

# How exposed are you?

## Gartner IT Security Summit 2008 Ensuring the Future Security of Information

29 SEPTEMBER – 1 OCTOBER 2008 ROYAL LANCASTER HOTEL, LONDON  
[europe.gartner.com/security](http://europe.gartner.com/security)

### GARTNER SUMMIT CHAIRS



**Jay Heiser**  
Research VP



**Tom Scholtz**  
Research VP

### KEYNOTE SPEAKERS



**Joseph Feiman**  
VP & Gartner Fellow



**Neil MacDonald**  
VP & Gartner Fellow



**John Pescatore**  
VP Distinguished  
Analyst, Gartner



Special Guest:  
**Science Fiction**  
Author, Ken MacLeod



Prof. Ross Anderson,  
Professor of Security  
Engineering,  
**Cambridge**  
**University**



Gordon Irving,  
Director Group  
Security,  
**Scottish Power**



Martin Smith,  
Chairman and Founder,  
**The Security**  
**Awareness Special**  
**Interest Group**

**Gartner**  
IT Security  
Summit 2008

# Ensuring the Future Security of Information

## Introduction from the Summit Chairs

New technologies, delivery models and digital ways of doing business mean that even successful security efforts are rapidly becoming obsolete. End users want to store sensitive data on a growing variety of inexpensive and powerful consumer and mobile devices. New software and service delivery models offer significant economic advantages... But only by taking your valuable information out of your data centre and out of your control. At the same time the business is demanding new and riskier services; partners and regulators are demanding ever higher levels of control and transparency.


Managing information risk today means looking ever further into the future. Increasingly mobile and distributed technologies, along with employee-owned devices, will require new forms of monitoring and data protection. Internet-based applications and services that store and process valuable information outside of your organization will need new levels of responsibility on the part of business managers. Regulations against data leakage will only be met through unprecedented levels of security awareness and information expertise on the part of the end user.

It is obvious that 'business as usual' is not an option. Security practices must become more aligned with business requirements. The emphasis must become less controls-focused, and more focused on the desired business outcomes of risk management decisions. Technology innovations such as virtualization and policy modelling offer unique opportunities for more effective policy enforcement, but acquiring and applying 'soft skills' around awareness, culture, communication and behavior will continue to be a challenge.

At the Gartner IT Security Summit, we will not only be highlighting today's most successful security, business continuity and compliance technologies and practices, but we will help you plan and position yourself for the challenges of tomorrow.

Gartner analysts, end user case presenters, and other industry experts will be providing you with their vision for the next decade of information protection. Learn how to create and implement your own roadmap to a more mature future.



  
**Jay Heiser**  
Research VP



  
**Tom Scholtz**  
Research VP

## Benefits of Attending

- **Take Control of Your Future:** gain knowledge to better serve your business needs
- **Up-to-the-Minute Gartner Insights:** enhance your knowledge with the latest analysis
- **Private Consultation:** book 30 minutes one-on-one consultation with a Gartner analyst
- **Gather the Latest Intelligence:** by booking an Analyst / User Roundtable seat
- **Learn From Industry Leaders:** delivering operational experience through in-depth case studies
- **Access Key Solution Providers:** evaluate offerings from leading vendors in the Summit exhibition
- **Maximize Networking Value:** through "Event Connect" allowing you to message other delegates onsite
- **Share Experiences:** with peers from your industry, across Europe, or cross-industry
- **Share Learning:** with colleagues by downloading all session slides from the website
- **Enhance Your Learning:** by purchasing the sessions, with live audio, on DVD

## KEY TOPICS

The Conference Will Focus on the Latest Issues for Security Professionals:

- Cutting the **COST** of information security
- Eliminating **COMPLIANCE** difficulties
- Managing your **RISK** profile
- Creating appropriate **IDENTITY** and **ACCESS** approaches
- Securing **MOBILE** data, application and devices
- Resolving **PRIVACY** issues within your organization
- Supporting and ensuring **BUSINESS** buy-in
- Designing **RESILIENCE** and **CONTINUITY** for your organization
- Implementing **VIRTUALIZATION** securely
- Identifying **OUTSOURCING** and **MANAGED SERVICE** opportunities
- Enhanced **GOVERNANCE** practices
- Preparing for security in the **WEB 2.0** era
- Adapting to the **CONSUMERIZATION** megatrend
- Ensuring security in **VIRTUAL WORLDS** and **SOCIAL SPACE**
- Developing **ARCHITECTURE** for holistic defense

## The NEW TRACKS for 2008

### 4 Tracks targeting all your key vulnerabilities:

# 1

#### Protecting the Infrastructure

The IT infrastructure will continue to evolve and security solutions must keep pace. History teaches us that future architectures, applications, platforms and networks will bring new vulnerabilities. But if we learn from the past, we can anticipate these risks, integrating security into the infrastructure.

# 2

#### Protecting the Data and Applications

Embarrassing news reports about data losses, and waves of identity theft highlight the need to protect data and applications more stringently. Today's methods may be flawed and costly. Tomorrow's data protection should be more uniform and economical to deploy and manage.

# 3

#### Governance and Security: Risk Management Strategies

Governance and management fads come and go and new approaches may be more effective than what we've done in the past. Will end users ever learn to safely use computers, or will strict controls over behaviour always be required? Organizations will need to carefully apply lessons learned in order to cost-effectively control the risks associated with information and technology.

# 4

#### Business Impact and Resilience

For most organizations today, a partial reduction in IT function can be hugely costly, and many companies are ill-prepared to recover from an IT disaster. Contingency planning for losses of information and functionality is increasingly being understood as a business imperative.

### DAY THREE: BEST PRACTICES AND IMPLEMENTATION DAY

A day devoted to operational best practices, implementation strategies, key methodologies and practical case studies. Also take part in the Gartner Magic Quadrant power session and closing panel debate. Day Three delegates only will be able to access all these presentations post-Summit and benefit from the additional networking and presentations.

### Who Should Attend

This event is open to both Gartner clients and non-client organizations.

It is aimed at senior IT professionals with a brief to support the business and drive innovation including:

- CIOs, CTOs, CISOs, VPs, directors, IT security officers, enterprise security architects, network managers, risk managers, internet security managers, business continuity managers, security analysts and consultants and all other professionals with an interest in security decisions

As well as representatives from leading suppliers of solutions, products and services.

# Meet the Analysts

Worldwide Expertise at Your Fingertips –  
Your Questions on Security Strategy Answered!

For over 25 years, Gartner analysts have been the trusted advisors to many of the world's largest and most demanding organizations. 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 clients worldwide. The value of this resource, combined with our deep analysis of technology vendors, is unrivaled. Gartner's IT Security Summit brings a level of experience and expertise that you simply cannot get anywhere else.



**Ant Allan**  
Research VP

*"Identity and access management is far more than just a set of tools. Success requires a strategic approach with an activity cycle that orchestrates people and processes as well."*

**Focus Areas:** Enterprise and consumer user authentication; password management, ESSO, user provisioning, role life-cycle management, authorization management.



