Gartner
IT Security Summit 2008

Information Security: Explore – Strategise – Envision – Implement

23 – 24 September 2008, Sydney Convention & Exhibition Centre, Sydney, Australia

CONFERENCE CHAIRS

Eric Ouellet
Research VP

Andrew Walls
Research Director

Register Today!
gartner.com/ap/itsecurity

Gartner
IT Security
Summit 2008

Introduction from the Conference Chairs

More than ever, a proactive IT security strategy is vital to success. As new generations of technology-savvy users and a growing wave of gadget-prone communication services are making their way into the workplace, they bring with them new security threats as well as new technical and management paradigms. All of this rapid change has the potential to create considerable chaos in security operations and the security marketplace.

Security remains a top concern for every C-level executive and security managers at all levels – for good reason. The proliferation of wireless devices, e-enabled applications, and advanced global systems for both employees and collaborative efforts with business partners and customers puts your data in the hands of more people in more places than ever before.

Security is most effective when it is integrated with core business processes. With thousands of security products and services on the market you need to know where to make strategic investments, how to govern security, and how to optimize process for the greatest efficiency.

We've created an Agenda that covers the security landscape, including emerging threats, the demands of compliance, planning for the unexpected and for new security infrastructures, and developing new processes to conquer these challenges.

The Gartner IT Security Summit 2008 will help you take advantage of emerging opportunities. Our Gartner Analysts will present a detailed vision of the future of IT security and show you how to strategically plan and tactically implement a successful security program.

We urge you to attend this important event, where you will forge strong connections with high-level professionals like yourself, view upcoming technologies and delve into your own critical issues in one-on-one sessions with our Analysts and security technology solution providers.

We look forward to seeing you in Sydney this September.

Eric Ouellet
Research VP

Andrew Walls
Research Director

Get answers to your most pressing challenges

- How do I optimise my security spending in a time of budget constraints?
- Are we keeping pace with new developments?
- What threats are we not protecting against?
- What new threats will occur?

Find out how key trends will impact your IT security strategy

- Creating and managing the right security strategies for a changing threat landscape
- Information security architectures and data protection: the right content and structure
- Risk management for information security practitioners
- The process-oriented activity cycle for security and risk management
- Effective processes and technologies for identity and access management, vulnerability and threat management, risk and control assessment, communications and relationship management
- Regulatory compliance and corporate governance
- Achieving maturity in business continuity management and disaster recovery
- Building security metrics that actually mean something
- Latest analyses of information security markets and vendors
- Managing the security impact of social network services

Three Tracks

Information Security: Explore – Strategise – Envision – Implement

As the business demands measurable results and threats expand exponentially, security managers have to anticipate and plan effective solutions for tomorrow. Through hundreds of client interactions and feedback, we've identified the key elements for you to develop an effective security control program.

Track A

Managing Security, Compliance and Risk

Compliance and risk management are not about technology. However, the fact is this: IT systems support the way an organisation lives and breathes. So how can you help business units within your organisation understand and manage IT-related risks and achieve compliance confidently? By systematically addressing IT risks across the enterprise and improving critical business and security management processes. Such a proactive approach enables top-line growth while still maintaining necessary levels of control in the complex areas of governance, regulations, risks, performance, sourcing, security, access control and vendor selection. This track focuses on the tools, strategies and tactics characteristic of a coordinated program for addressing regulatory, commercial and organisational risk effectively.

Track B

Secure Business Enablement

Innovative business models challenge security teams to envision new and more effective approaches to security in rapidly changing environments. Once you build it, it must be secure. Legacy access control technologies, fragmented user administration processes and directories, spoofable e-mail, and single-platform security administration products are all typical examples of business 'disabling' approaches that are no longer sufficient. You need techniques and tools that are business enablers. These sessions focus on best practices in defining and managing identity and access management, secure messaging, and supporting enhanced mobility.

