gartner email security market guide

Gartner Email Security Market Guide: Navigating the Evolving Landscape of Email Protection

gartner email security market guide serves as an essential compass for businesses and IT professionals looking to enhance their email security posture in today's increasingly complex threat environment. Email remains the primary communication method for enterprises worldwide, but it's also one of the most exploited attack vectors by cybercriminals. Understanding the insights and recommendations from Gartner's market guide can empower organizations to select the right email security solutions that align with their unique needs and evolving cybersecurity challenges.

Understanding the Gartner Email Security Market Guide

Gartner's market guides are well-respected industry resources that provide an objective overview of technology markets, vendor landscapes, and emerging trends. The Gartner email security market guide specifically focuses on the various solutions available to protect email infrastructures from threats such as phishing, malware, spam, business email compromise (BEC), and data leaks.

Rather than ranking vendors like a magic quadrant, the market guide offers a comprehensive landscape view, highlighting the strengths, capabilities, and potential gaps in different email security offerings. This helps decision-makers evaluate tools based on criteria such as threat detection efficacy, integration capabilities, deployment models, and cost-effectiveness.

Key Components Covered in the Market Guide

The guide typically covers multiple aspects that influence how organizations should approach email security:

- **Threat Landscape Analysis:** An overview of the evolving email-based threats including ransomware, advanced phishing techniques, and social engineering.
- **Solution Types:** Insights into cloud-based email security, on-premises appliances, and hybrid models, helping businesses choose deployment strategies.
- **Feature Set Evaluation:** Assessment of critical functions like sandboxing, URL rewriting, attachment scanning, and email encryption.
- **Vendor Capabilities:** Profiles of leading vendors, highlighting their unique selling points and areas of specialization.
- **Market Trends:** Emerging technologies such as AI-driven threat detection, automated incident response, and integration with broader security ecosystems.

Why Email Security Is More Crucial Than Ever

Email remains the frontline for cyberattacks, making robust protection a non-negotiable part of any organization’s cybersecurity strategy. According to Gartner’s research, email attacks are not only increasing in volume but also becoming more sophisticated. Threat actors employ tactics like spear-phishing, impersonation, and zero-day malware to bypass traditional defenses.

The Rising Threats in Email Communication

Cybercriminals are continuously refining their techniques. Here are some common threats that the Gartner email security market guide highlights:

- **Phishing and Spear-Phishing:** Targeted emails designed to trick recipients into revealing sensitive data or credentials.
- **Business Email Compromise (BEC):** Fraud schemes where attackers impersonate executives or trusted contacts to authorize fraudulent transactions.
- **Malware and Ransomware Delivery:** Malicious attachments or links that install harmful software on the victim’s device.
- **Spam and Unsolicited Content:** While less dangerous, spam can clutter inboxes and sometimes serve as a delivery mechanism for more serious threats.
- **Data Leakage and Compliance Risks:** Unauthorized sharing of sensitive business information via email.

These threats underscore why relying on basic spam filters or antivirus programs is no longer sufficient.

Choosing the Right Email Security Solution: Insights from the Gartner Email Security Market Guide

With so many vendors and technologies available, selecting the best email security solution can be overwhelming. The Gartner email security market guide provides valuable frameworks and criteria to streamline this process.

Evaluating Deployment Models

One of the first decisions organizations face is whether to adopt cloud-based, on-premises, or hybrid email security solutions. The market guide explains the pros and cons of each:

- **Cloud-based Solutions:** Offer scalability, ease of management, and often faster updates to counter new threats. Ideal for organizations embracing cloud-first strategies.
- **On-Premises Appliances:** Provide greater control over data and customization but require more internal resources and maintenance.
- **Hybrid Models:** Combine the benefits of both, allowing flexibility and incremental migration to the cloud.

Essential Features to Look For

The guide emphasizes that beyond deployment, the effectiveness of an email security tool depends on its capabilities. Key features include:

- **Advanced Threat Protection:** Real-time scanning for malware, sandboxing suspicious attachments, and URL analysis.
- **Anti-Phishing Technologies:** Machine learning algorithms that detect subtle signs of phishing and impersonation attempts.
- **Email Encryption:** Protecting sensitive communications from interception and unauthorized access.
- **Data Loss Prevention (DLP):** Preventing accidental or malicious data leaks through policy enforcement and content inspection.
- **Integration with SIEM and SOAR:** Enabling automated incident response and comprehensive threat visibility.
- **User Awareness and Reporting:** Tools to educate employees and streamline reporting of suspicious emails.

Vendor Landscape and Selection Tips

Gartner identifies a range of vendors offering specialized email security solutions, from established cybersecurity giants to innovative startups. When evaluating providers, consider:

- **Threat Intelligence Quality:** Does the vendor leverage global threat intelligence feeds and AI-driven analytics?
- **Ease of Deployment and Management:** How quickly can the solution be implemented and maintained?
- **Scalability:** Can the solution grow with your organization’s needs?
- **Customer Support and SLAs:** What level of support and guaranteed uptime does the vendor provide?
- **Compliance Support:** Does the product help meet industry-specific regulations such as GDPR, HIPAA, or PCI DSS?