**Christian Byrnes**  
Managing VP

*"As the function we used to know as Information Security achieves alignment with business needs, it becomes viewed as a significant aspect of Operational Risk Management."*

**Focus Area:** Risk program management.



**Carsten Casper**  
Research Director

*"Violating privacy laws is more than crossing a red light. Protecting privacy is more than just buckling up. Manage privacy, not the law."*

**Focus Areas:** Privacy legislation, EU and cross-border privacy, privacy certifications, compliance.



**Ruggero Contu**  
Principal Research Analyst

*"Driven by issues such as data privacy, compliance and perceived risk of damage to business, organizations in Europe are showing increasing interest in security technology and services; however differences within geography, vertical industry and company size are significant and will influence security strategy and spending across products."*

**Focus Areas:** Security market trends, forecasts, vendor dynamics and end users' wants and needs.



**Joseph Feiman**  
VP & Gartner Fellow

*"Application security is a preemptive action unlike network security which is a defensive action. You cannot win a war with defenses only."*

**Focus Areas:** Application security; technologies and methodologies that enable developing secure applications.



**Peter Firstbrook**  
Research Director

*"Organizations are under a continuous barrage of malware from the web and email. Multiple products and procedures across multiple IT disciplines are necessary to effectively defend the enterprise."*

**Focus Areas:** Antivirus, antispware, antispam, email security.



**John Girard**  
VP Distinguished Analyst

*"No matter how complex it seems to manage mobile company and personal devices, good planning will keep you out of the headlines and out of the courts."*

**Focus Areas:** Wireless network security, mobile device management and security, mobile data encryption/privacy, mobile user authentication, remote access VPNs.



**Arabella Hallawell**  
Research VP

*"Most companies today operate at extremes when it comes to security and global sourcing. But under or overestimating the role and costs of security is bad for business."*

**Focus Areas:** Privacy, international issues, email security and antispam, acceptable use policies, web filtering.



**Jay Heiser**  
Research VP

*"The new IT risk challenge is in controlling the use of your information, even when it is being used on someone else's computer."*

**Focus Areas:** Trust communities, risk management, compliance, forensics & investigation.



**Debra Logan**  
VP Distinguished Analyst

*"Better information governance is the key to better information security and data protection."*

**Focus Areas:** Information governance, enterprise information management, e-discovery, records management, enterprise content management.



**Neil MacDonald**  
VP & Gartner Fellow

*"Antivirus and personal firewalls are no longer sufficient for comprehensive endpoint protection."*

**Focus Areas:** Antivirus, host-based intrusion prevention and application security including ERP separation of duties.



**Mark Nicolett**  
VP Distinguished Analyst

*"With the rise in targeted attacks, IT organizations need to get better at finding and fixing security weaknesses before they are exploited, and need to more quickly discover patterns of inappropriate resource access."*

**Focus Areas:** Security information and event management; vulnerability management, IT GRC management.



**John Pescatore**  
VP Distinguished  
Analyst

*"Both threats and business models keep changing. Successful businesses will have security programs that move rapidly to neutralize new threats and to support new business initiatives."*

**Focus Areas:** Internet security, intrusion prevention, wireless security, network access control, metrics.



**Paul Proctor**  
VP Distinguished  
Analyst

*"Security and risk teams are shifting from security based on available budget to making business-orientated decisions to hit pre-determined targets of residual risk."*

**Focus Areas:** Security program management, audit and compliance, network security, risk management, content monitoring and filtering.



**Tom Scholtz**  
Research VP

*"The new version of ITIL has the potential to dramatically impact the way security is engineered into IT and business services. Are you ready for it?"*

**Focus Areas:** Security strategy/architecture, security organization, investment justification, secure outsourcing, ITIL security.



**Les Stevens**  
Research Director

*"Despite receiving high attention from senior executives and internal and external auditors, infosec departments still seem to struggle to establish relevant and enforceable policies."*

**Focus Areas:** Policies, risk management and assessment, security strategy, security organization; BCP/DRP.



**Andrew Walls**  
Research Director

*"At its core, information security is about anticipating, controlling and reacting to human behavior. Security tools work best when configured and managed to compensate for the patterns of behavior that are exhibited by users."*

**Focus Areas:** Security markets and issues, security management, governance and compliance, policy, risk management.



**Vic Wheatman**  
Managing VP

*"The key to a successful program is business alignment; many organizations focus on answers before they identify the questions that need to be asked."*

**Focus Areas:** Security organization, metrics, program maturity measurement, risk assessment.



**Roberta Witty**  
Research VP

*"Identity and access management solutions control the keys to your information kingdom. If you do it well, no one notices. If something goes wrong, everyone knows."*

**Focus Areas:** Identity and access management, business continuity management.

## YOUR ACCESS TO THE ANALYST COMMUNITY

Tackle your toughest challenges – registered delegates are extended the opportunity to book a complimentary, private 30 minute consultation with Gartner Analysts. You can ask questions about the analyst's presentation, or address specific issues within the analyst's area of expertise.

# Keynote Speakers



**Joseph Feiman**  
VP & Gartner Fellow  
Gartner

Joseph Feiman is a Vice President and Gartner Fellow in Gartner Research. Mr. Feiman focuses on applications security, technologies and methodologies enabling secure software life cycle, data privacy, security of large systems and packaged applications, legacies, SOA, Web 2.0, and security as a service.

Mr. Feiman's research earned him a Gartner Thought Leadership Award for two consecutive years — 2003 and 2004. His background includes system and application programming, research and development, and management and consulting.



**John Pescatore**  
VP Distinguished Analyst  
Gartner

John Pescatore is a Vice President and Gartner Fellow with 24 years experience in computer networks and information security.

Mr Pescatore is Gartner's lead analyst on all Internet-facing security issues, covering a broad range of enterprise critical areas. He also provides thought leadership in wireless security, ways to develop software without vulnerabilities and trustable computing platforms.

He is frequently quoted in such publications as BusinessWeek Online, InformationWeek, ZDNet, Computerworld, VNUnet Newswire, Business Wire and InforWorld Daily News.



**Professor Ross Anderson**  
Professor of Security Engineering  
Cambridge University

Ross is a co-founder of a new discipline; the economics of information security. Many security failures can be traced to wrong incentives rather than technical errors, and the application of microeconomic theory has shed new light on many problems that were previously considered to be intractable. The work is particularly important for understanding cyber-crime and online liability. It is also giving insights into system safety and dependability, and more traditional security problems. Ross also made seminal contributions to peer-to-peer systems; hardware tamper-resistance; emission security; copyright marking; crypto protocols; and the security of APIs. He chairs the Foundation for Information Policy Research and is a Fellow of the IET and the IMA.



**Gordon Irving**  
Director of Group Security  
Scottish Power

Prior to joining Scottish Power (now part of Iberdrola), Gordon spent 30 years in Strathclyde Police attaining the rank of Chief Superintendent. He was Head of Special Branch and latterly a Police Commander in Glasgow responsible for 800 officers and staff. Gordon has extensive experience in Counter Terrorism including involvement in the UK Counter Terrorism program. Gordon was also a senior investigating officer heading several murder enquiries. In addition to his security role Gordon is responsible for Business Continuity Management and Crisis Management across the group. Since 2001 Gordon has developed and implemented a strategy, framework and policy embedding business continuity into each business area alongside his work advocating and personally sponsoring a security awareness program within the organization.



**Neil MacDonald**  
VP & Gartner Fellow  
Gartner

Neil MacDonald is a Vice President, Distinguished Analyst and Gartner Fellow in Gartner Research. Mr. MacDonald is a member of Gartner's information security and privacy research team, focusing on operating system and application-level security strategies.

