

To navigate enterprise security in the future,  
you need a roadmap today.

# Ensuring the Future of Information Security

Now through the next 10 years

## 14th Annual Gartner IT Security Summit

June 2-4, 2008  
Gaylord National Resort & Convention Center  
Washington, D.C.  
[gartner.com/us/itsecurity](http://gartner.com/us/itsecurity)

### Keynote Guests



**Arlan Andrews**  
Founder, SIGMA,  
The Science Fiction  
Think Tank



**Greg Bear**  
Hugo & Nebula-Winning  
Author, Government  
Agency Advisor



**P.J. O'Rourke**  
Political Satirist,  
Journalist & Writer



**Scott Petry**  
Google



**Robert Sawyer**  
Futurist &  
Science-Fiction Writer



**Bruce Sterling**  
Writer, Speaker  
& Futurist

### Conference Chairs



**John Pescatore**  
VP, Distinguished  
Analyst, Gartner



**Victor S. Wheatman**  
Managing VP, Gartner

**\$200 early bird discount!**

Register by April 4 at  
[gartner.com/us/itsecurity](http://gartner.com/us/itsecurity)  
or call 1 866 405 2511

# Ensuring the Future of Information Security

## Now through the next 10 years

Despite new threats and technology solutions, it's relatively easy to plan for the next year or two. Peering out five to ten years is far more challenging.

And yet now, more than ever, it's vital to develop a proactive IT security strategy, one you can begin to implement right away.

As new generations of technology-savvy users and a growing wave of gadget-prone communication devices are making their way into the workplace, they bring with

them new security threats as well as new technical and management paradigms (see Key Trends for examples we'll explore at the Summit). All of this has the potential to create considerable chaos in the marketplace. The Gartner IT Security Summit 2008 will help you create your own roadmap to overcome challenges and take advantage of emerging opportunities.

Our analysts and speakers will present a detailed vision of the future IT security

landscape and show you how to strategically and tactically implement a plan.

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 sessions with over 30 Gartner analysts, numerous industry leaders and more than 100 IT security technology solution providers.

### Who should attend

- CIOs, CSOs, CISOs and CTOs
- IT vice presidents and directors
- Network managers
- Risk managers
- Auditors
- Senior business executives
- Anyone involved in enterprise-wide security and critical infrastructure protection

Prepare today for the future – walk away with a personalized roadmap to address new threats on the horizon.

- New breakthrough research
- New cutting-edge recommendations
- New end-user case studies
- New best practices
- New future-driven products and solutions
- New beautiful venue

## IT Security Summit 2008 Highlights

### Find out how key trends will impact your IT security strategy

- Secure Software Development
- Converged Solutions
- IT Security Modernization
- Consumerization of IT
- Virtualization
- Social Networking
- Virtual Life
- Quantum Computing

### Get answers to your most pressing challenges

- How do I optimize 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?
- Are we vulnerable?
- Will we be publicly exposed?

### Don't miss these exclusive Gartner features

- CPE credits towards CISSP certification
- IT Security Innovation Awards Presentations
- Interactive Audience Polling
- Analyst one-on-one sessions and Analyst-user roundtables\*
- Eight pre-conference tutorials (complimentary)
- Two SANS Institute pre-conference workshops (separate registration and fee)
- Access to over 100 leading IT security solution providers
- Numerous peer-to-peer networking opportunities

\*for Gartner clients only



### The Gartner Difference

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

# Explore. Strategize. Envision. Implement.

## What are you doing for the next 10 years?

The Summit is organized along six relevant IT security topics.

**A Protecting IT Infrastructures**  
 The IT Infrastructure will continue to evolve and security solutions must keep pace. If the past is prologue, then future architectures, applications, platforms and networks will hide new vulnerabilities. But if the market learns from the past, the new world may see sufficient security integrated into the infrastructure.

**B Enabling Secure Business**  
 Security isn't only "keeping the bad guys out." It's also "letting the good guys in" and enabling new, trust-based applications. Identity & Access Management and other promising projects have been complicated and the risks of project failure are high. How will day-to-day business become more secure in the next decade?

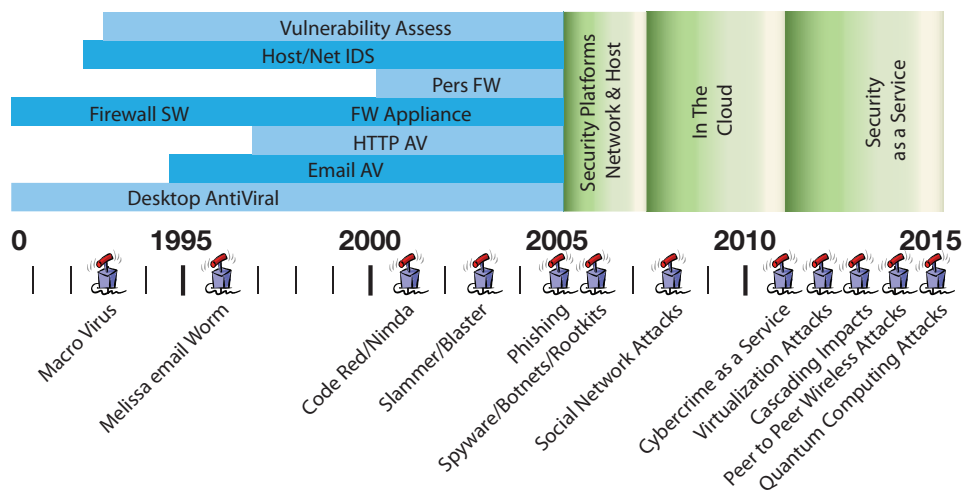
**C Security Governance**  
 Governance and management fads come and go and new approaches may be more effective than what we've done in the past. Will end users consciously govern themselves or will corporate edicts still be required? Corporations need to utilize what they already learned to bring corporate security governance into a sustainable future state.

**D Security Tools, Technologies and Techniques**  
 Point solutions address a specific problem but information security vulnerabilities tend to morph and become more complicated. Suites are not necessarily the answer, but converged and integrated products have presented their own challenges to end users. Knowing where things are going will become vital to protecting the enterprise.

**E Protecting Data and Applications**  
 The waves of identity theft and other cyber crimes 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.

**F Role of the CISO – Security Management Planning**  
 As information security departments are being re-chartered as IT Risk Management programs, the role of the CISO is also shifting. This track focuses on the skills and knowledge CISOs need to optimize their career growth over the next 10 years.

As security risks become more sophisticated and impactful on enterprises, so must the solutions. Plan for the worst and prepare for the best and most secure outcomes.



# Keynote Guests



**Arlan Andrews**  
Founder of SIGMA,  
The Science Think Tank

A Registered Professional Engineer and member of the Science Fiction and Fantasy Writers of America, Arlan has published over 400 fiction stories, fact articles, computer books and opinion pieces in 90 venues worldwide. While working at the White House Science Office in 1992, he observed a lack of imagination on the part of government technologists and forecasters and set up SIGMA to provide the practical futurism of science fiction for vital national needs.