Engaging with Gartner’s market guide not only highlights these considerations but also helps avoid common pitfalls like vendor lock-in or overpaying for features that aren’t essential.

Emerging Trends in Email Security Highlighted by Gartner

The email security landscape is dynamic, with new challenges and technologies constantly shaping the market. Gartner’s insights shed light on some key trends shaping future email protection strategies.

Artificial Intelligence and Machine Learning

AI-driven detection is becoming a game-changer in identifying sophisticated phishing attempts and novel malware strains. By analyzing behavioral patterns and anomalies, these technologies can spot threats that traditional signature-based methods miss.

Automation and Orchestration

Automated response workflows integrated with security orchestration, automation, and response (SOAR) platforms help reduce the time between detection and mitigation. This accelerates incident handling and lowers the burden on security teams.

Zero Trust and Identity Protection

Applying zero trust principles to email security means verifying every email’s origin and content before granting access or executing actions. This approach also involves integrating identity

verification and multifactor authentication to combat impersonation.

Cloud-Native Security Platforms

As organizations migrate their email infrastructure to cloud services like Microsoft 365 and Google Workspace, email security vendors are developing cloud-native solutions that seamlessly integrate with these platforms, offering better protection and user experience.

Implementing Best Practices Based on the Gartner Email Security Market Guide

Beyond technology selection, Gartner emphasizes the importance of comprehensive strategies that combine tools, processes, and people.

- **Regularly Update Security Policies:** Ensure email security policies evolve with emerging threats and business changes.
- **Employee Training:** Conduct ongoing phishing awareness and cybersecurity education to empower users as the first line of defense.
- **Continuous Monitoring and Analytics:** Implement monitoring solutions to detect anomalies and potential breaches swiftly.
- **Incident Response Planning:** Develop clear procedures for responding to email-related security incidents.
- **Leverage Threat Intelligence:** Use up-to-date threat intelligence to tune security tools and anticipate new attack vectors.

By combining these best practices with insights from the Gartner email security market guide, organizations can build a resilient email defense posture that adapts to changing risks.

Navigating the email security market can be complex, but with resources like the Gartner email security market guide, businesses gain a clearer understanding of the options and innovations available. By leveraging these insights and aligning email security investments with organizational priorities, companies can better protect their communications, data, and reputation against the persistent threats lurking in today’s digital inboxes.

Frequently Asked Questions

What is the Gartner Email Security Market Guide?

The Gartner Email Security Market Guide is a research report published by Gartner that provides an overview of key vendors, trends, and best practices in the email security market to help organizations make informed decisions.

Why is the Gartner Email Security Market Guide important for businesses?

The guide helps businesses understand the current email security landscape, assess vendor capabilities, and select the most suitable email security solutions to protect against phishing, malware, and other email-based threats.

What key trends does the Gartner Email Security Market Guide highlight?

The guide highlights trends such as the increasing use of AI and machine learning for threat detection, the rise of cloud-based email security solutions, and the growing importance of protecting against advanced phishing attacks and business email compromise.

How does Gartner evaluate vendors in the Email Security Market Guide?

Gartner evaluates vendors based on criteria such as product capabilities, deployment options, threat intelligence integration, ease of management, and overall market presence to provide a comprehensive overview of their strengths and weaknesses.

Can the Gartner Email Security Market Guide help with compliance requirements?

Yes, the guide includes information on how different email security solutions support compliance with regulations like GDPR, HIPAA, and others, helping organizations choose solutions that meet their regulatory needs.

How often is the Gartner Email Security Market Guide updated?

Gartner typically updates the Email Security Market Guide annually or as significant market changes occur to ensure the information remains current and relevant for decision-makers.

Where can organizations access the Gartner Email Security

Market Guide?

Organizations can access the Gartner Email Security Market Guide through Gartner's official website, often requiring a subscription or purchase, or via authorized partners and vendors who share the report for marketing purposes.

Additional Resources

Gartner Email Security Market Guide: Navigating the Complex Landscape of Cyber Defense

gartner email security market guide serves as a vital resource for organizations striving to protect their email infrastructures from an increasingly sophisticated array of cyber threats. As email remains one of the primary attack vectors for malware, phishing, and data breaches, enterprises must rely on comprehensive and well-analyzed market intelligence to identify robust email security solutions. Gartner’s guide offers a systematic overview of current vendors, technologies, and industry trends, assisting security professionals in making informed decisions amid a rapidly evolving threat landscape.

Understanding the Gartner Email Security Market Guide

The Gartner Email Security Market Guide stands out as an authoritative document that evaluates the email security ecosystem. Rather than being a traditional Magic Quadrant or a vendor ranking report, the guide functions as an analytical overview providing insights into market dynamics, solution categories, and vendor capabilities. By dissecting the strengths and limitations of various offerings, the guide helps organizations match their specific security requirements with suitable products and services.

