

Full Session
Descriptions
Included.

See details inside.

Gartner IT Security Summit 2003

The world's most important
conference on not getting **burned.**

June 2-4, 2003

Washington, DC

Washington Hilton & Towers

For the first time, Gartner has united its own
world-leading **Enterprise IT Security**
conference with **SECTOR5**, the premier
summit on protecting critical infrastructures.
One conference. All the issues.
Deep and wide.

Knowledge is the ultimate firewall.
Gartner IT Security Summit 2003 is
the ultimate knowledge download.

1 800 778 1997

+1 203 316 6757

www.gartner.com/us/itsecurity

Gartner

Gartner IT Security Summit 2003

The ultimate security firewall.

Table of Contents

Introduction	1-2
Pre-conference Tutorials, General Sessions and Keynotes	3-4
Enterprise IT Security Agenda-at-a-Glance	5
Enterprise IT Security Session Descriptions	6-8
SECTOR 5 Agenda-at-a-Glance	9
SECTOR 5 Participating Presenters and Session Descriptions	10-12
Enterprise IT Security Sponsors	13
SECTOR 5 Sponsors	14
Business Suite Sponsors	14
Registration Form	15

Special Keynote Speakers!



Tom Clancy
Best-Selling Author



Admiral Stansfeld Turner
Former Director of Central Intelligence

In today's highly unstable political world and highly volatile economic environment, any flaw in your IT security can spell disaster. Since extraordinary times demand extraordinary measures, we've brought together two powerful conferences — **Enterprise IT Security** and **SECTOR 5** — to create a single defining security event for IT professionals.

The unique dual-conference focus allows you to choose the agenda that is most relevant to your needs. You'll attend compelling Mastermind Keynotes and Panels each morning for the combined audience. Then spend your afternoon in hard-hitting Enterprise IT Security sessions or interactive SECTOR 5 best practice panelist sessions. And all Gartner IT Security Summit registrants are invited to attend complimentary pre-conference tutorials.

Gartner IT Security Summit's blockbuster agenda puts you at the epicenter of the information security world for three-and-a-half days of the smartest strategies, the newest tactics, and the latest technologies in IT security and critical-infrastructure protection.

ENTERPRISE IT SECURITY

In its 9th Successful Year

What is Enterprise IT Security?

At this world-leading event you'll attend dozens of in-depth, Gartner-led sessions examining IT and business strategies that are key to **acquiring, implementing, managing** and **measuring** information security.

Why Attend Enterprise IT Security?

- **Prepare yourself** for the coming changes in the IT marketplace over the next 5 years
- **Save time and money** by cutting through the clutter of competing security products to choose the ones that are right for you
- **Deflect attacks** with anti-virus and malware strategies
- **Understand the outsource alternative:** determine when, how, and whether or not to outsource
- **Maximize limited resources** with smarter buys and more effective deployment
- **Evaluate ROI and total cost of ownership** to justify your investment and get the best value from your budget
- **Create a Computer Incident Response Team (CIRT)** capable of dealing with any contingency

Who Should Attend Enterprise IT Security?

This event is custom-tailored to meet the needs of CIOs, CTOs, CSOs, VPs and Directors of IT, Network Managers, Risk Managers, Auditors and Senior Business Executives involved in security decisions.






See pages 5-8 for a complete list of Enterprise IT Security sessions and descriptions.

SECTOR5™

The World's Premier Summit on Exploring Strategies to Protect Critical Infrastructures

What is SECTOR 5?

Our second annual SECTOR 5 summit gathers the top minds in cyber and IT security from corporations, industry organizations and government agencies that represent **five critical-infrastructure sector groupings**:

-  **Sector 1 (S1) Transportation**
-  **Sector 2 (S2) Energy, Utilities and Water**
-  **Sector 3 (S3) Banking and Financial Services**
-  **Sector 4 (S4) Telecommunications and Information Services**
-  **Sector 5 (S5) Vital Health, Safety and Emergency Services**

As part of the first line of defense, you will work together with these experts and your industry peers to determine the best sector-specific approaches to security initiatives.

Over the course of the conference, each sector will progress through a series of interactive best practice panel sessions that systematically address the mission of network and organizational protection. Called "Concentrations", these focused discussion areas include:

- Concentration 1: Authentication, Biometrics and Identification**
- Concentration 2: Intrusion Detection, Response and Prevention, Viruses and Forensics**
- Concentration 3: Coordinated Crisis Response**
- Concentration 4: Security and Privacy**
- Concentration 5: Government's Role in the National Defense of Cyberspace**

Why Attend SECTOR 5?

As a SECTOR 5 delegate, your infrastructure-defense concerns will be addressed by some of the world's most respected security experts. You'll benefit from the frank exchange of ideas at **joint business and government panels...interactive, question-and-answer discussions** targeted to industry-specific forums...updates on how **pending legislation** will impact you...and extensive **case study presentations** that illustrate best practices.