**Greg Bear**  
Hugo and Nebula-Winning  
Author, Government Agency  
Advisor

Author of more than 30 books of science fiction and fantasy, Greg was awarded two Hugos and five Nebulas for his fiction, and is one of only two authors to win a Nebula in every category. He has advised Microsoft Corporation, the U.S. Army, the CIA, Sandia National Laboratories, Callison Architecture, Inc., Homeland Security and other groups and agencies.



**P.J. O'Rourke**  
Political Satirist,  
Journalist & Writer

With his books (*Parliament of Whores*, *Give War a Chance*, and *All the Trouble in the World*) becoming international best-sellers, P.J. O'Rourke has firmly established himself as the nation's premier political satirist.



**Scott Petry**  
Google

Scott joined Google in late 2007 as product management director. In this capacity Scott guides the integration of message security and compliance technology into Google enterprise applications.



**Robert Sawyer**  
Futurist, &  
Science Fiction Writer

Robert is author of award-winning science-fiction books, hundreds of feature articles and is a frequent on-air science commentator. He is also in demand as a keynote speaker all over the world. From state-of-the-art technologies like nanotechnology and carbon nanotubes to issues of privacy and prolonging life, Robert's specialty is extrapolating today's scientific, medical and ethical concerns into the near future.



**Bruce Sterling**  
Writer, Speaker, Futurist

Bruce is best known for his novels and short stories that helped define the cyberpunk genre. He coined the term "Wexelblat disaster," describing what happens when a natural disaster triggers a secondary, and more damaging, failure of human technology. Among his many books and collections is *The Zenith Angle*, about a cyber security expert who goes to work for the U.S. government fighting terrorism after the 9/11 attacks.

# Gartner Keynote Speakers

**"The Gartner Scenario: The Next Ten Years and Information Security"**



**Ken McGee**  
Vice President &  
Gartner Fellow

With 37 years as a professional in the IT industry, Ken specializes in emerging trends and technology for Gartner. He will provide an insightful overview of the economic and business issues affecting you and how they will impact your information security profile and security planning over the next decade. He'll also review the security questions most frequently asked of Gartner and examine longer-term trends that will affect the IT and information security industries.



**Neil McDonald**  
Vice President &  
Gartner Fellow

As an experienced analyst in information security, Neil is at the center of new threats and new technologies. He asks: Why can't our security infrastructure quickly adapt to changes in the threat environment from zero day and targeted attacks in ways similar to the human immune system? And why can't it quickly adapt to changes in business and regulatory policy? Neil believes it can, but significant change is required. His keynote presentation will explore this vision and what is necessary to see it realized.

# Gartner IT Security Analysts – Interact with the Best

Meet the Gartner analysts who will lead you into the future of IT security and help you map out a plan for the next 10 years. They are all at the top of their specialty fields, part of Gartner's large and formidable brain trust of talented, unbiased analysts. See analyst focus areas below:



**Ant Allan**  
Research  
VP

Information security topics, chiefly identity and access management and user authentication



**John Bace**  
Research  
VP

Compliance, risk and leadership



**Christian Byrnes**  
Managing  
VP

Technology direction, security trends and best practices



**French Caldwell**  
Research  
VP

Compliance, governance and risk practice



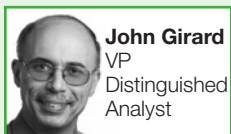
**Joseph Feiman**  
VP & Gartner  
Fellow

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



**Peter Firstbrook**  
Research  
Director

Client security best practices and technologies, including antivirus, spyware and spam



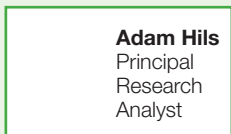
**John Girard**  
VP  
Distinguished  
Analyst

Business security and privacy solutions for wireless and mobile road warriors, extranet, remote offices and teleworkers



**Arabella Halliwell**  
Research  
VP

Security markets such as antivirus, e-mail security and Web filtering



**Adam Hills**  
Principal  
Research  
Analyst

Information security trends in the small and midsize business (SMB) marketplace



**Richard Hunter**  
GVP &  
Gartner Fellow

IT risk management and the business value of IT.



**Kelly Kavanagh**  
Principal  
Research  
Analyst

Professional and managed services for network and Internet security



**Gregg Kreizman**  
Research  
Director

Identity and access management, electronic signatures, public-key infrastructure and enterprise security architecture



**Nicole Latimer-Livingston**  
Research  
Director

Market share, trends and forecasts for security markets worldwide



**Avivah Litan, VP**  
Distinguished  
Analyst

Financial fraud, authentication, identity theft, fraud detection and prevention applications and other areas of information security and risk.



**Neil MacDonald**  
VP & Gartner  
Fellow

Operating system and application-level security strategies.



**Rex Murphy**  
Principal  
Research  
Analyst

Network security, physical security



**Mark Nicollet, VP**  
Distinguished  
Analyst

Vulnerability management, patch management, security information and event management and network access control



**Lawrence Orans**  
Research  
Director

Integration of security within internal networks, with a particular emphasis on network access control, VOIP and content filtering



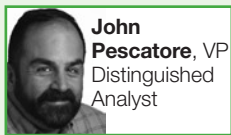
**Eric Ouellet**  
Research  
VP

Digital rights management, PKI, cryptography, secure e-mail, directories, identity and password management, biometrics, BCP/DRP and risk management



**Earl Perkins**  
Research  
VP

Security and identity, identity and privacy, Web services and DOA security, Software-as-a-service (SaaS) security



**John Pescatore, VP**  
Distinguished  
Analyst

Network security, Windows security, wireless LAN security, hardware security platforms and payment card industry security



**Paul Proctor**  
Research  
VP

Legal and regulatory compliance, event log management, security monitoring (host/network IDS/IPS), security process maturity risk management programs, forensics and data classification



**Tom Scholtz**  
Research  
VP

Security management strategies, technologies and trends, information security policy design, security organizational dynamics and security management processes



**Jeff Vining**  
Research  
VP

Homeland security and law enforcement



**Ray Wagner**  
Managing  
VP

Public key infrastructures and related applications, as well as the five-year security scenario



**Jeffrey Wheatman**  
Research  
Director

Security program management, security metrics, risk and vulnerability assessment, risk management and database security



**Vic Wheatman**  
Managing  
VP

Public key infrastructures and related applications, as well as the five-year security scenario



**Andrew Wills**  
Research  
Director

Information security practices and markets in the Asia/Pacific region



**Roberta Witt**  
Research  
VP

Business continuity management and disaster recovery



**Greg Young**  
Research  
VP

Network security

**Act now for \$200 discount! Register by April 4 at [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity) or call 1 866 405 2511**

# Agenda at a Glance

## Sunday, June 1

12:00pm	Pre Registration			
1:00pm	SANS Institute: Cutting Edge Hacking Techniques Workshop (Separate fee and registration apply)		SANS Institute: Web Application Security Workshop (Separate fee and registration apply)	
	Pre-Conference Tutorials			
4:00pm	<b>T1</b> Managing Mobility: the New Frontier of Security Challenges	<b>T2</b> Assess Yourself in X Easy Steps	<b>T3</b> Selecting Security Products Using Gartner's Magic Quadrants and Market Scopes	<b>T4</b> Non-US Security Firms: Opportunities for Innovation*
5:00pm	<b>T5</b> How to Securely Implement Virtualization	<b>T6</b> The Lessons Learned: Buying, Deploying and Managing IAM Systems	<b>T7</b> Data Loss Protection for Compliance-Driven Organizations	<b>T8</b> Security Solutions for Small and Medium Businesses (SMB)*