In recent years, the email security domain has expanded beyond basic spam filtering and antivirus capabilities. Advanced persistent threats, Business Email Compromise (BEC), and sophisticated phishing campaigns have necessitated multi-layered defenses incorporating artificial intelligence, behavioral analytics, and cloud-native architectures. Gartner’s guide captures these trends, highlighting how modern email security platforms integrate threat intelligence feeds, sandboxing, and encryption features to enhance protection.

Key Features and Functionalities Analyzed in the Guide

Central to the Gartner Email Security Market Guide is the comprehensive analysis of functional capabilities that define effective email security solutions. These features typically include:

- **Spam and Malware Filtering:** The foundational layer that filters out unsolicited emails and known malware signatures.
- **Phishing Detection and Prevention:** Advanced heuristics and machine learning models to

identify deceptive attempts, including spear-phishing.

- **Business Email Compromise Protection:** Specialized controls to detect and prevent fraudulent email activity targeting financial or confidential operations.
- **Data Loss Prevention (DLP):** Mechanisms to prevent sensitive information from leaving the organization via email.
- **Encryption and Secure Email Gateways:** Ensuring confidentiality and integrity of email communication through encryption standards.
- **Integration with Security Information and Event Management (SIEM):** Allowing for streamlined incident detection and response.
- **Cloud-based vs. On-premises Deployment:** Flexibility in deployment models to accommodate different organizational architectures.

These features are evaluated with respect to how vendors implement them, their efficacy, scalability, and ease of management.

Market Trends and Vendor Landscape

The Gartner Email Security Market Guide underscores a significant shift toward cloud-based email security solutions, driven by the widespread adoption of cloud email platforms such as Microsoft 365 and Google Workspace. Cloud-native email security services offer scalability, simplified management, and rapid updates to counter emerging threats. Notably, Gartner observes that hybrid deployments remain relevant for enterprises with stringent compliance or latency requirements.

Among the vendors profiled, established cybersecurity firms coexist with specialized email security providers, each bringing distinct strengths. Some vendors excel in integrating threat intelligence across multiple security layers, while others focus on user-friendly interfaces and automated remediation workflows. This diversity reflects the market’s maturation, giving buyers a broad spectrum of options tailored to different organizational needs and budgets.

Comparative Insights: Strengths and Limitations

A salient aspect of the Gartner Email Security Market Guide is its balanced approach in discussing both the advantages and challenges posed by various solutions:

- **Advanced Threat Protection (ATP):** Vendors employing AI and sandboxing techniques demonstrate improved detection rates but may introduce latency in email delivery.
- **User Awareness and Training Integration:** Some platforms incorporate security awareness tools, which enhance human defenses but require consistent user engagement.

- **False Positives and Email Deliverability:** Striking a balance between blocking malicious content and maintaining smooth communication remains a persistent challenge.
- **Pricing Models:** Subscription-based cloud services offer flexibility but can become costly at scale compared to traditional licensing.

These nuanced evaluations help organizations anticipate potential operational trade-offs when selecting email security solutions.

Strategic Considerations for Organizations

The Gartner Email Security Market Guide emphasizes that selecting the right email security platform is not merely about technology but also involves aligning with broader organizational objectives. Factors such as compliance mandates, user demographics, IT infrastructure, and incident response capabilities must inform decision-making.

For instance, organizations handling regulated data may prioritize solutions with robust encryption and detailed audit trails. Conversely, enterprises with distributed workforces might seek cloud-based services offering seamless integration with mobile devices and remote access. Gartner also highlights the importance of vendor support and continuous updates to counter zero-day exploits and evolving phishing tactics.

Recommendations for Effective Deployment

To leverage the strengths identified in the market guide, organizations should consider the following best practices:

1. **Comprehensive Risk Assessment:** Evaluate email threat vectors specific to the organization’s industry and operational model.
2. **Layered Security Approach:** Combine email security tools with endpoint protection, identity management, and network defenses.
3. **User Training and Phishing Simulations:** Enhance user vigilance alongside technological safeguards.
4. **Regular Policy Review and Updates:** Adapt email security policies to emerging threats and business changes.
5. **Vendor Evaluation and Proof of Concept:** Conduct trials to assess real-world performance and integration capabilities.

Such a strategic approach ensures that investments in email security translate into meaningful risk mitigation.

Future Outlook and Emerging Technologies

The Gartner Email Security Market Guide also casts light on future developments shaping the email security landscape. Artificial intelligence and machine learning are expected to become more sophisticated, enabling proactive threat hunting and automated incident response. Additionally, integration with broader Extended Detection and Response (XDR) frameworks promises more holistic visibility across attack surfaces.

Another emerging area is the use of blockchain and decentralized authentication methods to enhance email integrity and combat spoofing. While these technologies are still in nascent stages, Gartner’s guide suggests that forward-looking organizations keep abreast of such innovations to maintain a competitive edge.

The evolving regulatory environment, including data privacy laws and cybersecurity mandates, will further influence vendor offerings and organizational priorities. Adaptability and continuous monitoring will remain critical as threat actors refine their tactics.