Track C

Infrastructure Protection

Enterprises must prevent and limit damage to their business operations by deploying policies, processes and technologies to detect and block attacks — both internal and external — and minimise the vulnerabilities that enable attacks. The enterprise threat environment is changing rapidly, as are the approaches, applications and technologies enterprises use to engage customers and partners — your strategies must change with them. This track focuses on the processes, technologies and services needed to protect data, applications, systems and the network, as well as ways to discover and solve security weaknesses.

Benefits of attending

- New breakthrough research
- New cutting-edge recommendations
- New best practices
- Understand emerging trends and your best defenses
- Sharpen the way you communicate security to the business
- Drive down the cost of compliance while harvesting the benefits

Who should attend?

Anyone involved in enterprise-wide security and critical infrastructure protection including:

- CIO / CTO / CISO
- VPs, Heads, Directors, Managers of: security, risk, compliance, identity, access, fraud, e-commerce, privacy, governance, facilities, audit, data protection, disaster recovery

The Gartner difference

- Leading provider of events for IT professionals
- Highly discerning research that is objective, defensible and credible
- The largest and most informed team of research analysts
- Independent, not vendor driven
- Balance between strategic and practical

Meet the Gartner Analysts

Worldwide expertise at your fingertips

For over 25 years, Gartner analysts have been the trusted advisors to many of the world's largest and most demanding companies. No one sees the implications of technology so clearly, so consistently.

Gartner analysts draw constantly from the real-life challenges and solutions experienced by more than 45,000 Gartner clients worldwide. The value of this resource, combined with our deep analysis of technology vendors, is unrivalled.

Steve Bittinger,
Research Director, Australia
Focus areas: APAC security regulatory/governance, business continuity

Richard Harris,
Research VP, Australia
Focus areas: Business and technology strategy, competitive dynamics, management and innovation, risk management

Neil MacDonald,
VP & Gartner Fellow, US
Focus areas: Information security and privacy, operating system and application-level security strategies, windows security, host-based intrusion prevention systems, converged endpoint security, service-oriented application security, business process management security and the integration of security into the application development process

Eric Ouellet,
Research VP, Canada
Focus areas: Encryption and rights management, wireless security, smartcards, identity and access management, security certification, business continuity

Earl Perkins,
Research VP, US
Focus areas: Identity and access management, enterprise application, web services, service-oriented architecture (SOA), and software as a service (SaaS) security and identity issues; and secure development life cycles

Tom Scholtz,
Research VP, UK
Focus areas: Security management and operations, security architectures, budget and spending, secure outsourcing

Robin Simpson,
Research Director, Australia
Focus areas: Mobile devices, wireless technology management

Andrew Walls,
Research Director, Australia
Focus areas: APAC security markets and issues, security management, governance and compliance, policy, risk management

Ray Wagner,
Managing VP, US
Focus areas: Information security and privacy, identity and access management, web services security, public-key infrastructures, digital rights management, the information security organisation, and information security issues within emerging technologies

Deborah Weiss,
Research Director, Australia
Focus areas: Enterprise architecture, program management, portfolio management and IT strategic planning

One-on-One Meetings

Tackle your toughest challenges. Take the opportunity to book a 30 minute One-on-One meeting with a Gartner Analyst. You set the agenda according to your priorities, and the discussion is tailor made for you. Spaces are limited and appointments are made on a first come first served basis – so book early to avoid disappointment.