\*FOR HIGH TECH and TELCOM PROVIDERS ONLY

## Monday, June 2

7:00am	Registration					
7:00am	Continental Breakfast					
8:00am	<b>Welcome and Introductions: The Security Band Insecurity Blues</b> , Victor Wheatman, Managing VP, Gartner					
8:15am	<b>Opening General Session: The Gartner Scenario: The Next Ten Years and Information Security</b> Vice President and Gartner Fellow, Ken McGee					
9:30am	<b>Keynote Session - Mastermind Presentation: How Google Sees Information Security</b> - Scott Petry, Google					
10:45am	<b>Keynote Session - Science Fiction Writers Panel: Information Security and the Sci-Fi Future</b> - Moderator: Robert Sawyer, Futurist and Science Fiction Writer. Panelists: Arian Andrews, Founder, SIGMA, the Science Fiction Think Tank; Greg Bear, Hugo & Nebula-Winning Author, Government Agency Advisor; and Bruce Sterling, Writer, Speaker and Futurist					
11:45am	Attendee Lunch					
11:45am-1:45pm	Solution Showcase Dessert Reception and Analyst-in-a-Box Sessions (dessert on the showfloor ends at 1:45pm)					
	<b>Analyst-in-a-Box Sessions:</b> Concise twenty-minute sessions on key Gartner concepts plus question and answer sessions around important topics. Come meet Gartner's leading Information Security analysts in the conference show floor theater.					
	11:45-12:05 <b>Biometrics</b>	12:10-12:30 <b>Selecting Security Consultants</b>				
	<b>TRACK A</b> Protecting IT Infrastructures for the Next Ten Years	<b>TRACK B</b> Enabling Secure Business for the Next Ten Years	<b>TRACK C</b> Security Governance for the Next Ten Years	<b>TRACK D</b> Security Tools, Technologies and Techniques for the Next Ten Years	<b>TRACK E</b> Protecting Data and Applications for the Next Ten Years	<b>TRACK F</b> Role of the CISO – Security Management Planning
1:45pm	<b>A1</b> Network Security Scenario	<b>B3</b> PCI Data Security Standard; Nothing left to Comply with by 2018	<b>C1</b> Emerging IT Governance Risk and Compliance Technologies	<b>D1</b> The Future of Cryptography: Quantum and Beyond	<b>E1</b> Application Security in the Age of Web X.0	<b>F1</b> Risk Program Management – Your Role in the Next Decade
3:00pm	Solution Provider Sessions and Case Study Presentations					
4:15pm	Solution Provider Sessions and Case Study Presentations					
5:30pm	<b>A2</b> Future Wireless Security Exploits: Does Hollywood Know Something We Don't?	<b>B1</b> Federation and User Centric Identity – The Future Secure Identity Architecture for Your Businesses Partners and Consumers	<b>C3</b> Finding the Right CISO for Your Program in 2018	<b>D2</b> Windows is Collapsing: Architecting the Next-Generation Secure Client and Server OS	<b>E2</b> Case Study: Enterprise Security Architecture at Morgan State	<b>F2</b> Security Architectures of the Future
6:30pm	Solution Showcase Reception					

Agenda current as of February 22, 2008, and subject to change. For complete session descriptions visit [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity).

Register now at [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity) or call 1 866 405 2511.

**Tuesday, June 3**

7:00am	Networking Breakfast					
8:00am	<b>Keynote Session: Building a Real-Time, Adaptive Security Infrastructure</b> , Neil MacDonald, Vice President and Gartner Fellow					
9:15am	<b>A3</b> Security as a Service in 2018	<b>B2</b> Security in the Brave, Not-So-New World of Grid Computing	<b>C2</b> Case Study: Vanderbilt University – The Evolving Role of the CISCO	<b>D3</b> Case Study: Managing the Security of SOA/Web Services at Gartner	<b>E3</b> The Future of Database Security	<b>F3</b> Business Resiliency: A Pro-Active Approach for Managing Business Interruptions
10:30am	<b>A4</b> Network Access Control in the Next Ten Years	<b>B4</b> Who? The Persona in the Digital Mask	<b>C4</b> New Age E-Discovery for Security Practitioners	<b>D4</b> Securing the End Point in 2018	<b>E4</b> Security of Legacies, Big Applications, and Databases	<b>F4</b> Privacy Matters for the New CISO
11:30am	Attendee Lunch					
11:30am-1:30pm	Solution Showcase Dessert Reception and Analyst in the Box Sessions (dessert on the showfloor ends at 1:30pm)					
	<b>Analyst in the Box Sessions:</b> Concise twenty-minute sessions on key Gartner concepts plus question and answer sessions around important topics. Come meet Gartner's leading Information Security analysts in the conference show floor theater.					
	11:30-11:50 PCI Toolkit	11:55-12:15 InfoSec Market Shares and Forecast				
2:45pm	<b>A5</b> Managing Security Information and Emerging Vulnerabilities	<b>B5</b> Real Security for Virtual Spaces	<b>C5</b> IT Risk: Turning Business Threats into Competitive Advantage	<b>D5</b> The Paranoid's Guide to Internet Survival	<b>E5</b> Video Surveillance: Big Brother and Convergence	<b>F5</b> The Impact of ITIL V3 on Security and Risk: 2008-2018
4:00pm	Solution Provider Sessions and Case Study Presentations					
5:15pm	<b>A6</b> Stump the Analyst	<b>B6</b> Identity at Your Service(s): The Rise of Service-Based Identity and Access Management	<b>C6</b> Case Study: Security Information Management at Gaylord Entertainment	<b>D6</b> In 2018 You May Not Have a Phone, But You Will Still Need Secure VOIP.	<b>E6</b> Radically Transforming Security in a Virtualized World.	<b>F6</b> Compliance – Get IT Right or Go to Jail
6:15pm	Hospitality Suite Events					

**Wednesday, June 4**

8:00am	Breakfast with the analysts					
9:00am	<b>Keynote Session: PJ O'Rourke</b> , Political Satirist, Journalist & Writer					
10:30am	<b>A7</b> Network Access Control Case Studies	<b>B7</b> Electronic Signature Suites and Services - Preserving the Electronic Trail 10 Years from Now	<b>C7</b> The Case for Integrating Physical and Information Security	<b>D7</b> Activity Monitoring Across the Cloud	<b>E7</b> Gartner's Threat Forecast Timeline	<b>F7</b> Security Organization Models in the Next Ten Years
11:30am	Attendee luncheon					
12:30pm	Solution Provider Sessions and Case Study Presentations					
1:00pm	<b>A8</b> Is the Future of Security Open Source?	<b>B8</b> Good Morning, Dave! 2018: An Authentication Odyssey	<b>C8</b> CISCO Heaven: Take Me to the Promised Land	<b>D8</b> Reinventing Security-as-an-Application Service	<b>E8</b> The Next Ten Years in Secure Messaging	<b>F8</b> Tailored Security on a Budget: 'Off the Rack' Security Is So-oo 2008
3:00pm	<b>Gartner IT Security Innovation Awards Presentations</b>					
4:00pm	<b>General Session: Color of Security in 2018: Dark, Bright, or Gray?</b> An Interactive Session					

Enter the 4th Annual Gartner IT Security Innovation Awards Competition.