In summary, the Gartner Email Security Market Guide provides an indispensable lens through which enterprises can comprehend the multifaceted nature of email security solutions. By integrating market intelligence, vendor capabilities, and strategic recommendations, it equips security leaders to navigate the complex challenges posed by one of the most exploited channels in the cyber threat landscape.

Gartner Email Security Market Guide

gartner email security market guide: Financial Crimes Chander Mohan Gupta, 2023-05-15 The book's primary purpose is to understand the economic, social, and political impact of financial crimes and earning management on the Indian national economy. The book is divided into four parts that focus on different sectors which lead to financial crimes in a country: Financial crimes White Collar Crimes Cybercrimes Creative Accounting Investigating topics such as drug mafia, money laundering, online fraud, accounting fraud, and more, the comprehensive investigation of different aspects of financial crimes, this book offers insight into its central problems and how they can be controlled. It is ideal for financial crime researchers.

gartner email security market guide: *Computer Security Handbook, Set* Seymour Bosworth, M. E. Kabay, Eric Whyne, 2014-03-24 Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.

gartner email security market guide: Studies Combined: Cyber Warfare In Cyberspace - National Defense, Workforce And Legal Issues , 2018-01-18 Just a sample of the contents ... contains over 2,800 total pages .... PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE Cyberwarfare and Operational Art CYBER WARFARE GOVERNANCE: EVALUATION OF CURRENT INTERNATIONAL AGREEMENTS ON THE OFFENSIVE USE OF CYBER Cyber Attacks and the Legal Justification for an Armed Response UNTYING OUR HANDS: RECONSIDERING CYBER AS A SEPARATE INSTRUMENT OF NATIONAL POWER Effects-Based Operations in the Cyber Domain Recommendations for Model-Driven Paradigms for Integrated Approaches to Cyber Defense MILLENNIAL WARFARE IGNORING A REVOLUTION IN MILITARY AFFAIRS: THE NEED TO CREATE A SEPARATE BRANCH OF THE ARMED FORCES FOR CYBER WARFARE SPECIAL OPERATIONS AND CYBER WARFARE LESSONS FROM THE FRONT: A CASE STUDY OF RUSSIAN CYBER WARFARE ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES Addressing Human Factors Gaps in Cyber Defense Airpower History and the Cyber Force of the Future How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past THE COMMAND OF THE TREND: SOCIAL MEDIA AS A WEAPON IN THE INFORMATION AGE SPYING FOR THE RIGHT REASONS: CONTESTED NORMS IN CYBERSPACE AIR FORCE CYBERWORX REPORT: REMODELING AIR FORCE CYBER COMMAND & CONTROL THE CYBER WAR: MAINTAINING AND CONTROLLING THE “KEY CYBER TERRAIN” OF THE CYBERSPACE DOMAIN WHEN NORMS FAIL: NORTH KOREA AND CYBER AS AN ELEMENT OF STATECRAFT AN ANTIFRAGILE APPROACH TO PREPARING FOR CYBER CONFLICT AIR FORCE CYBER MISSION ASSURANCE SOURCES OF MISSION UNCERTAINTY Concurrency Attacks and Defenses Cyber Workforce Retention Airpower Lessons for an Air Force Cyber-Power Targeting ¬Theory IS BRINGING BACK WARRANT OFFICERS THE ANSWER? A LOOK AT HOW THEY COULD WORK IN THE AIR FORCE CYBER OPERATIONS CAREER FIELD NEW TOOLS FOR A NEW TERRAIN AIR FORCE SUPPORT TO SPECIAL OPERATIONS IN THE CYBER ENVIRONMENT Learning to Mow Grass: IDF Adaptations to Hybrid Threats CHINA’S WAR BY OTHER MEANS: UNVEILING CHINA’S QUEST FOR INFORMATION DOMINANCE THE ISLAMIC STATE’S TACTICS IN SYRIA: ROLE OF SOCIAL MEDIA IN SHIFTING A PEACEFUL ARAB SPRING INTO TERRORISM NON-LETHAL WEAPONS: THE KEY TO A MORE AGGRESSIVE STRATEGY TO COMBAT TERRORISM THOUGHTS INVADE US: LEXICAL COGNITION AND CYBERSPACE The Cyber Threat to Military Just-In-Time Logistics: Risk Mitigation and the Return to Forward Basing PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE Cyberwarfare and Operational Art CYBER WARFARE GOVERNANCE: EVALUATION OF CURRENT INTERNATIONAL AGREEMENTS ON THE OFFENSIVE USE OF CYBER Cyber Attacks and the Legal Justification for an Armed Response UNTYING OUR HANDS: RECONSIDERING CYBER AS A SEPARATE INSTRUMENT OF NATIONAL POWER Effects-Based Operations in the Cyber Domain Recommendations for Model-Driven Paradigms for Integrated Approaches to Cyber Defense MILLENNIAL WARFARE IGNORING A REVOLUTION IN MILITARY AFFAIRS: THE NEED TO CREATE A SEPARATE BRANCH OF THE ARMED FORCES FOR CYBER WARFARE SPECIAL OPERATIONS AND CYBER WARFARE LESSONS FROM THE FRONT: A CASE STUDY OF RUSSIAN CYBER WARFARE ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES Addressing Human Factors Gaps in Cyber Defense Airpower History and the Cyber Force of the Future How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past THE COMMAND OF THE TREND: SOCIAL MEDIA AS A WEAPON IN THE INFORMATION AGE SPYING FOR THE RIGHT REASONS: CONTESTED NORMS IN CYBERSPACE AIR FORCE CYBERWORX REPORT: REMODELING AIR FORCE CYBER COMMAND & CONTROL THE CYBER WAR: MAINTAINING AND CONTROLLING THE “KEY CYBER TERRAIN” OF THE CYBERSPACE DOMAIN WHEN NORMS FAIL: NORTH KOREA AND CYBER AS AN ELEMENT OF STATECRAFT AN ANTIFRAGILE APPROACH TO PREPARING FOR CYBER CONFLICT AIR FORCE CYBER MISSION ASSURANCE SOURCES OF MISSION UNCERTAINTY Concurrency Attacks and