From 2001-2003, Mr. MacDonald led Gartner's worldwide team of industry-focused analysts, extending Gartner's research relevancy outside of the IT department to business executives wanting to use information technology to better run their business. When this research team was folded back into the main research organization in 2004, Mr. MacDonald rejoined the Information Security research team.



**Martin Smith**  
Chairman and Founder  
The Security Awareness  
Special Interest Group

Martin gained his degree in behavioral psychology before spending 15 years as a commissioned officer in the RAF as a pilot and then in counter-espionage and counter-terrorism duties. After being awarded membership of the Most Excellent Order of the British Empire (MBE) for this work, he left the Service to carve out a career in the commercial sector. He joined Touche Ross Management Consultants before becoming the Senior Director of Corporate Security for Kroll Associates. He then joined Standard Chartered Bank as Head of Information Security before forming his own specialist consultancy The Security Company (International) Limited renowned for implementation of effective security awareness campaigns for major corporations around the world.



**Special Guest**  
Science Fiction Author  
Ken MacLeod

Ken was born in Stornoway, Isle of Lewis, Scotland, on August 2, 1954. He is married with two children and lives in West Lothian. He has an Honours and Masters degree in biological subjects and worked for some years in the IT industry. Since 1997 he has been a full-time writer. He is the author of eleven novels, from The Star Fraction (1995) to The Night Sessions (forthcoming, 2008), and many articles and short stories. His novels have received one BSFA award and three Prometheus Awards, and several have been short-listed for the Arthur C. Clarke and Hugo Awards. Ken MacLeod's weblog is "The Early Days of a Better Nation" <http://kenmacleod.blogspot.com>

## AT A GLANCE SCHEDULE

### Monday 29 September

- 06.30** Delegate Registration
- 08.00** Morning Tutorials
- 09.10** Conference Opening & Welcome Presentation
- 12.30** Lunch & Solution Showcase
- 18.00** Networking Drinks Reception

### Tuesday 30 September

- 08.30** Opening Sessions
- 12.00** Lunch & Solution Showcase
- 16.10** Conference Close

### Wednesday 1 October Best Practices & Strategy Implementation Day

- 08.10** Opening Sessions
- 12.35** Lunch & Networking for Country and Industry Peer Groups
- 17.00** Conference Close

## MORNING TUTORIALS

New starter in the field and need to get up to speed? Or an experienced leader wanting a refresher on the latest issues? In 2008 book your place for a Gartner tutorial and learn core information to ensure your grip of emerging themes and latest opportunities.

### Basics of Vulnerability and Patch Management

An effective IT Security program requires processes and technologies that span Operations and Security. Collaboration and coordination are needed in areas such as vulnerability configuration, patch, and event management. Come learn about which operations and technologies are converging and ways to implement effective security configuration and patch management processes.

What are the components of an effective vulnerability management program?  
How can operations processes and technologies be applied to solve problems?

**Peter Firstbrook and Mark Nicolett, Gartner**

### Mobile Management and Security Convergence: Strategies for Success, Tactics for Progress

Mobile device utilization continues to rise rapidly at many levels. Vendors offer an overlapping, complex, expensive and confusing set of security choices. This presentation provides actionable advice and indicates the smart choices for the future

What are the drivers for the security and management of mobile devices?

How will the security configuration and mobile management markets for laptops and small devices evolve?

What are best practices in mobile device management?

**John Girard, Gartner**

### Managing Risk Using Gartner Risk Assessment Method

Assessing information security risk is often spoken about but seldom consistently applied. A systematic approach is needed that assimilates risk related information to facilitate appropriate risk mitigation. The Gartner Delphic Risk Assessment Methodology is such an approach.

What is GRAM and what can I use it for?

How do I identify and analyze risks using GRAM?

How do I mitigate and track risks using GRAM?

**Les Stevens, Gartner**

## PLENARY SESSIONS

### Gartner Keynote I: Building a Real-Time Adaptive Security Infrastructure

Security infrastructure must become adaptive to changes in business policy and the environment. Why can't our security infrastructure quickly adapt to changes in the threat environment in ways similar to the human immune system? Why can't our security infrastructure adapt to changes in regulatory policy? We believe it can. However, significant change is required both from vendors and security departments. This presentation explores this vision and its realization.

**Neil MacDonald, VP & Gartner Fellow, Gartner**

### Gartner Keynote II: Color of Security in 2018: Dark, Bright, or Grey?

Web X.O, the myriad of applications and websites created by non-IT professionals, will be challenging to secure. Globally distributed applications will be difficult to firewall. Yet, security start-ups will continue innovate, and software services and packages will be coming out of assembly with imbedded security protection features. Gartner analysts will debate whether we will be more secure in 10 years.

**Joseph Feiman, VP & Gartner Fellow, Neil MacDonald, VP & Gartner Fellow, John Pescatore, VP Distinguished Analyst, Gartner**

### Security Market Players: Magic Quadrant Power Session

Meet the Gartner analysts at their best – ad hoc on stage. Ask questions about vendors or tools. Hear the Gartner position on key technology providers in Security Information and Event Management, User Provisioning, Content Monitoring and Filtering, Data Loss Protection, Personal Firewalls and Mobile Data Protection – unscripted, unfiltered, unbiased.

Who is hot? Who is not?

Which vendors will survive consolidation?

Which vendors understand where the market is going?

**Mark Nicolle, VP Distinguished Analyst, Peter Firstbrook, Research Director, John Girard, VP Distinguished Analyst, Paul Proctor, VP Distinguished Analyst, Gartner**

**EXTERNAL KEYNOTES**

**20/20 Keynote: The Mark 1 Human Being – Your Biggest Danger or Your Strongest Asset in the Fight to Improve Information Security**

Promoting long-term behavioral change across the organization is the key requirement for delivering effective security. To do so requires an appropriate business case and a very strong aware of the human vulnerabilities that hamper delivery of robust security. In a unique two part keynote, security guru Martin Smith will present a unique perspective on how to innovate awareness and reduce security breaches to be followed by Scottish Power's Director of Group Security, Gordon Irving, who will describe how to ensure this happens in practice.

- How have human factors become such a key concern?
- A short tour around recent data security breaches
- The importance of senior management support

**Martin Smith**, Chairman and Founder, **The Security Awareness Special Interest Group** and **Gordon Irving**, Director of Group Security, **Scottish Power**

**Sci-Fi Plenary: Hack the Future – All Your Firewalls Are Belong to Us**

Computers, the Internet, and even computer viruses were once science fiction. Today they're reality, but they're changing reality all the time. The amount of computer power you can buy for a thousand pounds continues to double every eighteen months. This exponential progress takes us into 'science fiction' territory faster than we think. Let a science fiction writer take you on a virtual tour of tomorrow, and see how the challenges of the coming decades are already being wargamed in the science fiction of today.

- What's sure to happen? What could happen? What could happen that we can't expect?
- What can IT security learn from its enemies: hackers, spammers, and people who store passwords on Post-IT notes?
- Do the biggest risks to your system come from outside the IT world entirely?