Agenda at a glance

DAY 1 Tuesday 23 September	
07:30	Registration
08:30	Tutorials
09:45	Keynote Speaker
11:15	Morning Sessions
12:55	Lunch
13:45	Afternoon Sessions
17:00	Guest Speaker
18:00	Networking Reception

DAY 2 Wednesday 24 September	
08:00	Registration
08:30	Morning Sessions
10:40	Premier Sponsor Panel
12:50	Lunch
13:35	Afternoon Sessions
15:00	Closing Keynote
16:00	Conference Close

Guest Keynote

Thinking Out of the Box

Jack Dann

Author

The bestselling, multi-award winning author of *The Memory Cathedral* and *The Man Who Melted* discusses the exponential curve of technological progress that is now accelerating into a singularity—or spike—beyond which predication fails. He describes how science fiction writers think themselves into the future, what they get wrong, and the next 'Big Thing' we're most certainly going to miss. In a free-wheeling speculation on nanotechnology, virtual reality, and artificial intelligence, he extrapolates futures where hackers wake up the internet and quantum computers make cryptology obsolete…and he invites you to imagine virtual worlds where avatars are alive and code can kill.

Analyst/User Roundtables

Discuss key issues with experts and peers alike. You are invited to participate in topic focused Analyst/User Roundtable discussions on specific HOT topics. Limited to 10 end-users per session.

Business Continuity Management Best Practices

Steve Bittinger

An integrated security program includes managing the associated risks to the business, and planning how to keep the business running in the event of a disaster or extended disruption. At this end-user roundtable, come and share your experiences of what works and what doesn't in the area of business continuity management.

The Business Value of Security

Eric Ouellet

Security professionals and business leaders don't always speak the same language; it can be difficult to articulate the value of a security investment in a non-technical business context. In this roundtable session delegates will learn and share proven techniques for communicating the business value of security to non-technical executives.

Developing a Risk Management Program

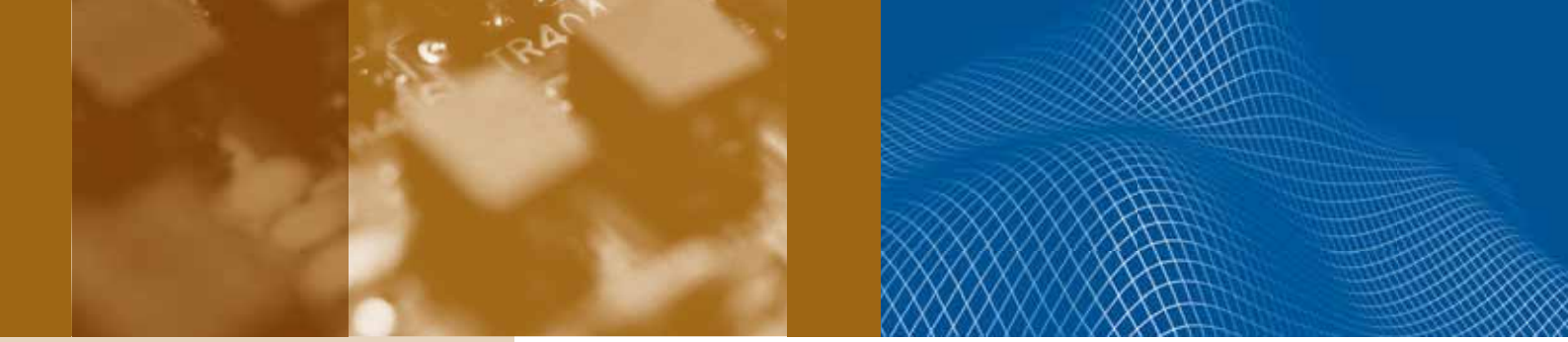
Richard Harris

Security is both a tool of risk management, and a domain requiring its own risk management techniques. This roundtable session will focus on the latest techniques for risk management, including methods of integrating security into an enterprise risk management program.

Identity and Access Management Best Practices

Ray Wagner

Identity and Access Management (IAM) technologies are many, and it is often difficult to assess which are right for a particular enterprise. IAM programs can be complex and take years to establish. At this end-user roundtable, come and share your experiences of what works and what doesn't in the area of Identity and Access Management.