Defenses Cyber Workforce Retention

gartner email security market guide: *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 DescriptionThis 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.

gartner email security market guide: *Understanding Cybersecurity Technologies* Abbas Moallem, 2021-12-14 Cyberattacks on enterprises, government institutions, and individuals are exponentially growing. At the same time, the number of companies, both small and large, offering all types of solutions has been increasing too. Since companies rely on technological solutions to protect themselves against cyberattacks, understanding and selecting the right solutions among those offered presents a significant challenge for professionals, company executives, and newcomers to the cybersecurity field. FEATURES Presents descriptions for each type of cybersecurity technology and their specifications Explains applications, usages, and offers case studies to enhance comprehension Offers an easy-to-understand classification of existing cybersecurity technologies Provides an understanding of the technologies without getting lost in technical details Focuses on existing technologies used in different solutions, without focusing on the companies that offer these technologies This book is intended to help all professionals new to cybersecurity, students, and experts to learn or educate their audiences on the foundations of the available solutions.

gartner email security market guide: *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.

gartner email security market guide: Official (ISC)2® Guide to the ISSAP® CBK (ISC)2 Corporate, 2017-01-06 Candidates for the CISSP-ISSAP professional certification need to not only demonstrate a thorough understanding of the six domains of the ISSAP CBK, but also need to have the ability to apply this in-depth knowledge to develop a detailed security architecture. Supplying an authoritative review of the key concepts and requirements of the ISSAP CBK, the Official (ISC)2® Guide to the ISSAP® CBK®, Second Edition provides the practical understanding required to

implement the latest security protocols to improve productivity, profitability, security, and efficiency. Encompassing all of the knowledge elements needed to create secure architectures, the text covers the six domains: Access Control Systems and Methodology, Communications and Network Security, Cryptology, Security Architecture Analysis, BCP/DRP, and Physical Security Considerations. Newly Enhanced Design – This Guide Has It All! Only guide endorsed by (ISC)2 Most up-to-date CISSP-ISSAP CBK Evolving terminology and changing requirements for security professionals Practical examples that illustrate how to apply concepts in real-life situations Chapter outlines and objectives Review questions and answers References to free study resources Read It. Study It. Refer to It Often. Build your knowledge and improve your chance of achieving certification the first time around. Endorsed by (ISC)2 and compiled and reviewed by CISSP-ISSAPs and (ISC)2 members, this book provides unrivaled preparation for the certification exam and is a reference that will serve you well into your career. Earning your ISSAP is a deserving achievement that gives you a competitive advantage and makes you a member of an elite network of professionals worldwide.

gartner email security market guide: *Financial Cryptography and Data Security* Aggelos Kiayias, 2017-12-22 This book constitutes the thoroughly refereed post-conference proceedings of the 21st International Conference on Financial Cryptography and Data Security, FC 2017, held in Sliema, Malta, in April 2017. The 30 revised full papers and 5 short papers were carefully selected and reviewed from 132 submissions. The papers are grouped in the following topical sections: Privacy and Identity Management; Privacy and Data Processing; Cryptographic Primitives and API's; Vulnerabilities and Exploits; Blockchain Technology; Security of Internet Protocols; Blind signatures; Searching and Processing Private Data; Secure Channel Protocols; and Privacy in Data Storage and Retrieval.

gartner email security market guide: Open Source Intelligence in the Twenty-First Century C. Hobbs, M. Moran, D. Salisbury, 2014-05-09 This edited book provides an insight into the new approaches, challenges and opportunities that characterise open source intelligence (OSINT) at the beginning of the twenty-first century. It does so by considering the impacts of OSINT on three important contemporary security issues: nuclear proliferation, humanitarian crises and terrorism.