**Deadline is April 25.**

Each year Gartner recognizes world-class security initiatives and promotes the sharing of best practices. Do you believe your security implementation is an advance beyond common practices? Has it increased security or cut security costs? We want to hear your story!

**Past Recipients have included:**

Lehman Brothers, Penn State University and the City of Virginia Beach  
Winners receive two free passes to Gartner IT Security Summit 2008, a Gartner IT Security Innovation Award trophy and a \$500 American Express gift certificate.

For details, go to [gartner.com/us/itsecurityinnovation](http://gartner.com/us/itsecurityinnovation)

# Session Descriptions >>> Explore, plan and implement

## Pre-Conference Workshops

### SANS Institute – Cutting-Edge Hacking Techniques Workshop (separate registration and \$495 fee apply).

This session will provide you with up-to-date knowledge on the latest hacks developed over the last twelve to eighteen months. In addition to detailed descriptions of how the attacks function, you'll get hands-on experience with the tools and their defenses. Laptop required.

### SANS Institute – Web Application Security Workshop (separate registration and \$495 fee apply)

This workshop covers the critical security issues in Web applications, including common vulnerabilities, how attackers leverage those vulnerabilities and some of the vital principles of defending against potential attacks. The course helps you ensure that your company and its assets are more secure as you conduct business on the Web. Laptop required.

## Pre-Conference Tutorials

### (T1) Managing Mobility: The New Frontier of Security Challenges

As mobility permeates society, enterprises must remain vigilant in keeping corporate policies, expenses and security practices updated. This session looks at every aspect of keeping enterprise information secure and costs and risks in line with benefits – all with an eye towards future investment.

- How will pervasive mobility increase IT management and security challenges?

- Which management and technology practices must be updated to avoid disasters and downtime?
- What key implementation decisions will provide the greatest benefits with the least cost and complexity?

**John Girard**

### (T2) Assess Yourself in X Easy Steps

The more mature an organization's risk-based processes are, the more proactive their approach to risk management and resilient they can be in the face of incidences. Learn how to assess the overall process maturity of your risk program using Gartner's risk maturity program assessment tool.

- What key processes make up a risk management program?
- How can you assess your current level of process maturity?
- How can you correlate process maturity with overall risk program maturity?

**Jeffrey Wheatman**

### (T3) Selecting Security Products Using Gartner's Magic Quadrants and Market Scopes

Get help choosing the best security products for your circumstances. Our analysts spend a great deal of time independently analyzing products, services and the companies that provide them. This session explains the process and describes how Gartner research products can be optimally used in making buying decisions.

- What research methodology does Gartner use?
- How do product and service attributes impact ratings in Gartner's published research?
- How can you most effectively use Gartner's research in your decision-making?

**John Pescatore**

### (T4) Non-U.S. Security Firms: Opportunities for Innovation

The market for security products and services in Europe and Asia is exploding and local vendors are scrambling to satisfy customer demand. Some of the security companies based abroad are more innovative and less expensive than the market leaders here, while providing similar—often better—customer service.

- How must vendors tackle cultural, political, legal and linguistic barriers to compete against agile, local vendors?
- What will be the impact of governments and corporations that increasingly want vendors to make substantial investments in local facilities and staff?

**Andrew Walls**

### (T5) How to Securely Implement Virtualization

This tutorial discusses the specific security issues related to virtualization and provides detailed guidance for secure virtual server deployments.

- Should the security of virtual servers be treated the same as physical servers?
- How are major vendors approaching security with their architectures?
- What are specific implementation recommendations for a more secure deployment of virtualization?

**Neil MacDonald**

### (T6) Lessons Learned: Buying, Deploying and Managing IAM Systems

What does the ideal RFP or tender contain for identity and access management systems? What questions should you ask before buying a system? Are there best practices for deploying user provisioning? Once a system is installed, what organizational structure is best suited for

optimal use? Explore these and other questions in a survey of attendees' experiences.

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

**Earl Perkins**

### (T7) Data Loss Protection for Compliance-Driven Organizations

Content Monitoring and Filtering/Data Loss Protection technologies are increasingly commonplace in the arsenal of compliance tools for many organizations. 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?
- What 5 points must organizations consider when deploying CMF/DLP solutions?

**Eric Ouellet**

### (T8) Security Solutions for Small and Medium Businesses (SMB)\*

Beginning with market sizing, market share and forecasting, the presentation then explores SMB security requirements. Vendors and buyers are learning painful and expensive lessons when they try to scale down an enterprise product or supersize an SMB product. SMBs have very different options, budgets, buying patterns, expertise and technical requirements for security that services their IT landscapes.

- How are SMBs different?
- What are SMB's greatest security needs?
- How can security vendors effectively market in the SMB space?

**Adam Hils and Nicole Latimer-Livingston**

## General and Keynote Sessions

### The Gartner Scenario: The Next Ten Years and Information Security

To kick off the conference, Gartner Vice President and Fellow Ken McGee provides an overview of the economic and business issues affecting Gartner clients and how they will impact their information security profile and security planning over the next decade. Further, he'll review the security questions most frequently asked of Gartner, and project which questions will become important over the next several years. Finally, Gartner's predictions for the origin of future growth in the IT and Information Security industry will be presented.

**Ken McGee**

### Mastermind Presentation: How Google Sees Information Security

Scott Petry describes lessons learned, best practices and pitfalls to avoid in the role that he plays. He walks through some common security scenarios to gain insight into recent security events, compliancy regimes and technology changes, and describes how Google will address security and current and upcoming offerings.

**Scott Petry, Google**

### Science Fiction Writers' Panel: Information Security and the Sci-Fi Future

Hear from members of the SIGMA panel advising the Department of Homeland Security on anti-terrorist and anti-cybercrime scenarios. Our esteemed panel will participate in a lively discussion of these timely issues:

- What can information security learn from science fiction?
- What issues in privacy, reliability, data integrity and network security have been explored by sci-fi authors?
- What is the relevancy to today's infosec practitioner?

### 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 from zero day and targeted 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 explores this vision and what is necessary to see it realized.

**Neil MacDonald**

### P.J. O'Rourke – Political Satirist, Journalist & Writer. Session TBA.

### IT Security Innovation Awards Presentations

Winners present their case studies demonstrating originality and advancements in security programs, the application of technology or the use of leadership resulting in an improved security profile. Interested in applying? Visit [gartner.com/us/itsecurityinnovation](http://gartner.com/us/itsecurityinnovation)

### Color of Security in 2018: Dark, Bright, or Gray?

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 to innovate, and software services and packages will be coming out of assembly with imbedded security protection features. Ultimately, will security threats be contained at the acceptable levels, or will fear rule the Web? Gartner analysts and audience members debate whether we will be more secure in 10 years.