Plenary Sessions

Opening Keynote

Myths, Misconceptions and Paranoia's Breaking Down The Barriers to Effective Security Management

As organisations embark on a security management program they run into many real and perceived obstacles that distract them from focusing on business priorities. Organisations who are not disciplined in effectively addressing myths, misconceptions and paranoia's will continue to fail and lower the value of their security programs. In our opening keynote session, Gartner's leading security analysts will show you how to break down these barriers in order to Explore, Strategise, Envision, and Implement more effectively.

Closing Keynote

Magic Quadrant Powerhouse Session

Meet the Gartner analysts at their best - adhoc on stage. Get the latest information on the IT Security tools and markets to help you explore, strategise, envision, implement. Ask questions about vendors or tools. Hear the Gartner position on the technology providers relevant to your immediate requirements – unscripted, unfiltered, unbiased.

Track A

Managing Security, Compliance and Risk

Tutorial: Control Self-Assessment as a Tool for Risk Management

Richard Harris

Control self-assessment is the process of having internal controls evaluated by operational personnel so that business objectives will be met. Similarly, IT control assessments can be performed to establish the efficacy of IT internal controls and determine an organisation's threat exposure.

- Pros and cons of control self-assessment
- Establishing a control self-assessment program
- Tools to automate the self-assessment/risk management process

Emerging IT Governance Risk and Compliance Technologies

Tom Scholtz

IT Governance, Risk and Compliance Management (GRCM) is a set of capabilities that can improve an IT organisation's external audit posture, reduce compliance reporting costs, and improve an organisation's ability to effectively address IT risks. Technology selection and deployment advice is provided for this emerging market.

- How can IT GRCM technology reduce compliance costs and improve an organisation's ability to assess risk?
- Who are the major IT GRCM technology providers?
- How can organisations effectively deploy IT GRCM technologies?

Managing Security Information and Emerging Vulnerabilities

Eric Ouellet

Organisations need to implement new ways to find and fix security weaknesses as threats evolve and new IT delivery methods are adopted. The technologies and services that will be needed to manage security information and eliminate vulnerabilities will be evaluated in this session.

- What are the essential components of an effective emerging vulnerability management program?
- What new technologies and services should organisations employ to manage new vulnerabilities and security information?
- What policies, procedures and rules are appropriate for an agile application organisation?

New-Age E-Discovery for Security Practitioners

Andrew Walls

If you thought e-discovery of internal Electronically Stored Information (ESI) was bad, just wait. The problems posed by e-discovery are worsening as litigators and regulators focus on the digital persona of e-discovery custodians well beyond the firewalls of their organisations. This means that personal e-mail accounts as well as social networking sites and virtual reality may become the targets of litigators and regulators.

If it can be established there is a element to their work that may be information relevant and a cause for action.

- What is the e-discovery mandate organisations must address?
- How are organisations deploying resources to address the e-discovery mandate?
- Why is the e-discovery mandate evolving and growing in complexity and what does this mean for information security?

Business Resiliency: A Proactive Approach for Managing Business Interruptions

Steve Bittinger

Business interruptions that impact day-to-day operations frequently occur and can have serious, long-lasting consequences. Organisations must counter and respond to them in a pro-active manner that ensures organisational resiliency is cost-effective and sustained. This presentation will discuss how Business Continuity Management (BCM) can be used to reduce operating costs, drive revenue, maintain brand and promote community reputation.

- How can BCM be positioned as a leading risk management activity?
- How does an enterprise make the business case for BCM?
- What are the trends and best practices in BCM planning?

The Impact of ITIL V3 on Governance, Risk and Compliance Strategies

Tom Scholtz

The new release of ITIL takes a life-cycle view of service management, as opposed to the functional approach of previous versions. It emphasises the engineering of risk and security components into the 'service platform warranty' for business and IT services. While this is a major improvement in approach, it does have major practical implications on IT security, risk and compliance strategies.

- What is new about ITIL V3?
- How will these changes impact SRC strategies (for the better and for the worse)?
- What can you do to prepare for and leverage ITIL V3?