**Ken MacLeod**, Science Fiction Author

**Guru Keynote: Security Economics And Beyond**

The economics of information security has recently become a thriving and fast-moving discipline. As distributed systems are assembled from machines belonging to principals with divergent interests, incentives are becoming as important to dependability as technical design. There has been recent ground-breaking research on:

- Computer crime, including spam, phishing and other scams
- Dependability, including the economics of bugs, patching, antivirus products and website takedown services
- Privacy - what people really care about, and what will turn them against companies or governments

**Prof. Ross Anderson**, Professor of Security Engineering, **Cambridge University**

From EU level policy, to the legal landscape for compliance, to the evaluation of your career prospects and rightful salary demands – achieving optimum position in your chosen profession requires a broad awareness of industry settings. To compliment the case study content this year's agenda also features a number of positional sessions regarding broader issues.

**Legal Perspective:  
Zen and the Art of International Data Protection Compliance**

Complicated contracts, SLAs, guidance notes, and a universe of lawyers claiming the sky is falling, all add to confusion over data protection compliance. But we can find our way towards a reasonably calm compliance philosophy.

- What is the simplest compliance strategy when off-shoring personal data?
- Why are my service agreements getting cluttered up with data protection clauses?
- How can I keep the lawyers under control on international data transfer deals?

**Robert Carolina**, Principal, **Origin Solicitors**

**European Policy:  
Strategic Issues for Data Protection in Europe - a Perspective from the European Data Protection Supervisor**

Data protection and information security are increasingly relevant for organisations, both in public or private sector, whether operating online or off-line. Preserving the trust and confidence of clients and protecting a good reputation have become strategic issues of prime importance. This presentation will address how to approach issues such as:

- Security breach notifications
- Need for more global privacy
- The future of Directive 95/46/EC

**Peter Hustinx**, **European Data Protection Supervisor - EDPS**

**Professional Development:  
Career Advice for Security Professionals - Your Salary in 2008 – What's the Real Story?**

The managing director of a major recruitment specialist will answer your key question – "I am a \_\_\_\_\_ what should I be paid?" In partnership with the Institute of Information Security Professionals a new independent survey is able to show you the quick and honest answer:

- What do people in my role REALLY learn?
- What is the present position by sector, responsibility and title?
- Where are salaries going?

**Iain Sutherland**, **Managing Director**, **Information Security Solutions**

## END-USER CASE STUDIES

Compliment your strategic knowledge of key areas by attending out end-user case studies designed to show actual projects; how they have worked in practice, what obstacles were overcome and what tactics have been adopted. Make comparisons, benchmark your work and learn what will work for you.

### Embedding an Effective Privacy Compliance Program in Accenture

Accenture is a pioneer in developing Binding Corporate Rules for data privacy and protection. Accenture is now focusing on building a client data protection program. The session will describe development and implementation of the program, the building blocks and steps being taken to protect personal data.

- 7 elements of an effective data privacy program
- Handling Accenture and client personal data
- Ensuring stakeholder buy-in

**Bojana Bellamy**, Global Data Privacy Compliance Lead, **Accenture**

### Secure Integration in a Heterogeneous Environment: Solutions at Handelsbanken

Information within the business has become ever more fragmented yet demand continues to rise for ever more complex integration of that information. This session charts work to ensure higher traceability, accountability and non-repudiation:

- How can you maintain accountability in complex transaction flows?
- How do you meet the needs of multiple methods of authentication?
- How do you trace a transaction back to a user with acceptable levels of non repudiation?

**David Böling**, IT Architect, **Handelsbanken**

### Who Am I and How Do I Prove It? Identity Management at HBOS

Identity management is becoming an ever greater issue both for businesses and customers, especially in online environments. This session will discuss both the issues and a model that could potentially resolve some of the problems.

- How can you prove who you are?
- How can businesses verify your identity?
- What can we, as information security professionals, do to improve identity management and reduce identity theft?

**Jim Brady**, Senior Information & IT Risk Analyst, **HBOS**

### Measuring the Implementation Status of Information Security at Amadeus

To gain support for information security, we need to show value and the progress of implementation. In case of information security hard facts alone, are not sufficient you also have measure the soft facts.

- What are the challenges for measuring information security?

- How to judge the maturity of a security organization
- What KPI makes the difference?

**Roland Ficht**, Director Infrastructure and Corporate Information Security, **Amadeus**

### Implementing Information Management Policies: the Approach at the Welsh Assembly Government

High profile data losses have put a spotlight on information handling within organizations, whilst robust information management policies are in place, compliance checks and audits sometimes show that the application of policies is patchy. Unless those working in organizations adhere to policies and best practice then there is a risk of compromise and loss of information assets. The presentation will explore:

- Role of leaders
- Role of training
- Role of assurance

**Dr Michael Harrington**, Director Corporate Information and Services, **Welsh Assembly Government**

### Building an IT Security Masterplan for Performance and Profit in the Republic and Canton of Jura

This session focuses on how we built its 2008-2010 IT security masterplan taking into account emerging trends, resource management, budget demands and the strategic vision of the organization.

- How did we set about prioritizing the needs and assessing the risk levels of all sixty departments?
- What methods did we adopt to ensure IT staff motivation?
- How did we obtain the commitment of the Government for our masterplan?

**Bruno Kerouanton**, Head of IT Security, **Republic and Canton of Jura**

### 'Taming of the Shrew': Diageo's Work to Secure Tomorrow's Enterprise and Mitigate Today's

The challenge is to deliver a cost effective solution for security and risk that releases business value. A solution that is simple to implement, cross-functional in impact and easier to get buy-in will always win hands down.

- How much compliance is too much?
- How do we turn security from business barrier to business driver?
- What part will end users play in the solution for this new type of workforce?

**Dr Claudia Natanson**, Chief Information Security Officer, **Diageo**

### Negotiating an Information Security Policy Through the Approval Process at the Organization for the Prevention of Chemical Weapons

This discussion will center on how to gain the organizational mandate for creating an information security policy. The talk will examine best practices in information security policies and practical advice on how to negotiate a policy through the approval process.

Getting organizational backing  
How laws, regulations, culture and mission combine to shape the policy  
How to successfully negotiate the policy through the bureaucratic maze

**Paul S. Raines**, Head, IT Information Security, **Organization for the Prevention of Chemical Weapons**

### Information Security Audits as an Accepted Business Support Tool at Novartis

Audits are often seen as a threat and organizations sometimes prepare by 'window dressing' whilst trying to hide deficiencies, risks and compliance issues. This presentation describes how audits can be a valuable component of risk management efforts.

- A risk-focused and business-integrated approach to auditing
- Pros and cons of this risk management component
- Describing how to transform 'normal' audits

**Manfred Schreck**, Head of Group Information Security, **Novartis**

### The Drive for True Mobility: Answering the Requirement for High Availability and Redundancy to Maintain Critical Information Access at Vodafone

Mobility and globalization have been a disruptive influence on the way businesses work. This presentation will look at the steps Vodafone have taken to protect their mobile access to email and critical business information, even if critical IT facilities are down.

- Accommodating planned or unplanned downtime in security planning
- Ensuring protection of your chosen mobility platform
- Operational measures to prevent disruption of critical services and systems

**Paul Stonadge**, Head of Professional Services, **Vodafone**

## CONTENT PARTNERSHIP WORKSHOPS

To enhance the range of knowledge and information available to delegates, Gartner has invited three key authorities in the information security field to contribute content to the 2008 Summit. ISACA, (ISC)<sup>2</sup>, and the SANS Institute will be running workshop sessions as part of the Best Practices and Implementation Day.

