted. It involves a comprehensive assessment of vendors based on two primary ...

Magic Quadrant for Identity and Access Management as a ...

This Magic Quadrant rates vendors on their abilities to be global, general purpose identity and access management (IAM) service providers for multiple use cases. The vendors in this Magic ...

Mag i c Quad rant f o r Manag e d N e two rk S e rv i c e s

Managed LAN services (MNS for LAN) must include the management of enterprise LAN customer premises equipment (CPE), such as campus switches and wireless access points. It provides ...

Magic Quadrant for Privileged Access Management

ARCON is a Leader in this Magic Quadrant, ARCON was established in 2006 in London, and is now based out of Mumbai, India. ARCON's PASM functionality is provided by the ...

eMudhra is Recognized with an Honorable Mention in ...

Magic Quadrant for Access Management is market-specific research done by Gartner to provide industry experts with a wide-angle view of competitor positions. The research is based on ...

Magic Quadrant for Privileged Access Management

Dec 3, 2018 · By 2022, more than half of enterprises using privileged access management (PAM) tools will emphasize just-in-time privileged access over long-term privileged access, up from ...

[Access Management Gartner Magic Quadrant](#)

Access Management Gartner Magic Quadrant

Related Articles

- [access control system training](#)
- [accounting crossword puzzle answers](#)
- [accounting bdo italian italia](#)

[Back to Home](#)