You'll also learn how to avoid false starts and wasted resources through first-hand accounts of what works (and what doesn't) at **Birds-of-a-Feather** sessions. No other event offers you this unparalleled opportunity to draw upon the collective intellect of your peers — not just from within your specific critical infrastructure of interest, but on a cross-sector basis. **Share expertise and enhance your organization's ability to develop informed and thorough security strategies.**

Who Should Attend SECTOR 5?

This conference is for professionals charged with developing strategies and best practices, identifying key issues and vulnerabilities, and defending and running critical infrastructures and national interests.

SECTOR 5 Registration Qualification. Due to the nature of certain discussions and in the interest of creating audiences of industry-based peers, Gartner reserves the right to qualify registrants based on job title and company/organization affiliation. Please go to sector5.biz/who_can_attend.shtml for a table of job functions/titles that are entitled to participate. *NOTE: Due to the sensitivity of certain panel-session discussions, attendance by members of the press/media will be restricted or limited.*

See pages 9-12 for a complete list of SECTOR 5 sessions and descriptions.

IT Security Summit 2003 Contributing Organizations

As of 3/24/03

AlGeBRS
Allfirst
Ameren
AMS
Arlington County Government
Avaya
B.I.T.S.
BearingPoint
Blockade
Bluefire
BMC Software
Business Layers
Cisco
Clearswift
Computer Associates
Computer Sciences Corp.
Configuresoft
Cooley Godward LLP
Courion Corporation
Credant Technologies
Decru
ECommSecurity
EDS
Intercept
Ernst & Young
Federal Express
FORTINET
Foundstone
Freight Transportation
G-Log
GuardedNet
Guardent
I/O Software
IBM
Intel
Intellitactics
Internet Security Systems
Intrado
IntruVert
KPMG LLP
Lancope
Mazu Networks
Merrill Lynch
MessageLabs
Microsoft
M-Tech
National Security Corp.
nCircle
NetContinuum
Netegrity
NetScreen
Network Associates
Network Intelligence
NFR Security
Nokia
NOL Group/APL, Limited
Northrop Grumman
Oblix
Oracle
Partners Healthcare
Patchlink Corp
Pentasafe
PricewaterhouseCoopers
Privacilla.org
Prudential
QinetiQ
Qualys
Radware
Remedy
RSA Security
S1
Sabre Laboratories
SAIC
Sanctum Inc.
SCANA
SecureLogix
SecureWave
Securify
SilentRunner
Sourcefire
Southeastern Pennsylvania Transportation Authority
SPI Dynamics
Stratum8 Networks
Sun Microsystems
Symantec Corporation
Symark Software
Top Layer
Trend Micro
Tripwire
TruSecure
Unisys
UPS
VeriSign
Verizon Federal Network Systems
Voцент Solutions
Waveset
Whale Communications

IT Security Summit Shared Sessions

COMPLIMENTARY PRE-CONFERENCE TUTORIALS

Please note that Tutorials are on Sunday,
5:30 – 6:30 PM.

(T1) PKI, Digital Signatures

Victor Wheatman, Vice President, Research Area Director, Gartner

Once promoted as a security panacea, PKI is past the “Peak of Inflated Expectations” and well into the “Trough of Disillusionment” on the Gartner hype cycle. Key issues include:

- What are the differences between digital and electronic signatures?
- How will PKI disappear into applications to provide productivity without calling attention to itself?

(T2) Internet Security 101

Richard Stiennon, Research Director, Gartner

This tutorial establishes the key requirements for today’s Internet-standards-based networks, as well as the protections required for Web servers and the applications maintained by them.

- What core elements comprise effective, multilayered Internet security strategies?
- What are the relative roles of firewalls, intrusion detection, Web assurance products and antivirals in protecting enterprise networks?
- What are the missing pieces in products designed to protect TCP/IP networks, and what should enterprises do to address the gap between product availability and vulnerabilities?

(T3) Enterprise Security Strategies for Windows

John Pescatore, Vice President, Gartner

Viruses, worms and Web site hacking have continued to pound on Windows-based PCs and Web servers, to the tune of billions of dollars of worldwide impact. Terrorist attacks and threat of cyber crime and information warfare caused CXOs to elevate the priority of security in enterprise software and systems decisions. Microsoft has tried to react to increased concerns about security by promising to move to “Trustworthy Computing.”

- Will Microsoft’s Trustworthy Computing Initiative change how enterprises will need to secure Windows-based system?
- How will emerging standards and technologies, such as wireless, XML and Web services, affect implementing and managing PC and server security?
- How will Windows security management be implemented in both homogeneous and heterogeneous environments?

(T4) Rule Sets in Firewalls

John P. Dubiel, Vice President, Gartner

This tutorial looks at the concepts of security rule sets and how they can be applied to firewalls. Further, how can firewall rule sets be used within a security architecture containing other firewalls and security devices and how a coordination of rule sets provide stronger protection than a single rule set.

- What are the best practices for establishing, maintaining and testing rule sets?
- What are some of the common problems posed by applications and protocols blocking effective rule set deployment?
- How should rule set administrators solve the problems posed by coordination among multiple devices in a security architecture?