Selecting Security Consultants

Andrew Walls

The prospect of implementing security controls via vendor-owned and managed technology offers several potential benefits with attendant risks. This session offers Gartner's view on the present and future role security as a service plays in enterprises and the vendors that will deliver security as a service.

- Which security controls and technologies will present the best opportunities for low-cost, fast deployment security as a service delivery now and in the future?
- What safeguards must enterprises put into place to implement security as a service effectively and safely?
- What types of vendors and service providers can offer true security as a service?

Agenda subject to change

Track B
Secure Business Enablement

Tutorial: The Lessons Learned – Buying, Deploying and Managing Identity and Access Management Systems

Earl Perkins

What does the ideal RFP or tender contain for Identity and Access Management (IAM) systems? What kind of questions should be asked before buying a system? Are there best practices for deploying user provisioning? Once a system is installed, what organisational structure is best suited for ensuring the best use of the system can be realised? These and other questions will be explored in a survey of customer experiences.

- What goes into an ideal RFI, RFP or tender for IAM?
- What are key best practices in IAM program implementation?
- How do you manage an installed IAM system effectively?

Best Practices for IAM Program Governance and Project Management

Ray Wagner

Identity and Access Management (IAM) programs can be complex and take years to establish. While IAM can contribute towards IT and enterprise governance, this requires a higher level of governance across all IAM. Governance addresses the efficient and effective use of IAM, and that demands effective IAM project management as well.

- How do IAM technologies contribute to IAM governance?
- What are best practices IAM governance?
- How can we use the Systems Development Life Cycle (SDLC) for an IAM project?

Getting to the Problem of the Root: Best Practices for Managing Superuser Privileges and Shared Account Passwords

Earl Perkins

Organisations are under increasing pressure to reduce the number of users having permanent full superuser privileges, and to implement better control over and greater accountability for use of shared accounts with similar privileges.

- How can you most efficiently and effectively contain use of full superuser privileges?
- How can you manage individuals' use of shared privileged accounts in a controlled and auditable manner?
- What are the best practices for dealing with embedded application-to-application passwords?

Wireless E-Mail and Messaging Security

Robin Simpson

Supporting workforce collaboration is a priority for most organisations today. The convergence of e-mail and other communication tools such as IM, VoIP, SMS, and web chat offers a range of benefits, but it has also significant implications for security and compliance. We will discuss real and perceived security threats, and ways to manage them.

- What are the key trends for e-mail, messaging and personal communications?
- What are the major security threats?
- How do you secure your wireless e-mail and messaging deployments?

Real Security for Virtual Spaces

Andrew Walls

Virtual worlds, social network applications and real world mapping environments are merging and integrating to form complex, geographically distributed social and business interaction environments. As corporations move into these dynamic environments to access new markets and to enhance customer interaction and staff collaboration, new security risks are created for the organisation and for the individuals that work within the virtual environments. The assurance of security within these new and rapidly changing environments requires a well coordinated and fluid approach to risk management with strong support and participation by business stakeholders.

- Why does security in virtual spaces require skills and knowledge in physical, personnel and IT security operations?
- How can staff be prepared for potentially offensive interactions within virtual environments?
- How will vendor support for security in virtual worlds vary and be influenced by local legal issues?

Identity at Your Service/s: The Rise of Service-Based Identity and Access Management

Earl Perkins

Will there ever be a day when customers can 'buy' Identity and Access Management services (IAM), rather than installing products within their enterprise? Is that day already here? Are the identity and access management products themselves built as service-oriented architecture (SOA) based solutions to make such implementations easier, whether implemented in-house or by service providers?

- How viable is service-based IAM? What form will it take?
- What are the key questions customers must ask before using service-based IAM?
- What is the current state of service-based IAM architecture?

The Next 10 Years in Secure Messaging

Eric Ouellet

New forms of spam are emerging. Requirements for monitoring outbound email are increasing. Sender reputation is becoming an important issue. IM, consumer web mail and web 2.0 are redefining the scope of messaging, and what it takes to secure it.