### SANS Institute Workshop: Frontline Solutions for Security Professionals

This presentation begins with the foundation of a defense-in-depth approach to security and covers methodology for practical application. Using real-world examples we highlight areas where vulnerabilities are most likely to occur.

- Outlining a best practices approach to incident handling and forensics
- Employing foundational concepts to your organization to avoid common IT pitfalls
- Guidance on mitigating vulnerabilities and related exposures

### SANS Institute Breakout: Latest Trends in Computer Hacking

The systems containing your most vital information are under attack every day. To properly protect these systems you need to understand the attacker's tactics and strategies.

- Identifying key methods used by hackers
- Indicating attack vectors currently being exploited
- Demonstrating ways you can protect your vital data from these attacks

**Jess Garcia**, SANS Certified Instructor, **SANS Institute**

SANS is the most trusted source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security. Its programs now reach more than 165,000 security professionals. A wide range of individuals are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.



(ISC)<sup>2</sup> members can receive up to 24 CPE Credits for attending the Summit.

### ISACA Workshop: COBIT and Val IT for the Security Professional

COBIT and Val IT are effective governance frameworks designed to support the implementation and fulfillment of the security function within the organization. Roger Southgate, ISACA's President IT Governance Standards and leader of the London COBIT Development Group will cover:

- An introduction to the COBIT and Val IT frameworks
- Drilling down into the support available for information security
- Exploring the resources of value to IT professionals

**Roger Southgate (CISM, CISA, FCCA, MBA)** Leader, **London COBIT Development Group** and President, IT Governance Standards, **ISACA**

ISACA, previously known as the Information Systems Audit and Control Association, now goes by its acronym only, to reflect the broad range of IT governance professionals it serves. The Certified Information Security Manager® (CISM®) certification program launched in 2002 and developed specifically for experienced information security managers, and those who have information security management responsibilities has added impetus to the growth in ISACA membership worldwide to more than 75,000 since its inception in 1967. ISACA's strong chapter network provides local support and networking opportunities via more than 175 chapters located in over 70 countries.



### (ISC)<sup>2</sup> Workshop: Managing Careers as Well as Risks

Drawing on (ISC)<sup>2</sup> experience as a member organization representing over 60,000 professionals worldwide, this session will examine issues around acquiring the right personnel, managing skills obsolescence and other developing requirements of a mature Information Security operation.

- Growing choices for people working in the field
- The changing workforce profile and evolution of accountability
- Incentives for gaining and retaining talent

**John Colley**, Managing Director EMEA, **(ISC)<sup>2</sup>**

The International Information Systems Security Certification Consortium, Inc. - (ISC)<sup>2</sup>® - is the globally recognized Gold Standard for certifying information security professionals. Founded in 1989, (ISC)<sup>2</sup> has certified over 60,000 information security professionals in 135 countries. (ISC)<sup>2</sup> issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, Certification and Accreditation Professional (CAP®), and Systems Security Certified Practitioner (SSCP®) credentials to those meeting necessary competency requirements. The CISSP, CISSP-ISSEP®, CISSP-ISSAP® and SSCP are among the first information technology credentials to meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel.



## Track 1 Sessions: Protecting the Infrastructure

### Mobile Security Megatrends: Future Strategies to Avoid Worst-Case Scenarios

Enterprises are vulnerable because mobile access standards continue to evolve. Understanding the architecture, integration and security strategies will enable enterprises to stay ahead of users' demands for new technologies and remote access capabilities.

What strategies, best practices and technologies will enable wireless and mobile security?

What integration will assure secure use of mobile technologies?

How will future standards and technologies affect today's mobile enterprise security approaches?

**John Girard, Gartner**

### Real Security for Virtual Social Spaces

Virtual worlds and social networks are merging into complex, geographically distributed social and business interaction environments. Unless controlled, the opportunity of new markets and enhanced customer interaction and collaboration might be overcome by corporate and individual security risks.

How do physical, personnel and IT security skills apply in the virtual world?

How do you prepare your staff for hostile interactions within virtual environments?

What level of risk mitigation do the vendors provide?

**Andrew Walls, Gartner**

### Activity Monitoring Across the Cloud

IT service and cloud based delivery methods complicate user activity monitoring and resource access becomes critical and more complex. Safe use of networks and applications will require monitoring and analytical technologies and services.

How will monitoring requirements evolve over the next decade?

Which technologies can be used for monitoring cloud-based services?

How do you analyze user activity data across the cloud?

**Mark Nicolett, Gartner**

### Network Security Scenario

Encrypt, inspect, block and don't slow it down and the network gets increasingly more difficult to secure. But as the network gets more application and user-aware, network security can take major steps forward. Learn how to secure the network today and leverage new network security capabilities without breaking the budget.

How is the security infrastructure market evolving?

What are the most effective technologies and best practices?

**John Pescatore, Gartner**

### Securing the End Point

Cyber criminals are increasingly successful, malware proliferation is at an all time high, targeted attacks and zero day threats are increasing. Attackers are improving faster than AV vendors and enterprises can't adopt new HIPS and firewall technologies fast enough.

What are the trends in malware development?

Which technologies and practices will protect networks?

What will future end point protection platforms look like?

**Peter Firstbrook, Gartner**

### The Next 10 Years in Secure Messaging

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 can you prevent the introduction of malware through messaging vectors?

What procedures are relevant to monitoring employee email?

What are the most effective methods of implementing proper levels of messaging hygiene?

**Ababella Hallawell, Gartner**

### Best Practices in Network Access Control

Interest in NAC remains high, but adoption has been slow. We review common technical, political and operational obstacles to NAC and how to overcome them. We also explore how building identity awareness into networks will impact NAC during the next 10 years.

What is the status of NAC today?

What role will Cisco, Microsoft and other vendors play in advancing NAC?

Where and how should you start deploying NAC in your network?

**John Pescatore, Gartner**

### Security in the Age of Web 2.0

Web 2.0 will be an enormous challenge to enterprises' security. Individuals will become developers and get free access to attack machines, theft enablers and enterprise-strength technologies. This presentation analyzes Web 2.0 security threats and vulnerabilities, ways to protect enterprises' and individuals' applications, and changes that enterprises should undergo to meet security challenges.

What makes Web 2.0 applications insecure?

What processes and technologies will secure Web 2.0?

**Joseph Feiman, Gartner**

### How to Securely Implement Virtualization

Virtualization offers an opportunity to radically transform our standard approaches to information security. Trusted hypervisors, malicious code isolation and simulation, trusted compliance watchdogs and transparent deep packet inspection will all be enabled using virtualization techniques.

Will virtualization help mitigate or exacerbate information security?

How can virtualization deliver host-based IPS without agents?

Which security services are suitable for this model in what timeframe can they be adopted?

**Neil Macdonald, Gartner**

## Track 2 Sessions: Protecting the Data and Applications

### Securities of Legacies, Big Applications and Databases

Legacy applications, packaged systems and databases are valuable assets that should be protected against external and insider attacks. They have thousands of distributed users and are no longer confined to a secure data center.

What are the security risks that major enterprise assets are facing?

What processes should be put in place to protect them?

What new technologies and vendors will enable better security?