gartner email security market guide: Data Mining and Exploration Chong Ho Alex Yu, 2022-10-27 This book introduces both conceptual and procedural aspects of cutting-edge data science methods, such as dynamic data visualization, artificial neural networks, ensemble methods, and text mining. There are at least two unique elements that can set the book apart from its rivals. First, most students in social sciences, engineering, and business took at least one class in introductory statistics before learning data science. However, usually these courses do not discuss the similarities and differences between traditional statistics and modern data science; as a result learners are disoriented by this seemingly drastic paradigm shift. In reaction, some traditionalists reject data science altogether while some beginning data analysts employ data mining tools as a “black box”, without a comprehensive view of the foundational differences between traditional and modern methods (e.g., dichotomous thinking vs. pattern recognition, confirmation vs. exploration, single method vs. triangulation, single sample vs. cross-validation etc.). This book delineates the transition between classical methods and data science (e.g. from p value to Log Worth, from resampling to ensemble methods, from content analysis to text mining etc.). Second, this book aims to widen the learner's horizon by covering a plethora of software tools. When a technician has a hammer, every problem seems to be a nail. By the same token, many textbooks focus on a single software package only, and consequently the learner tends to fit the problem with the tool, but not the other way around. To rectify the situation, a competent analyst should be equipped with a tool set, rather than a single tool. For example, when the analyst works with crucial data in a highly regulated industry, such as pharmaceutical and banking, commercial software modules (e.g., SAS) are indispensable. For a mid-size and small company, open-source packages such as Python would come in handy. If the research goal is to create an executive summary quickly, the logical choice is rapid model comparison. If the analyst would like to explore the data by asking what-if questions, then dynamic graphing in JMP Pro is a better option. This book uses concrete examples to explain

the pros and cons of various software applications.

gartner email security market guide: Computerworld , 2004-09-13 For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

gartner email security market guide: Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer Dadwal, Sumesh Singh, 2019-11-15 Connected customers, using a wide range of devices such as smart phones, tablets, and laptops have ushered in a new era of consumerism. Now more than ever, this change has prodded marketing departments to work with their various IT departments and technologists to expand consumers' access to content. In order to remain competitive, marketers must integrate marketing campaigns across these different devices and become proficient in using technology. The Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer is a pivotal reference source that develops new insights into applications of technology in marketing and explores effective ways to reach consumers through a wide range of devices. While highlighting topics such as cognitive computing, artificial intelligence, and virtual reality, this publication explores practices of technology-empowered digital marketing as well as the methods of applying practices to less developed countries. This book is ideally designed for marketers, managers, advertisers, branding teams, application developers, IT specialists, academicians, researchers, and students.

gartner email security market guide: Cloud Data Centers and Cost Modeling Caesar Wu, Rajkumar Buyya, 2015-02-27 Cloud Data Centers and Cost Modeling establishes a framework for strategic decision-makers to facilitate the development of cloud data centers. Just as building a house requires a clear understanding of the blueprints, architecture, and costs of the project; building a cloud-based data center requires similar knowledge. The authors take a theoretical and practical approach, starting with the key questions to help uncover needs and clarify project scope. They then demonstrate probability tools to test and support decisions, and provide processes that resolve key issues. After laying a foundation of cloud concepts and definitions, the book addresses data center creation, infrastructure development, cost modeling, and simulations in decision-making, each part building on the previous. In this way the authors bridge technology, management, and infrastructure as a service, in one complete guide to data centers that facilitates educated decision making. - Explains how to balance cloud computing functionality with data center efficiency - Covers key requirements for power management, cooling, server planning, virtualization, and storage management - Describes advanced methods for modeling cloud computing cost including Real Option Theory and Monte Carlo Simulations - Blends theoretical and practical discussions with insights for developers, consultants, and analysts considering data center development

gartner email security market guide: The Digital Selling Handbook: Grow Your Sales by Engaging, Prospecting, and Converting Customers the Way They Buy Today Bill Stinnett, 2022-10-18 Actionable advice for sales professionals and business owners for growing sales in today's increasingly virtual marketplace Rapid changes in where and how people live, work, and do business in recent years, have triggered major shifts in how customers shop for and buy virtually everything! Sales and marketing professionals are faced with the harsh reality of rethinking their entire approach to engaging clients in today's virtual marketplace—or risk quickly becoming irrelevant. They need to rethink their entire sales approach—and Digital Selling Handbook shows them how to do it. This comprehensive guide builds readers' understanding of customer psychology and buying behavior in the new digital-first world. It provides best practices for engaging customers using a variety of methods. Digital selling expert and founder of Sales Excellence, Inc., Bill Stinnett covers the entire sales and marketing process, showing how to: Create a magnetic personal brand that attracts prospective customers Engage customers earlier in the buying process Develop an evergreen lead machine using strategies of world-class organizations Write articles, emails, and social media posts that trigger customer action Find and create new opportunities through outbound

prospecting Turn customer conversations into sales opportunities and revenue Finding and attracting new business will always be one of the most vital aspects of business success. In today's transformed world of selling, those with the smartest, more forward-looking strategies will be the ones to come out on top. The Digital Selling Handbook provides everything you need keep ahead of the curve and in front of the competition.