**Joseph Feinman, John Pescatore, Neil MacDonald**

## Track A Protecting IT Infrastructures

### (A1) 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. Beyond appliance litter and a parade of emerging vendors, here are steps that can better secure the network today and make better leverage of new network security capabilities without breaking the budget.

- How is the security infrastructure market evolving?
- What are the most effective technologies and best practices?

**Greg Young**

### (A2) Future Wireless Security Exploits: Does Hollywood Know Something We Don't?

Wireless and mobile technology continues to conjure up fears about how it will be used to exploit people and disrupt business. This session introduces Gartner's methods to identify and give reality checks to future threats.

- What is real versus hype about wireless security exploits?
- How will wireless security exploits change in the future and how will security technologies change to meet new threats?
- What best practices will help you defend against current and future wireless security exploits?

**John Girard**

### (A3) Security as a Service in 2018

Implementing security controls via vendor-owned and managed technology offers potential benefits with attendant risks. This session offers Gartner's view on the present and future role security plays as a service and the vendors that will deliver it.

- What security controls and technologies present the best opportunities for low-cost, fast, deployment security as a service delivery?

- What safeguards must be in place to implement security as an effective service?
- What vendor/service providers offer true security as a service?

**Kelly Kavanagh**

### (A4) Network Access Control in the Next 10 Years

Interest in NAC remains high, but adoption has been slow. In this session, 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 first start deploying NAC in your network?

**Lawrence Orans**

### (A5) Managing Security Information and Emerging Vulnerabilities

Organizations 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 are evaluated in this session.

**Mark Nicollet**

### (A6) Stump the Analyst

Bring it on! No agenda, no slides, no net. Just a brave Senior Analyst (or two) fielding your toughest questions on anything at all pertaining to information security. Can you stump the analyst? Give it your best shot. It should be a lively session to say the least.

**John Pescatore**

---

## (A7) Network Access Control Case Studies

---

An informal poll taken at last year's Security Summit reflected that more organizations are still in the planning stages of NAC. They will share their success stories and you will have the opportunity to ask questions.

- How have their organizations benefited from NAC?
- What key factors led to the success of the project?
- What can you learn from their mistakes and growing pains?

**Lawrence Orans**

---

## (A8) Is the Future of Security Open Source?

---

This session delves into the current state of open source security, revealing why many enterprises and agencies are now using it while still paying for security products. The presentation scrutinizes open source security, asking:

- Are there enough open source security products that can make an enterprise secure?
- What open security products are actually available?
- How badly could you get hacked on Day One if you use open source security?

**Greg Young**

---

## Track B Enabling Secure Business

---

### (B1) Federation and User Centric Identity— The Future Secure Identity

---

Architecture for Your Business Partners and Consumers Federation technology and practices have matured and implementations are increasingly common. However, today's federations are confined to well-defined communities of interest, and federations don't completely address ease-of-use and privacy protection. The future identity architecture must include the best of today's federations and the evolving user-centric identity frameworks.

- How have federated identity requirements and market offerings evolved?
- How are emerging user-centric identity frameworks progressing?

- How will today's federation capabilities merge with personal identity frameworks?

**Greg Kreizman and Ray Wagner**

---

### (B2) Security in the Brave, World of Grid Computing

---

Although grid computing has been a resource in research and higher education for years, it only recently emerged as a resource for corporations. The shared nature of grid computing promises strong benefits in terms of computational power, but is accompanied with risks to data confidentiality, integrity and availability.

- How must data and algorithms be structured to protect corporate assets?
- What are the issues when geographic distribution of grid computing resources occur?
- How can you assure data integrity and are sophisticated cryptographic tools the answer?

**Andrew Wells**

---

### (B3) PCI Data Security Standard: Nothing Left to Comply with by 2018

---

Breaches of credit/debit card data have led to substantial fraud and companies have spent millions cleaning up the wreckage. Pressure to comply with the Payment Card Industry Data Security Standard has increased, but compliance still remains low. This presentation highlights Gartner's best practice recommendations to protect customer data and demonstrate PCI compliance.

- What did we learn from the TJX data breach and how are other merchants responding?
- What are best practices for complying with PCI?
- What are the long-term solutions and why will the PCI DSS become obsolete by 2018?

**Avivah Litan**

---

### (B4) Who? The Persona in the Digital Mask

---

By 2018, digital identities will constitute the bulk of a person's complete identity, so much so that a person's civil identity, attributed by the State, will likely be founded in cyberspace. Organizations managing

workers' and customers' digital identities will increasingly rely on trusted (original) identity providers.

- Just what is "identity" anyway?
- How can organizations manage users' digital identities and access rights?
- Will the State be the most significant provider of civil identity information?

**Ant Allan**

---

### (B5) Real Security for Virtual Spaces

---

Virtual worlds, social network applications and real world mapping environments merge to form complex, geographically distributed social and business interaction environments. As corporations move into these dynamic environments to access new markets and enhance customer interaction and staff collaboration, new security risks are created. The assurance of security within these new and rapidly changing environments requires a well-coordinated, fluid approach to risk management.

- 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?
- How will vendor support for security in virtual worlds be influenced?

**Andrew Wells**

---

### (B6) Identity at Your Service: The Rise of Service-Based Identity and Access Management

---

Will there ever be a day when customers can "buy" identity and access management services, rather than installing products within their enterprise? And is that day already here? Are the identity and access management products themselves built as service-oriented, architecture-based (SDA) solutions to make such implementations easier? Let's take a good look from your perspective.

- How viable is service-based identity and access management?
- What form will it take?
- What are the key questions customers must ask?
- What is the current state of service-based identity and access management architecture?

**Earl Perkins**

---

### (B7) Electronic Signature Suites and Services: Preserving the Electronic Trail 10 Years from Now

---

Despite technology-neutral e-signature laws in North America and a history of point solution adoption, there is increased interest in deploying e-signature software suites and hosted services to ensure that the important signature process steps are properly managed and that signed records can stand up in court for years to come.

- How do software suites and hosted services address the important signature process control points?
- Which e-signature technologies are winning market share?
- Who are the e-signature software suite and e-signature service providers?

**Greg Kreizman**

---

### (B8) "Good Morning, Dave!" 2018: An Authentication Odyssey

---

Authentication in 2018 will be far simpler for enterprises with standardized methods and federation services and for users, with simple, passive authentication. But for several years organizations will have to choose from an increasing variety of authentication methods and users will continue to be faced with varying degrees of inconvenience.

- What authentication methods are available today?
- How can enterprises select and implement methods that best fit their use cases?
- What technological and social changes will be necessary to get there from here?

**Ant Allan**

---

## Track C Security Governance

### (C1) Emerging IT Governance Risk and Compliance Technologies

IT GRCM capabilities can improve an IT organization's external audit posture, reduce compliance reporting costs and improve the 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 the ability to assess risk?
- Who are the major IT GRCM technology providers?
- How can organizations effectively deploy IT GRC technologies?