**Joseph Feiman, Gartner**

### Reinventing Security-as-an-Application Service

The next generation of service-oriented applications will require security delivered as on-demand services, configured via policy and enforced at run-time. We discuss Identity Services, SOA, BPMS, RBAC 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?

**Neil MacDonald, Gartner**

### Managing Legacy Content to Decrease IT Costs and Reduce Business Risks

Ignoring legacy data and content costs money and resources, and leads to regulatory and legal exposure. E-mail archiving, content management, records management, backup and recovery, and proactive information management must be part of your information management strategy.

Who has information retention management responsibility?

How do you effectively manage the costs and risks of undisciplined information management?

How can you use process discipline, technology and best practices to manage legacy information?

**Debra Logan, Gartner**

### The Identity and Access Management Scenario

IAM remains a cornerstone of secure business enablement. Managing users' identities and their access rights is becoming increasingly centralized and abstracted from the infrastructure, improving security efficiency and effectiveness and enabling business.

What is IAM and what problems does it solve?

What are the security, risk management and business benefits of IAM?

What are the key elements of a successful IAM program?

**Ant Allan, Gartner**

### The Future of Database Security

Databases continue to grow in size and importance as organizations move more and more data into them. But efforts at securing them have lagged behind: we need to take further steps to provide the necessary security.

Why are databases so important from a risk perspective?

What are some of the limited steps we have taken to protect these core assets?

What can we do to make them more secure?

**Mark Nicolett, Gartner**

### Using Data Loss Prevention to Detect Sensitive Data Enterprise-wide

Content Monitoring and Filtering/Data Loss Protection technologies are increasingly common compliance tools for many organizations. However, many 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 leaders in each market segment?

What 5 points must organizations consider when deploying CMF/DLP solutions?

**Paul Proctor, Gartner**

### Will Security and Portability Mix? New Criteria for Virtual Data Loss Prevention

Every company is struggling with demands for portable information access. Data loss prevention is failing under an avalanche of portable media devices and internet portals. Demands far exceed legacy remote access needs.

How can corporate data be productively used on noncorporate workstations?

What decision factors determine the best methods for secure, portable remote access?

Which vendors enable enterprises to reliably enforce security policies and standards on non-corporate workstations?

**John Girard and Jay Heiser, Gartner**

### Do You Know Where Your Data Are? Data Security in the World of Geographically Distributed Processing and Storage

Outsourced data storage and processing offers significant benefits but also introduces security risks. The outsourcer's security, the stability of the host countries and potential surveillance expose corporate business processes to significant risks.

How can the security of corporate data and processes be assured in remote environments?

What regulations and laws apply to transborder data flows?

Can the movement of data in an outsourced environment be monitored by the client?

**Andrew Walls, Gartner**

### Getting to the Problem of the Root

Organizations 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 like privileges.

How can you most efficiently and effectively contain use of superuser privileges?

How can you manage use of shared privileged accounts in a controlled and auditable manner?

What are the best practices for handling embedded application-to-application passwords?

**Ant Allan, Gartner**

## Track 3 Sessions: Governance and Security: Risk Management Strategies

### The Impact of ITIL V3 on Security and Risk: 2008 Through 2018

ITIL Version 3 takes a life-cycle view of service management. It emphasizes the engineering of risk and security components into the 'service platform' of IT services. This has major practical implications on IT security strategies.

What is new about ITIL V3?

How will these changes impact security strategies (for the better and for the worse)?

What can you do to prepare for and leverage ITIL V3?

**Tom Scholtz, Gartner**

### Security Architectures of the Future

In perfect world, security controls, policies, processes and behaviors become fully integrated into the fabric of the enterprise. In the real world, many 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?

**Tom Scholtz, Gartner**

### Europe 2008: Evolving Security Strategies

End users survey shows how companies in Western Europe are implementing IT security, and what the expected changes in strategy are in 2008.

What is end users orientation towards adoption of security products?

Are there differences in strategy on security across Western Europe?

Is security improving and what is the perception of costs from incidents suffered?

**Ruggero Contu, Gartner**

### Regulatory Compliance in Europe: Time to Get Organized

Around the world, regulatory drivers are not the same. Corporate governance, privacy principles and data retention requirements vary. For these three areas, we will compare the status quo in the US and in Europe.

What makes the regulatory landscape in the US and in Europe so different?

Do we learn from US experience? Do they learn from us?

What do regulations mean for IT departments?

**Carsten Casper, Gartner**

### Emerging IT Governance, Risk and Compliance Technologies

IT GRCM is a set of capabilities that can improve an IT organization's external audit posture, reduce compliance reporting costs, and improve an organization's ability to effectively address IT risks.

How can IT GRCM technology reduce compliance costs and improve an organization's ability to assess risk?

Who are the major IT GRCM technology providers?

How can organizations effectively deploy IT GRCM technologies?

**Paul Proctor, Gartner**

### Information Governance Tools and Techniques to Manage Risk

Using the Gartner Enterprise Information Management Framework, this presentation examines the following key issues:

What are the components of an information governance strategy?

What are the organizational and process effects of information governance?

How is information governance related to IT security issues?

What are the emerging best practices around information governance?

**Debra Logan, Gartner**

### Policies: Proactive Plan for Protection or Purposeless Pile of Paper?

Are policies really the foundation of information security management and the mechanism to direct the selection and implementation of security measures or are they piles of virtual paper with an ever-increasing last access date?

What are the common problems with policy development and implementation?

How do I go about communicating policies and ensuring compliance?

What tools are there to help me with policy management and compliance?

**Les Stevens, Gartner**

### Transpass the Border, Not the Law: Privacy in International Corporations

Since rarely a day passes without another privacy breach notification, consumers are increasingly aware of their privacy rights. Data protection and IT implementations can no longer live in parallel worlds.

What variations in national privacy laws and practice are relevant to business and IT?

How to choose from a portfolio of cross-border transfer instruments?

Are privacy profiles the right way to develop a global privacy strategy?

**Carsten Casper, Gartner**

### Communities of Trust Case Studies

How do you allow access to your sensitive corporate information by persons who don't work for your company? Secure, multi-enterprise, collaborative environments just can't be created using traditional security mechanisms, but new trust services can enable enterprises to control their data even on non-corporate desktops.

How are today's organizations enabling trust across the extended enterprise?

What are the security and convenience tradeoffs?

**Jay Heiser, Gartner**

## Track 4 Sessions: Business Impact and Resilience

### Beyond Disaster Recovery: Enabling Workforce Continuity

After ten years of effort on technology recovery, the focus is now turning to ensuring that the workforce is ready, willing and able to leave family and home — often recovering from the same crisis — and help the enterprise. Key issues:

What workforce issues should enterprises be aware of when dealing with crises?

What are the trends in workforce recovery?

What are the best practices for workforce continuity?

**Roberta Witty, Gartner**

### Integrating Physical and Information Security

This presentation examines the prospects for merging physical security programs and IT security and risk programs, the organizational structure and changes associated with such an operational merger and the benefits and pitfalls.

What are the benefits of integrating physical and cyber security?

How should organizations structure their security functions across physical and IT security?

What are the major obstacles to integrating physical and IT security?

**Christian Byrnes, Gartner**

### Managing Business Continuity Plans for Business Resilience

Organizations have struggled to develop pragmatic business continuity plans due to lack of strategic direction, executive buy-in and funding, resulting in paper exercises with no value. This presentation provides practical guidance for developing, implementing and maintaining business continuity plans.