gartner email security market guide: Telecommunications Directory Gale Group, 2001 This new 12th edition of Telecommunications Directory features approximately 6,800 entries including increased coverage of international telecommunications companies. This resource provides detailed information on telecommunications companies providing a range of products and services from cellular communications and local exchange carriers to satellite services and Internet service providers. Entries are arranged alphabetically by organization name and typically include a list of products and services; complete contact information, including URLs where available; and a profile of the organization's activities. Telecommunications Directory also includes a glossary defining more than 500 terms, acronyms, concepts, standards and government rulings.

gartner email security market guide: 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.

gartner email security market guide: Introduction to Communications Technologies Stephan Jones, Ronald J. Kovac, Frank M. Groom, 2015-07-28 Thanks to the advancement of faster processors within communication devices, there has been a rapid change in how information is modulated, multiplexed, managed, and moved. While formulas and functions are critical in creating the granular components and operations of individual technologies, understanding the applications and their purposes in the

gartner email security market guide: Ransomware Evolution Mohiuddin Ahmed, 2024-12-23 Ransomware is a type of malicious software that prevents victims from accessing their computers and the information they have stored. Typically, victims are required to pay a ransom, usually using cryptocurrency, such as Bitcoin, to regain access. Ransomware attacks pose a significant threat to national security, and there has been a substantial increase in such attacks in the post-Covid era. In response to these threats, large enterprises have begun implementing better cybersecurity practices, such as deploying data loss prevention mechanisms and improving backup strategies. However, cybercriminals have developed a hybrid variant called Ransomware 2.0. In this variation, sensitive data is stolen before being encrypted, allowing cybercriminals to publicly release the information if the ransom is not paid. Cybercriminals also take advantage of cryptocurrency's anonymity and untraceability. Ransomware 3.0 is an emerging threat in which cybercriminals target critical infrastructures and tamper with the data stored on computing devices. Unlike in traditional ransomware attacks, cybercriminals are more interested in the actual data on the victims' devices, particularly from critical enterprises such as government, healthcare, education, defense, and utility providers. State-based cyber actors are more interested in disrupting critical infrastructures rather than seeking financial benefits via cryptocurrency. Additionally, these sophisticated cyber actors are

also interested in obtaining trade secrets and gathering confidential information. It is worth noting that the misinformation caused by ransomware attacks can severely impact critical infrastructures and can serve as a primary weapon in information warfare in today’s age. In recent events, Russia’s invasion of Ukraine led to several countries retaliating against Russia. A ransomware group threatened cyber-attacks on the critical infrastructure of these countries. Experts warned that this could be the most widespread ransomware gang globally and is linked to a trend of Russian hackers supporting the Kremlin’s ideology. Ensuring cyber safety from ransomware attacks has become a national security priority for many nations across the world. The evolving variants of ransomware attacks present a wider and more challenging threat landscape, highlighting the need for collaborative work throughout the entire cyber ecosystem value chain. In response to this evolving threat, a book addressing the challenges associated with ransomware is very timely. This book aims to provide a comprehensive overview of the evolution, trends, techniques, impact on critical infrastructures and national security, countermeasures, and open research directions in this area. It will serve as a valuable source of knowledge on the topic.

gartner email security market guide: Security , 2006

gartner email security market guide: Plunkett's Infotech Industry Almanac, 2001-2002 Jack W. Plunkett, Plunkett, 2001 InfoTech being any technology that moves or manages voice, data or video - whether that movement be via wireless methods, fiber optics, traditional copper wire, telephony, computer network or emerging methods. Each industry segment & the most outstanding corporations within those industries are featured. It includes dozens of tables, indexes by product, services & geography, plus corporate rankings for sales, profits & research budgets. Complete profiles on Plunkett's InfoTech 500 Firms include companies in telecommunications, software, hardware, on-line services, information management, systems integration, outsourcing & more.

Related to gartner email security market guide

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner 称预计 2026 年超过 80% 的企业将使用生成式 AI 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？一、Gartner公司与魔力象限 1979年，Gartner

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

为什么 Gartner 等分析机构都在强调“全栈超融合软件”？ 作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

如何获得Gartner、iSuppli、IDC之类的原报告？ - 知乎 我有过两种免费获得 Gartner 报告的经历：1. 用大学邮箱注册，@unimelb.edu.au 我们学校有部分订阅。（母校威武）你们可以用所在组织邮箱注册一下，说不定订阅了。2. 去领导者象限的

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

Gartner最新发布的2025年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

Gartner 报告解读 | 中国 IT 基础设施 4 大趋势与 8 大重点技术 近些年，面对数字化转型、信息化发展、政策监管与地缘政治等外部因素，以及降本增效的内部需求，不少中国企业在制定 IT 基础设施发展策略时遇到多重挑战。为帮助国内

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner 称预计 2026 年超过 80% 的企业将使用生成式 AI 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？ 一、Gartner公司与魔力象限 1979年，Gartner

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

为什么 **Gartner** 等分析机构都在强调**“**全栈超融合软件**”**？作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