**Paul Proctor and Mark Nicolette**

### (C2) Case Study: Vanderbilt University – The Evolving Role of the CISO

Gartner predicted that the role of the chief information security officer would transition from operations to strategy and governance. Participate in a discussion with the Chief Information Security Officer, Vanderbilt University and Medical Center who has experienced this transition first hand.

**Mark Johnson, CISO,** Vanderbilt University and Medical Center

### (C3) Finding the Right CISO for Your Program in 2018

Looking ahead, it's 2018. We've seen sweeping changes in the security and risk landscape over the last 10 years. Focus has moved from buying tools and being reactive, to developing processes and being proactive. The key to this successful turn of events has been putting the right leader in place.

- What are the hallmarks of a good CISO?
- How do we find the best candidate?
- How do we make sure the individual is right for the job?

**Jeffrey Wheatman**

### C4 New Age E-Discovery for Security Practitioners

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 organizations. This means that personal e-mail accounts as well as social networking sites and virtual reality may become targets.

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

**John Bace**

### (C5) IT Risk: Turning Business Threats into Competitive Advantage

IT risk has left the data center and is now a business risk, which, if not properly managed, has serious business consequences. Based on the Harvard Business School/ Gartner Press book *IT Risk: Turning Business Threats into Competitive Advantage*, this presentation discusses the business consequences of IT risk as related to availability, access, accuracy and agility.

- How will IT risk drive business decision-making?
- What approaches to IT risk management will be most effective?
- How should senior executives encourage effective management of IT risk?

**Richard Hunter**

### (C6) Case Study: Security Information Management at Gaylord Entertainment

With an implementation timeline influenced by PCI Compliance obligations, Gaylord deployed a Security Information Management solution as the authoritative source of security log information. Security logs from all major devices are aggregated and correlated spanning three server platforms, all network devices, security tools and scanners, etc. The company collects more than 200 million events per day, at

an average storage size of 100 MB/day.

- What were the challenges and what lessons were learned?
- What timeline was required and space needed for the logs?

**Mark Burnette,** Executive Director of IT Operations & Strategy, Gaylord Entertainment Company

### (C7) The Case for Integrating Physical and Information Security

This presentation examines the merger between physical and IT security systems, with a focus on implementing a holistic security posture. It also examines the organizational structure and changes associated with this type of operational merger, as well as the benefits, pitfalls and best practices.

- What are the potential benefits?
- How should security functions be structured across physical and IT security? What are the major obstacles?

**Rex Murphy**

### (C8) CISO Heaven: Take Me to the Promised Land

They have to exist. Enterprises that 'get' security. Places where the CISO is actually part of the C-Team. Places where people, even the CEO, listen. Places where the lack of a security approval means the project doesn't get done. Places where the security organization is funded correctly. Places where putting out fires or just slowing them down isn't the entire job description. Places where, maybe, the future lies. We'll speak with several CISOs who actually work there, or who aspire to get there: CISO Heaven.

- What does CISO Heaven look like?
- How does one get to CISO Heaven?
- What are CISO Heaven organizations doing in 2008, both tactically and strategically?

**Ray Wagner,** Moderator with Panelists TBA

## Track D Security Tools, Technologies and Techniques

### (D1) The Future of Cryptography: Quantum and Beyond

This presentation briefly traces the controversial history of encryption through public key cryptography and PKI and ultimately projects future challenges.

- What cryptographic algorithms are safest to use?
- What is the current status of quantum computing?
- How can enterprises anticipate developments in quantum cryptanalysis?

**Eric Ouellet**

### (D2) Windows is Collapsing: Architecting the Next Generation Secure Client and Server OS

Has Microsoft's Windows OS become too monolithic and bloated? We believe that Microsoft developers will break with application compatibility and radically change their approach to security.

- How will future operating systems and applications improve or inhibit good security?
- What will the next generation secure client OS look like?
- How might other vendors deliver secure client OS or system-level features?

**Neil MacDonald**

### (D3) Case Study: Managing the Security of SOA/Web Services at Gartner

Much like other enterprises, Gartner will rely on SOA designs to meet its information processing need. Unlike past architectural changes, we are attempting to identify security issues before development and deployment. Here we review Gartner's web services security objectives and programs and analyze strengths, weaknesses and the rationales for

- How will SOA affect security planning and processes?
- When will web services security be ready for standardized processes and technology?
- How can the Security team effectively partner with application developers?

**Mike Zboray**

---

#### (D4) Securing the End Point in 2018

---

Computer criminals are becoming more cunning, innovative and productive. Malware proliferation and diversity are at an all-time high and the incidence of targeted attacks and zero day threats are increasing. Attackers is advancing state-of-the-art malware faster than traditional AV vendors are improving defenses and considerably faster than enterprises are adopting new HIPS and firewall technologies.

- What are the trends in malware development?
- What new security technologies and best practices show promise for corporate networks?
- What will future end-point protection platforms look like?

**Peter Firstbrook**

---

#### (D5) The Paranoid's Guide to Internet Survival

---

Cyber-attacks continue to escalate. Under-the-radar and undetected attacks are launched directly against consumers and enterprises, compromising valuable customer and corporate data. Targeted attacks are also on the rise and traditional anti-virus and anti-spyware filters are unable to stop them. In an increasingly uncertain environment, it's critical to know who you're interacting with at all times.

- What are the trends?
- How have consumer attitudes and security practices changed?
- What technologies are available to enterprises?
- What are the best practices for enterprises to secure data and accounts?

**Avivah Litan**

---

#### (D6) In 2018 You May Not Have a Phone, But You Will Still Need Secure VOIP

---

Voice is the most mission-critical, widely deployed and, historically, most reliable of all applications. That won't change in 2018, even though your phone may be just a piece of software. This session analyzes VOIP and unified communications trends and provides strategies for securing them.

- What are the unique challenges?

- What are the best practices?
- Which vendors are leading the way with innovative VOIP security solutions?

**Lawrence Orans**

---

#### (D7) Activity Monitoring Across the Cloud

---

As IT service and cloud-based delivery methods are adopted, the ability to monitor user activity and resource access becomes critical and more complex. A combination of monitoring and analytical technologies and services will be needed on the network and across systems and applications.

- How will monitoring requirements evolve over the next 10 years?
- What are the capabilities and limitations of these evolving technologies?
- How can monitoring technologies and services be used to analyze user activity data across the cloud?

**Mark Nicolett and Paul Proctor**

---

#### (D8) Reinventing Security-As-An-Application Service

---

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. The 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?

**Neil MacDonald**

---

### Track E Protecting Data & Applications

---

#### (E1) Application Security in the Age of Web X.0

---

Web X.0 will be an enormous challenge to enterprise security. Individuals will become developers and get free to access attack machines, theft enablers and enterprise-strength technologies, as well as to access advice, training, mentoring and tech support from global communities.

This presentation analyzes Web X.0 security threats and vulnerabilities, ways to protect enterprise and individual applications and changes that enterprises should make.

- What makes Web X.0 applications insecure?
- What processes and technologies will secure Web X.0?
- How will IT organizations change to meet the new security challenges?

**Joseph Feiman**

---

#### (E2) Case Study: Enterprise Security Architecture at Morgan State University

---

With a mix of constituencies and varied requirements, the university is an interesting environment for managing technology. Dr. Akpose discusses the challenges of securing the modern enterprise, examining lessons learned from enterprise architectural frameworks and developmental methodologies.