Key Issues:

What is the scope and structure of BCM and BCP?

What is the role of BIA and risk assessment?

How do I go about implementing and maintaining my plans?

**Les Stevens, Gartner**

### The Business Case for Emergency Preparedness and Business Resiliency

Business continuity management (BCM) is a process enterprises can use to reduce operating costs, drive revenue, maintain their brand and promote community reputation in the face of growing operational risks.

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?

**Roberta Witty, Gartner**

### Integrating Security & Privacy Requirements into IT Sourcing & Procurement

Third party access to production data or systems, outsourcing of HR and CRM applications, maintenance of different privacy and security policies, and inconsequential penalties in security SLAs are some of IT's security and privacy questions when addressing IT sourcing and procurement. Key issues:

What are the security and privacy and country risk issues associated with sourcing?

What steps do you need to take to address sourcing security concerns?

**Arabella Hallawell, Gartner**

### Creating an Effective Security and Risk Management Culture

Information doesn't stop at the network interface; it continues through the organization right into human brains. Today's CISO is expected to bring about a cultural change, bringing people security back into balance with computer security.

How do you know what level of risk control the business really needs?

Which activities encourage management support for IT risk management?

How do you discourage employees from circumventing security?

**Jay Heiser, Gartner**

## ANALYST/USER ROUNDTABLES

Analyst / User Roundtables are a chance for you to spend 45 minutes in the company of a Gartner analyst expert and 8 of your peers letting you raise your issues and receive group consideration, alternative solutions and commercially valuable feedback.

Why not come and have YOUR say on the subjects of most importance to you?

Use this opportunity to understand the experiences of your peers and to receive deeper perspectives on core Summit topics including:

### Security Awareness Communication and Training

Moderator: Jay Heiser

### Secure Software Development Best Practices

Moderator: Joseph Feiman

### Wireless and Mobile Security

Moderator: John Girard

### Best Practices for Security Organization

Moderator: Tom Scholtz

### E-Discovery and Information Governance Best Practices

Moderator: Debra Logan

### Compliance in Europe: Experiences and Lessons Learnt

Moderator: Carsten Casper

### Identity and Access Management Programs

Moderator: Ant Allan

## Day 3: Best Practices and Implementation Day

These sessions running across three tracks focus on operational best practices, strategies for implementation and practical methodologies. They are accompanied by supporting end-user case studies as well as workshops.

### Best Practices in Network Access Control

John Pescatore, **Gartner**

### Will Security and Portability Mix? New Criteria for Virtual Data Loss Prevention

John Girard and Jay Heiser, **Gartner**

### Policies: Proactive Plan for Protection or Purposeless Pile of Paper?

Les Stevens, **Gartner**

### Security in the Age of Web 2.0

Joseph Feiman, **Gartner**

### Do You Know Where Your Data Are? Data Security in the World of Geographically Distributed Processing and Storage

Andrew Walls, **Gartner**

### Trespass the Border, Not the Law: Privacy in International Corporations

Carsten Casper, **Gartner**

### End-User Case Study — 'Taming of the Shrew': Diageo's Work to Secure Tomorrow's Enterprise and Mitigate Today's

Dr Claudia Natanson, Chief Information Security Officer, **Diageo**

### End-User Case Study — (ISC)<sup>2</sup> Workshop: Managing Careers as Well as Risks

John Colley, Managing Director EMEA, **(ISC)**

### Workshop — SANS Institute: Frontline Solutions for Security Professionals

Jess Garcia, SANS Certified Instructor, **SANS Institute**

### End-User Case Study — Embedding Effective Privacy Compliance Program in Accenture

Bojana Bellamy, Global Data Privacy Compliance Lead, **Accenture**

### End-User Case Study — Who Am I and How Do I Prove It? Identity Management at HBOS

Jim Brady, Senior Information and IT Risk Analyst, **HBOS**

### Workshop — ISACA: COBIT and Val IT for the Security Professional

Roger Southgate (CISM, CISA, FCCA, MBA) Leader, London COBIT Development Group and President, IT Governance Standards, **ISACA**

### How to Securely Implement Virtualization

Neil Macdonald, **Gartner**

### Getting to the Problem of the Root

Ant Allan, **Gartner**

### Communities of Trust Case Studies

Jay Heiser, **Gartner**

### End-User Case Study — Secure Integration in a Heterogeneous Environment: Solutions at Handelsbanken

David Böling, IT Architect, **Handelsbanken**

### End-User Case Study — Building an IT Security Masterplan For Performance and Profit in the Republic and Canton of Jura

Bruno Kerouanton, Head of IT Security, **Republic and Canton of Jura**

### End-User Case Study — Information Security Audits as an Accepted Business Support Tool at Novartis

Manfred Schreck, Head of Group Information Security, **Novartis**

### Security Market Players: Magic Quadrant Power Session

Mark Nicolle, Peter Firstbrook, John Girard, Paul Proctor, **Gartner**

### Gartner Keynote II Color of Security in 2018: Dark, Bright, or Grey?

Joseph Feiman, Neil MacDonal, John Pescatore, **Gartner**



## TAILOR YOUR OWN AGENDA IN ADVANCE!

To enable you to build your own personal agenda and select the sessions that are relevant to you, please use our online Agenda Builder to ensure you make the right decisions and get the best value from the Summit. For details please visit

[www.europe.gartner.com/security](http://www.europe.gartner.com/security)

## Meet Innovative Technology and Service Providers at the Forefront of IT Security

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. Visit the demonstration forum, attend the Solution Provider Sessions and join in the networking drinks reception for informal relationship-building.

### Platinum Sponsors

#### CA



CA (NYSE: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure.

[www.ca.com/security](http://www.ca.com/security)

#### Finjan



Finjan is a global provider of web security solutions for the enterprise market. Our real-time, appliance-based web security solutions deliver the most effective shield against web-borne threats, freeing enterprises to harness the web for maximum commercial results. Finjan's real-time web security solutions utilize patented behavior-based technology to repel all types of threats arriving via the web.

[www.finjan.com](http://www.finjan.com)

#### Fortify Software



Fortify makes business software hacker-proof. Companies have built perimeter defenses with firewalls or anti-virus software, then perforated these walls to communicate with partners and customers leaving the software assets inside vulnerable to the ever increasing number of daily security breaches. With Fortify 360 companies make the software itself impenetrable.

[www.fortify.com](http://www.fortify.com)

#### McAfee



McAfee is the world's largest dedicated security technology company. It delivers proactive and proven solutions, services that secure systems and networks. With its security expertise and innovation, McAfee empowers customers, businesses and service providers by enabling them to comply with regulations, data protection, prevent disruptions, identify vulnerabilities and monitor and improve their security.

[www.mcafee.com](http://www.mcafee.com)

#### Net IQ



NetIQ is a leading provider of integrated systems, security and compliance management solutions. With powerful features such as real-time security monitoring and protection, mapping threat indicators, policy violation alerts and expedited incident forensics & resolution, NetIQ Security Management solutions deploy quickly and easily to reduce enterprise risk, decrease compliance costs and increase the security of critical information assets.