- How should organisations prevent the introduction of malware through messaging vectors?
- What policies and procedures are relevant to monitoring employee email?
- What are the most effective methods of implementing proper levels of messaging hygiene?

Track C
Infrastructure Protection

Tutorial: Data Loss Prevention for Compliance-Driven Organisations

Eric Ouellet

Content Monitoring and Filtering/Data Loss Protection (CMF/DLP) technologies are becoming more and more common place in the arsenal of compliance tools for many organisations. However, many continue to struggle when it comes to selecting and deploying meaningful CMF/DLP solutions and achieving their intended compliance goals.

- What are the typical deployment scenarios and which CMF/DLP solutions are the best options for each?
- Who are the market leaders for each market segment?
- What are the five points organisations must consider when deploying CMF/DLP solutions?

Security Architectures of the Future

Deborah Weiss

In a perfect world, security controls, policies, processes and behaviors become fully integrated into the fabric of the enterprise. In the real world, technical, environmental and organisational practicalities mitigate against this.

- What is a conceptual vision of the security architecture of 2012 – dreams and realities?
- What are the characteristics of future security architectures – services, application, platform and network infrastructure implications?
- Laying the foundations – what are contemporary security architecture best practices?

Building a Real-Time, Adaptive Security Infrastructure

Neil McDonald

Security infrastructure must become adaptive – to changes in business policy and to changes in the environment. Why can't our security infrastructure quickly adapt to changes in the threat environment from day zero and target attacks in ways similar to the human immune system? Why can't our security infrastructure quickly adapt to changes in business and regulatory policy? We believe it can; however, significant change is required both from IT security vendors and IT security departments. This presentation will explore this vision and what is necessary to see it realised.

Tailored Security on a Budget: 'Off the Rack' Security is so 2008

Tom Scholtz

Today's security-conscious enterprise is compelled to buy many different, often overlapping, security functions in the form of hardware, software, and services. It is challenging to navigate the muddle of vendor marketing, solution packaging, and industry FUD to decide how best to derive value from capital and operational expenditures while maintaining adequate security. In ten years, the budget and security conscious enterprise will have the ability to build a dynamic services-based security architecture comprising 'push' and 'pull' services, paid from a master security debit account.

- How do enterprises overreact to the latest attacks?
- How can security budgets be impacted by large, panic-driven capital projects?
- What new delivery modes for information security will raise the security baseline?

Radically Transforming Security in a Virtualised World

Neil McDonald

Virtualisation offers an opportunity to radically transform our standard approaches to information security. On desktops and servers, the virtualisation layer can be used to perform introspection on hosted workloads - essentially delivering host-based IPS without agents. Trusted hypervisors, malcious code isolation and simulation, trusted compliance watchdogs and transparent deep packet inspection will all be enabled using virtualisation technologies.

- Will virtualisation help mitigate or exacerbate information security?
- How can virtualisation deliver host-based IPS without agents?
- Which security services are suitable for a virtualised approach, and which are not?

The Risk Management Activity Cycle

Ray Wagner

Risk management and risk-based activities cover security, risk assessment, business continuity, compliance, and privacy. IT departments are stretched trying to address the complexity and breadth of all these requirements. Gartner has developed an activity cycle that shows the relationship between these disciplines and embodies the best practices to execute them effectively and efficiently.

- What are the best practices to address security, privacy, business continuity, and compliance effectively and efficiently?
- How should you organise an effective risk management function?
- How do you know your organisation is effectively protected against reasonably anticipated threats?

Reinventing Security as an Application Service

Neil McDonald

Applications must become security aware. The next generation of service-oriented applications will require we deliver security as a set of on-demand services consumable by applications, configured via policy and enforced for compliance at run-time. This presentation will discuss Identity Services, SOA, BPMS, role-based access control and emerging capabilities for model-driven security in applications development.

- How will applications 'call' security on demand services?
- What are some examples of 'Security as an Application Service' today?
- Which vendors are best positioned for providing 'Security as an Application Service'?