**Dr. Wole Akpose,**  
Morgan State University

---

#### (E3) The Future of Database Security

---

Databases are where much of the value and risk in future enterprises will reside. Historically, we haven't done a good job in protecting the data that sits in these critical repositories. If we are going to continue to improve our security posture and limit our risks, we need to follow the steps outlined in this presentation.

- Why are databases so important from a risk perspective?
- What are some of the limited steps we've taken to protect these core assets?
- What more can we do to make them more secure?

**Jeffrey Wheatman**

---

---

#### (E4) Security of Legacies, Big Applications and Databases

---

Application legacies, packaged systems and production databases (such as Oracle, SAP, and IBM) are an enterprise's most valuable assets. They should be protected against both external and internal attacks. The critical nature of protecting those assets cannot be overestimated.

- What are the security risks that major enterprise assets face?
- What processes can protect them?
- What new technologies and vendors will enable better security of these assets? databases?

**Joseph Feiman**

---

#### (E5) Video Surveillance: Big Brother and Convergence

---

Video surveillance is emerging as an important technology application for securing organizations. The earlier reactive mode of deploying systems is changing to a more proactive role with the convergence of access controls and facial recognition onto IP-based networks. This presentation examines the technological advancements and privacy challenges revolutionizing the way video surveillance will be used over the next 10 years.

- Where will the evolution take us?
- What will be the impact on existing network infrastructures?
- How should enterprises deal with privacy issues?

**Jeff Vining and John Pescatore**

---

#### (E6) Radically Transforming Security in a Virtualized World

---

Virtualization offers an opportunity to radically transform our standard approaches to information security. On desktops and servers, the virtualization layer can be used to perform introspection on hosted workloads, essentially delivering host-based IPS without agents. 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 and which are not?

**Neil MacDonald**

### (E7) Gartner's Threat Forecast Timeline

Financially motivated, targeted attacks have increased the impact of cyber incidents. In this session Gartner forecasts what types of threats will emerge and provides standard methodology for ranking them. We also outline some of the information security investments that will need to deal with emerging threats.

- What will be the key security threats over the next 10 years?
- How will intrusion prevention and incident response practices have to change?
- What role will governments and Internet infrastructure providers play?

**John Pescatore**

### (E8) The Next 10 Years in Secure Messaging

New forms of spam are emerging. Requirements for monitoring outbound e-mail 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 policies and procedures are relevant to monitoring employee e-mail?
- What are the most effective methods of implementing proper levels of messaging hygiene?

**Arabella Hallawell**

## Track F Role of the CISO – Security Management Planning

### (F1) Risk Program Management: Your Role in the Next Decade

An IT Risk Management program is related to enterprise or operational risk management, as well as to other IT-related risk functions. This presentation introduces the themes that are built on in the remainder of this Boot Camp track.

- What stays the same in the move from InfoSec to Risk Management?
- What classes of risk are managed under IT Risk Management?
- How does the ITRM function relate to operational risk functions?

**Chris Byrnes**

### (F2) Security Architecture of the Future

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 organizational practicalities mitigate against this.

- What is a conceptual vision of the security architecture of 2012?
- What are the characteristics of future security architectures?
- What are contemporary security architecture best practices?

**Tom Scholtz**

### (F3) Business Resiliency: A Proactive Approach for Managing Business Interruptions

Business interruptions that impact day-to-day operations can have serious, long-lasting consequences. Organizations must counter and respond to them in a proactive manner, ensuring that organizational resiliency is cost-effective and sustained. This presentation discusses 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?

**Roberta Witty**

### (F4) Privacy Matters for the New CISO

Companies are struggling to manage a myriad of privacy regulations and concerns related to their customers and employees, here and worldwide. This session details emerging privacy issues, governance models and best practices.

- How are privacy requirements evolving?
- How should companies set up an effective privacy function?
- Which vendors, technologies and standards should be considered?

**Arabella Hallawell**

### (F5) The Impact of ITIL V3 on Security and Risk 2008 - 2018

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

- What's new about ITIL V3?
- How will these changes impact SRC strategies?
- What can you do to prepare for and leverage ITIL V3?

**Tom Scholtz**

### (F6) Compliance – Get It Right or Go to Jail

Enterprises worldwide recognize the critical importance of many types of compliance, notably regulatory, organizational and commercial. Many individuals and organizations across the enterprise have a crucial stake in the compliance function, including legal, auditors, line-of-business managers, IT security and, most critically, senior executives and the board of directors. Everyone must have a clear understanding of the rapidly changing roles and responsibilities of compliance professionals.

- What are the best practices for implementing a compliance program?
- How will enterprise stakeholders and compliance converge over the next decade?
- What technologies will emerge?

**French Caldwell**

### (F7) Security Organization Models in the Next 10 Years

At the core of all successful risk and security programs is a business-focused, risk-driven security organization. The "ideal" structure for this organization varies by industry and overall enterprise approach to risk management. This presentation addresses three important considerations.

- Where should risk management report in your organization in 2018?
- What should your security organization focus on – people, process or tools?
- How and why should you integrate security into your enterprise risk framework?

**Jeffrey Wheatman**

### (F8) Tailored Security on a Budget ("Off the Rack" Security is Sooo 2008)

Today's security-conscious enterprise is compelled to buy many different, often overlapping, security functions. How do you navigate the muddle of vendor marketing and industry FUD to choose the best value while maintaining adequate security? In 10 years, enterprises will have to build a dynamic, services-based security architecture comprising "push" and "pull" services, paid from a master security debit account.

- Why do enterprises overreact to attacks?
- How are security budgets impacted by panic-driven capital projects?
- What new delivery modes for information security will raise the security baseline?

**Adam Hils**

# Sponsors\*

---

## Get the facts for informed decision making

Gartner sponsors are among the world's leading solution providers. Our Solution Showcase focuses on personal problem solving with breakthrough innovations. Top-level vendor representatives can provide valuable input to help you strategize, customize and ultimately make decisions to transform your IT security program for the next 10 years. As an attendee, you do more than visit sponsor booths. At the Gartner IT Security Summit you can:

- Hear detailed case studies involving their products and services
- View demonstrations
- Meet one-on-one to discuss your needs
- Network with peers considering similar purchases

## PREMIER

---



Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information and interactions by delivering software and services that address risks to security, availability, compliance and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at

[symantec.com](http://symantec.com).



VeriSign, Inc. (NASDAQ: VRSN), operates digital infrastructure services that enable and protect billions of interactions every day across the world's voice, video and data networks. Additional news and information about the company is available at

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



Trend Micro, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe.

[trendmicro.com](http://trendmicro.com)



WebSense, Inc. delivers intelligent content protection to more than 42 million employees worldwide. Our Web filtering, Web security, e-mail filtering and information leak prevention technologies allow businesses to share information safely within organizations, between organizations and over the Internet. For more information visit

[websense.com](http://websense.com).