[www.netiq.com](http://www.netiq.com)

#### Nokia



Nokia security solutions help companies protect against viruses, abuse, hackers, and information theft so business keeps moving. Together, with partners like Check Point and Sourcefire, Nokia provides network and mobile security solutions so companies can provide an increasingly mobile workforce access to business information without compromise.

[www.nokiaforbusiness.com](http://www.nokiaforbusiness.com)



### Ounce Labs

Ounce Labs' solutions enable organizations to identify, prioritize and eliminate business risk to the enterprise caused by software security vulnerabilities. With Ounce Labs, organizations strengthen application security, protect confidential information and verify compliance with both internal policies and industry mandates such as PCI, FISMA, HIPAA and others.

[www.ouncelabs.com](http://www.ouncelabs.com)



### PGP

PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications allow organisations to meet current needs and expand as security requirements evolve.

[www.pgp.com](http://www.pgp.com)



### Secure Computing

Secure Computing® is a global leader in Enterprise Gateway Security Solutions. Powered by our TrustedSource™ technology, our best-of-breed portfolio of solutions provide Web Gateway, Messaging Gateway, and Network Gateway security, as well as Identity and Access Management. Secure Computing is proud to be the security solutions provider to many of the most mission-critical and sensitive environments in the world.

[www.securecomputing.com](http://www.securecomputing.com)



### Sophos

Sophos enables enterprises to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. We protect over 100 million users in nearly 150 countries.

[www.sophos.com](http://www.sophos.com)



### Utimaco Safeware - The Data Security Company

Utimaco is a leading global provider of data security solutions, enabling organizations to safeguard their data assets against intentional or unintentional loss, and to comply with privacy laws. Utimaco's complete range of data security solutions provide full 360 degree data protection for data at rest, in motion and in use.

[www.utimaco.com](http://www.utimaco.com)



### VeriSign

VeriSign provides Internet Infrastructure Services for the digital world. We protect businesses and consumers online with our SSL certificates, authentication solutions and fraud detection services and we run the .com and .net registries. Operating in 75 countries, we serve over 400,000 customers and support over 30 billion interactions every day.

[www.verisign.com](http://www.verisign.com)

### Verizon Business Security Solutions powered by Cybertrust



Verizon Business secures data and identities at the device, along networks, and around the world. Our professional services, managed services and technologies are delivered through full outsourcing, managed and hosted services and self-service models. In 2007 Verizon Business acquired Cybertrust, an information security leader for 15 years, incorporating the focused security expertise of Cybertrust into all its security solutions.

[www.verizonbusiness.com](http://www.verizonbusiness.com)

## Silver Sponsors



### ArcSight

ArcSight (NASDAQ:ARST) is global leader in compliance and security management, enabling enterprises and government agencies to comply with policy, safeguard assets, and control business risks.

[www.arcsight.com](http://www.arcsight.com)



### dns

dns is a leading provider of information security services. Offering services from setting strategy to 24/7 managed services dns work across the full security lifecycle.

[www.dns.co.uk](http://www.dns.co.uk)



### Qualys

Qualys, the leader in on-demand vulnerability management, allows security managers to effectively strengthen the security of their networks, conduct automated security audits and ensure compliance.

[www.qualys.com](http://www.qualys.com)



### Sourcefire

Sourcefire (Nasdaq: FIRE), SNORT® creator, is the leader in Enterprise Threat Management (ETM) – unifying IPS, NBA, NAC, and Vulnerability Assessment technologies under one management console.

[www.sourcefire.com](http://www.sourcefire.com)



### TippingPoint

TippingPoint, the leader in intrusion prevention systems (IPS), provides the IPS-Secured Network, which delivers attack control, access control and application control.

[www.tippingpoint.com](http://www.tippingpoint.com)

## Bronze Sponsor

### loglogic

[www.loglogic.com](http://www.loglogic.com)

## Media Partners



## Important Dates

- **Now – 1 August 2008:**  
Register now for your early bird saving!
- **June 2008:** Website is updated with the Event agenda. Browse the topics, analysts and read about the keynotes!
- **July 2008:** Select which sessions you are planning to attend and build a personalized agenda using our unique online agenda builder.
- **July – 2 September 2008:** Now is the time to book your 30-minute One-on-One (private consultation) with your preferred Gartner analyst!
- **1 September 2008:** Access Summit documentation / presentations online
- **29 September – 1 October 2008:**  
Summit time!



### SPONSORSHIP OPPORTUNITIES

If your organization is interested in sponsoring this event, please contact Darren McCormack or Nigel Murphy for further details.

**Tel: +44 (0)1784 26 7429**  
[darren.mccormack@gartner.com](mailto:darren.mccormack@gartner.com)

**Tel: +44 (0)1784 26 7055**  
[nigel.murphy@gartner.com](mailto:nigel.murphy@gartner.com)

Gartner UK Ltd. is a company registered in England & Wales with the registration number 2266016.

The registered office is Tamesis, The Glanty, Egham, Surrey, TW20 9AW, United Kingdom.

## Upcoming Events

Gartner is the leading provider of research and analysis on the global information technology industry. Our goal is to support organizations as they drive innovation and growth through the use of technology.

As in our research, our events help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of technology.

**For a full listing of our events please visit [www.europe.gartner.com/events](http://www.europe.gartner.com/events)**

### Data Center Summit

21 – 23 October, Amsterdam

### Symposium/ITxpo

3 – 7 November, Cannes

### Gartner Strategie & Technologie Konferenz

2 – 3 December, Frankfurt

### Enterprise Architecture Foundation Seminar

3 – 4 December, Amsterdam

## TAILOR YOUR OWN AGENDA IN ADVANCE!

To enable you to build your own personal agenda and select the sessions that are relevant to you, please use our online Agenda Builder to ensure you make the right decisions and get the best value from the Summit. For details please visit

[www.europe.gartner.com/security](http://www.europe.gartner.com/security)

## Update your Profile

Gartner Events realize your time is precious. That is why we only want to send you information that is relevant to your role. Update your profile with us and we will send you information that is best suited to you.

Visit [experiencegartner.com](http://experiencegartner.com)

Return address: Gartner, Global DM, PO Box 952, Crawley, RH11 7WG, United Kingdom



## Registration

### How to Register

**Online:**

europa.gartner.com/Security

**Tel:** +44 (0) 208 879 2430

**Email:** [emea.registration@gartner.com](mailto:emea.registration@gartner.com)

### Registration Rates

**Summit only:**

Standard Rate: €2,695 + 17.5% VAT

Early Bird Rate: €2,395 + 17.5% VAT

*(offer ends 1 August 2008)*

### Why register early?

- Save €300 on the standard conference rate-available on cash registrations only
- Save time – we'll send you your fast track entry badge so you can skip the queues onsite
- Priority One-on-One booking with the analyst of your choice

### Special Team Discounts – because Security Is Not a Solo Effort!

4 for the price of three!

Register as a team of 3 or more and:

- Receive one additional free pass
- Get preferential access, as a team, to your preferred analyst of choice
- Exclusive meeting rooms for intra-team meetings onsite, subject to availability

*Note: Available on the Standard Rate only.*

*One discount applies*

### Gartner Clients:

We also accept Gartner Conference tickets as full payment for days 1 and 2 of the Summit. An additional fee of €495 + 17.5% VAT for the third day will apply. If you are a client with queries about tickets, please contact your sales representative or email [emea.events@gartner.com](mailto:emea.events@gartner.com)