Agenda subject to change

Special Features

Solution Provider Sessions

Get up-to-date with the latest Solution Provider offerings, strategies and best practices. Listen to case studies, new directions and real world examples of how the latest solutions provide results.

Sponsor's Showcase

At the Summit we'll help you develop a "short list" of technology providers who can meet your particular needs. We offer you exclusive access to some of the world's leading technology and service solution providers in a variety of settings before you commit valuable IT dollars. Visit the demonstration forum and attend the sponsor presentations.

Networking Reception

Attend the Networking Reception on Tuesday evening at 18.00 to meet and exchange ideas with like-minded delegates. A perfect networking environment and one you can benchmark against, as you swap notes and gain a deeper understanding of issues from a variety of perspectives.

> *"Fantastic session, addressing issues that are relevant in any business. As an employee of a tertiary institution this session provided a great amount of information about moving our security program forward and developing process maturity."*
>
> **Mark Zimmerli.** ICT Security Officer, University of Tasmania

Media Sponsors

as at 31 March 2008

AISA Australian Information Security Association

ASM AUSTRALIAN SECURITY MAGAZINE

ISACA® Serving IT Governance Professionals Sydney Chapter

SC MAGAZINE

Premier Sponsors

as at 1 June 2008

Gartner Events premier sponsor

IBM

McAfee®

Platinum Sponsors

as at 1 June 2008

ca

NOKIA

Novell®

Silver Sponsors

as at 1 June 2008

Canon advanced simplicity®

SOPHOS secured.

Pricing Options

Single Registration	Prices
Early Bird – Save AU$450! (Register & Pay by Friday 22 August 2008)	**AU$2,300.00** (inclusive of GST)
Standard Single	**AU$2,750.00** (inclusive of GST)

Team Registration	Prices
Early Bird Team 3 Advantage – Save AU$650 pp (Register & Pay by Friday 22 August 2008)	**AU$2,100.00** (inclusive of GST)
Early Bird Team 5 Advantage – Save AU$850 pp (Register & Pay by Friday 22 August 2008)	**AU$1,900.00** (inclusive of GST)
Standard Team 3 Advantage – Save AU$250 pp	**AU$2,500.00** (inclusive of GST)
Standard Team 5 Advantage – Save AU$450 pp	**AU$2,300.00** (inclusive of GST)

Register Online Now!

Web
gartner.com/ap/itsecurity

Enquire Now!

Email **gartner@infosalons.com.au**
Phone **1300 766 663** (within Australia) or
+61 2 9280 1295† (outside Australia)

Hotel Accommodation

Our accredited agency, Info Salons Australia Pty Ltd (ISA) & Accommodation Pty Ltd (ITA), can assist with your accommodation bookings. To take advantage of the Summit rates, contact ISA to complete your accommodation booking or to obtain further information.

For your travel requirements, please contact your designated travel agent.

Info Salons Australia Pty Ltd
ABN: 34 003 947 037

Office hours:
Monday to Friday 9.00am - 5.00pm – AEST

Phone: **02 9211 7222**
+ 61 2 9211 7222 (outside Australia)

Fax: **02 9211 1075**
+ 61 2 9211 1075 (outside Australia)

Email: **accommodation@infosalons.com.au**

Upcoming Gartner events, great solutions…

Service Orientated Architecture Summit	Tokyo, Japan	15-16 July
IT Governance Forum	Tokyo, Japan	3-4 September
Enterprise Architecture Foundation Seminar	Canberra, Australia	10-11 September
IT Security Summit	Singapore	19 September
	Sydney, Australia	23-24 September
Symposium/ITxpo	Tokyo, Japan	27-29 October
Symposium/ITxpo	Sydney, Australia	11-14 November
China Outsourcing Summit	Chengdu, China	18-20 November

For more information about Gartner's events, please visit **gartner.com/ap/events**