## PLATINUM

---



Through strategic development, global expansion and strategic acquisitions, BT has evolved to be a leader in networked IT services, bringing together infrastructure, security, contact center and mobility solutions for the risk-resilient enterprise. From professional services and consultancy, to managed services, to full outsourcing and IT transformation, BT is BRINGING IT ALL TOGETHER.

[bt.com](http://bt.com)



[hp.com](http://hp.com)



Enterasys delivers Secure Networks™ that ensure the confidentiality, integrity and availability of IT services and the business users that rely on them – without sacrificing performance. Thousands of enterprises worldwide rely on our convergence, connectivity and compliance solutions to deliver granular, policy-based visibility and control of individual user and application priority and security.

[enterasys.com](http://enterasys.com)



The disciplines of IT operations and security management are converging, yet the point products keep multiplying, piling on more cost and complexity. With LANDesk you can control and secure your mixed IT environment from a single console and simplify your world for less money and training, and with little or no new infrastructure.

[landesk.com](http://landesk.com)



Fortify makes software hacker-proof. Companies have done all they can to erect defenses with fire walls or anti-virus software. Yet the number of successful hacker attacks increases daily. That's because the software inside these perimeter defenses is vulnerable – and that's what hackers target. Fortify gives companies the solution they need to make their software impenetrable.

[fortity.com](http://fortity.com)



McAfee protects what the world values—from personal photos and music to the confidential records of global enterprises. Our products work together to make security affordable and manageable for everyone. The threats are tougher, and the perpetrators trickier. But as it has been for nearly 20 years, McAfee's superior protection is trusted by millions worldwide.

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

## PLATINUM (continued)



MessageLabs is a leading provider of integrated messaging and web security services, with over 16,000 clients ranging from small business to the Fortune 500 located in more than 86 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging.

[messagelabs.com](http://messagelabs.com)



The Security Division of EMC

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle—no matter where it moves, who accesses it or how it is used.

[rsa.com](http://rsa.com)

## SUNGARD® Availability Services

SunGard Availability Services is the pioneer and leading provider of Information Availability solutions, helping to ensure uninterrupted access to mission-critical data and systems. We enable nearly 10,000 clients worldwide to keep people and information connected through customized enterprise-wide solutions that support people, processes and infrastructure.

[availability.sungard.com](http://availability.sungard.com)



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.

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



SecureWorks provides the most effective Managed Security Services to over 2,000 clients in three flexible delivery options: managed, monitored and on-demand. We leverage our industry-leading threat visibility, advanced technology and 24x7 team of experts to protect clients from internal and external threats, while facilitating compliance efforts.

[secureworks.com](http://secureworks.com)



TippingPoint addresses the security needs of complex network environments for enterprises, government agencies, service providers and academic institutions. With TippingPoint's IPS-Secured Network, all network traffic is protected against internal/external attacks and device/user policies are enforced to ensure 360-degree compliance, all while simultaneously accelerating network performance. TippingPoint's solutions are complemented by the Digital Vaccine® service, powered by DVLabs.

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



Qualys, Inc. is the leading provider of on demand security risk and compliance management solutions. Qualys is the only security company that delivers these solutions through a single software-as-a-service platform. QualysGuard® allows organizations to strengthen the security of their networks and conduct automated security audits to ensure compliance with policies and regulations.

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



Sourcefire®, Inc. (NASDAQ: FIRE), SNORT® creator, is a leader in Enterprise Threat Management (ETM) solutions. The Sourcefire 3D™ System unifies IPS, NBA, NAC and Vulnerability Assessment technologies under one management console. Customers are equipped with an efficient and effective layered security defense — protecting network assets before, during and after an attack.

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



Vontu, now part of Symantec, is the leader in Data Loss Prevention solutions that combine endpoint and network-based technology to accurately detect and automatically protect confidential data wherever it is stored or used. By reducing the risk of data loss, Vontu solutions help ensure public confidence, demonstrate compliance and maintain competitive advantage.

[vontu.com](http://vontu.com)

## SILVER

Aladdin Knowledge Systems

Application Security, Inc.

ArcSight

Array Networks

BeCrypt, Inc.

Beta Systems Software

BigFix

Brabeion Software Corporation

Configuresoft

Credant Technologies

DBI

ENTRUST

Eurekify

Fortinet

Guardium

Imprivata

InfoExpress, Inc.

Intellitactics

M-Tech Information Technology, Inc.

nCipher

netForensics

NetIQ Corporation

nuBridges, Inc.

PGP Corporation

Protegrity

Rapid7, LLC

Reflex Security

SafeBoot

St. Bernard Software

SAVVIS, Inc.

SenSage

Sybase iAnywhere

Symark International

Tripwire, Inc

Veracode

Vericept

Voltage Security

\*As of February 20, 2008.

## Sponsor Opportunities

Are you interested in becoming a valued Gartner Sponsor? For further details, please contact:

**Stephen Gibertoni**

(Companies A-G)

+1 203 316 6360

[stephen.gibertoni@gartner.com](mailto:stephen.gibertoni@gartner.com)

**David Calabrese**

(Companies H-R)

+1 203 316 6298

[david.calabrese@gartner.com](mailto:david.calabrese@gartner.com)

**David Sorkin**

(Companies S-Z)

+1 203 316 3561

[david.sorkin@gartner.com](mailto:david.sorkin@gartner.com)

## Media and Association Partners



# Gartner®

56 Top Gallant Road, P.O. Box 10212, Stamford, CT 06904-2212 USA

PRESORTED  
STANDARD  
U.S. POSTAGE  
**PAID**  
GARTNER

Priority Code

Please use priority code  
when you register

## Gartner® IT Security Summit 2008

### 14th Annual Gartner IT Security Summit

June 2-4, 2008  
Gaylord National Resort & Convention Center  
Washington, D.C.

[gartner.com/us/itsecurity](http://gartner.com/us/itsecurity)

## If You Attend Only One IT Event This Year, This Is the One!

- Exceptional Case Study speakers from Gaylord Entertainment Group, Vanderbilt University and Morgan State University and others
- Captivating keynote addresses and panel discussion with renowned futurists and sci fi writers
- Special presentation of 2008 Gartner IT Security Innovation Awards Winners. Interesting in applying? Apply by April 25. Visit [gartner.com/us/itsecurityinnovation](http://gartner.com/us/itsecurityinnovation) for details.
- CISSP® CPE Certification

## Act now for \$200 discount!

Register by April 4 at [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity) or call 1 866 405 2511

## How to Register

### Registration Fees

Conference registration fee includes: Conference attendance, documentation and planned functions

Early Bird Price: \$1,795  
(If credit card payment received on or before  
April 4, 2008)

Standard Price: \$1,995  
(If credit card payment received after April 4, 2008)

SANS Institute Pre-Conference Workshop: \$495  
(not included in fees above)

### Gartner Event Tickets

We accept Gartner conference tickets as full payment. If you are a client with questions about tickets, please contact your sales representative.



## All New Venue!

### Gaylord National Resort & Convention Center

Gaylord National is a brand-new facility and one of the main focal points of National Harbor: a dynamic, 300-acre waterfront destination that incorporates the best America has to offer in quality retail, dining and entertainment.

Low Hotel Rates: Only \$221/night with the Gartner group rate