如何获得**Gartner、iSuppli、IDC**之类的原报告？ - 知乎 我有过两种免费获得 Gartner 报告的经历： 1. 用大学邮箱注册，@unimelb.edu.au 我们学校有部分订阅。（母校威武）你们可以用所在组织邮箱注册一下，说不定订阅了。 2. 去领导者象限的

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

Gartner最新发布的**2025**年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

Gartner 报告解读丨中国 **IT** 基础设施 **4** 大趋势与 **8** 大重点技术 近些年，面对数字化转型、信息化发展、政策监管与地缘政治等外部因素，以及降本增效的内部需求，不少中国企业在制定 IT 基础设施发展策略时遇到多重挑战。为帮助国内

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。 Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner 称预计 **2026** 年超过 **80%** 的企业将使用生成式 **AI** 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？ 一、Gartner公司与魔力象限 1979年，Gartner

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

为什么 **Gartner** 等分析机构都在强调**“**全栈超融合软件**”**？作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

如何获得**Gartner、iSuppli、IDC**之类的原报告？ - 知乎 我有过两种免费获得 Gartner 报告的经历： 1. 用大学邮箱注册，@unimelb.edu.au 我们学校有部分订阅。（母校威武）你们可以用所在组织邮箱注册一下，说不定订阅了。 2. 去领导者象限的

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

Gartner最新发布的**2025**年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

Gartner 报告解读丨中国 **IT** 基础设施 **4** 大趋势与 **8** 大重点技术 近些年，面对数字化转型、信息化发展、政策监管与地缘政治等外部因素，以及降本增效的内部需求，不少中国企业在制定 IT 基础设施发展策略时遇到多重挑战。为帮助国内

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。 Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner 称预计 **2026** 年超过 **80%** 的企业将使用生成式 **AI** 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？ 一、Gartner公司与魔力象限 1979年，Gartner

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

为什么 **Gartner** 等分析机构都在强调**“**全栈超融合软件**”**？作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

如何获得**Gartner、iSuppli、IDC**之类的原报告？ - 知乎 我有过两种免费获得 Gartner 报告的经历： 1. 用大学邮箱注册，@unimelb.edu.au 我们学校有部分订阅。（母校威武）你们可以用所在组织邮箱注册一下，说不定订阅了。 2. 去领导者象限的

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

Gartner最新发布的**2025**年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些

代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

Gartner 报告解读 | 中国 IT 基础设施 4 大趋势与 8 大重点技术 近些年，面对数字化转型、信息化发展、政策监管与地缘政治等外部因素，以及降本增效的内部需求，不少中国企业在制定 IT 基础设施发展策略时遇到多重挑战。为帮助国内

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner 称预计 2026 年超过 80% 的企业将使用生成式 AI 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？ 一、Gartner公司与魔力象限 1979年，Gartner

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商业

为什么 Gartner 等分析机构都在强调“全栈超融合软件”？ 作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

如何获得Gartner、iSuppli、IDC之类的原报告？ - 知乎 我有过两种免费获得 Gartner 报告的经历：1. 用大学邮箱注册，@unimelb.edu.au 我们学校有部分订阅。（母校威武）你们可以用所在组织邮箱注册一下，说不定订阅了。 2. 去领导者象限的

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据齐

Gartner最新发布的2025年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

Gartner 报告解读 | 中国 IT 基础设施 4 大趋势与 8 大重点技术 近些年，面对数字化转型、信息化发展、政策监管与地缘政治等外部因素，以及降本增效的内部需求，不少中国企业在制定 IT 基础设施发展策略时遇到多重挑战。为帮助国内

Related to gartner email security market guide

Darktrace Named a 2025 Gartner® Peer Insights™ Customers’ Choice for Email Security Platforms (Morningstar1mon) Cambridge, UK, Aug. 19, 2025 (GLOBE NEWSWIRE) -- Darktrace, a global leader in AI for cybersecurity, has been named a Customers’ Choice in the 2025 Gartner® Peer Insights™ Voice of the Customer for

Darktrace Named a 2025 Gartner® Peer Insights™ Customers’ Choice for Email Security Platforms (Morningstar1mon) Cambridge, UK, Aug. 19, 2025 (GLOBE NEWSWIRE) -- Darktrace, a global leader in AI for cybersecurity, has been named a Customers’ Choice in the 2025 Gartner® Peer Insights™ Voice of the Customer for

Ridge Security Recognized as a Strong Performer in the 2024 Gartner® Peer Insights ™ Voice of the Customer. (Business Wire2mon) MILPITAS, Calif.--(BUSINESS WIRE)--Ridge Security, a leader in automated penetration testing and AI-powered security validation for CTEM, today announced Gartner Peer Insights placed it in the

Ridge Security Recognized as a Strong Performer in the 2024 Gartner® Peer Insights ™ Voice of the Customer. (Business Wire2mon) MILPITAS, Calif.--(BUSINESS WIRE)--Ridge Security, a leader in automated penetration testing and AI-powered security validation for CTEM, today announced Gartner Peer Insights placed it in the

Related Articles

- the girl can t help it
- 5 nf 1 worksheets
- the aquitaine progression robert ludlum

Back to Home