GENERAL SESSIONS

Information Security Scenario: Towards a Common Defense in CyberSpace

Vic Wheatman, Vice President, Research Director, and Richard Hunter, Vice President, Gartner

Enterprises work on a daily basis to secure their systems through continually evolving technologies such as firewalls, intrusion protection systems and antivirals. Meanwhile, public officials and private sector analysts raise the specter of large-scale cyber-attacks mounted by nation-states, criminal organizations, or terrorists. Public and private security professionals must find a balance and determine the realism. Is a common defense in cyberspace necessary? If so, what models exist for constructing a common defense in the current environment? What changes will new policies and procedures cause industries, enterprises, and individuals in terms of sharing vulnerabilities and risking personal freedoms?

Digital Pearl Harbor: Is It Only a War Game?

The joint Gartner/US Naval War College exercise titled “Digital Pearl Harbor,” first conducted in July 2002 with almost 100 participants from four critical infrastructure industries, is one of the most rigorous attempts to-date to define realistic scenarios for large-scale cyber-attacks. The news from the Digital Pearl Harbor exercise is less frightening than novelistic visions of cyber-Armedgeddon, but sobering enough for anyone charged with defending critical infrastructure against cyber-attack.

IT Security Summit Shared Sessions

MASTERMIND PANELS

Mastermind Government Defenders Panel

It takes a tough crew to protect cyberspace in a free society. This panel, comprised of some of the most experienced cyber-security and law-enforcement professionals in the world, discusses issues, threats, and opportunities as seen by the government agencies charged with protecting the innocent from the dangerous in cyber space.

Expert Insights and Intelligence on Cyber Threats

Intelligence, the key to PREVENTION. This is what ALL corporations, vital interests and government agencies strive to achieve when it comes to the threats and possibilities of cyber crime and/or cyber terrorism. Having the right intelligence and the right information allows IT security professionals and those responsible for the safe-guarding of critical data, employees and citizens, to understand what the possible next threats are, and where they may emanate from. This, in return, may PREVENT loss or damage from happening. Join this Mastermind session and gain valuable strategic insights concerning where the next threats may emerge and how to handle them.

Corporate CIO/CISO Mastermind Panel

What keeps corporate CIOs and CISOs up at night? Is it the 16-year-old joy-riding hacker; a possible internal security breach which puts their company on the front page of the Wall Street Journal; a potential cyber-attack from politically motivated threat agents funded by foreign interests? Or is it the daily, weekly, annual implementation of a strategic security plan in a highly dynamic environment? This session with leading CIOs and CISOs probes these questions from the perspective that the bottom line matters.

SPECIAL KEYNOTES

From Fiction to Reality with Tom Clancy

Tom Clancy, Best-Selling Novelist



Tom Clancy is the best-selling novelist and popular commentator on technology and the military. Who better than Clancy, whose own

works of fiction are already legendary for their vision, techno-savvy, and keen understanding of military operations, to make sense of all of it for our conference attendees? Clancy will be featured in a wide-ranging "fireside chat" with leading Gartner analysts, providing his unique perspective and creative intelligence on today's pressing concerns over national security and the intersection of technology with the expanding scope of threats facing the United States.

Where We Stand on the War on Terrorism

Admiral Stansfield Turner, USN (ret.), Former Director of Central Intelligence



A former Director of the Central Intelligence Agency and a U.S. Navy Commander, Admiral Stansfield Turner is an expert on global security.

During his tenure at the CIA, he was responsible for spearheading major technological developments and managerial reforms. In addition to authoring four books (including the best-selling *Caging the Genies: A Workable Plan for Nuclear, Chemical and Biological Weapons*), Turner is a Senior Research Scholar at the Center for International and Security Studies at the University of Maryland. Turner will share his perspective on national and homeland security, modern warfare, terrorism and information gathering. His presentation will focus on what it takes to "win" the war against terrorism and how we can reduce the threat to manageable proportions. He will also tackle the tough issue of how to balance effectiveness against terrorists with intrusions into our liberties and privacy.

Start putting your cyber-crime defense into action.

Register now!

CALL 1 800 778 1997 or +1 203 316 6757 or go to gartner.com/us/itsecurity

FREE Diagnostic Evaluation

Test your own organization's security preparedness.

Visit

gartner.com/us/itsecurity today and take our short IT Security Self-Diagnostic Test to see how your organization's approach measures up against some of the key indicators of a sound security strategy.

Enterprise IT Security

Sunday 1 June 2003

4:00 PM – 6:00 PM	Pre-Event Registration			
5:30 PM – 6:30 PM	Pre-Event Tutorials			
Complimentary!	(T1) PKI, Digital Signatures	(T2) Internet Security 101		
	(T3) Enterprise Security Strategies for Windows	(T4) Rule Sets in Firewalls		

Monday 2 June 2003

7:00 AM	Registration			
7:00 AM – 8:30 AM	Continental Breakfast			
8:30 AM – 9:00 AM	Welcome and Introductions			
9:00 AM – 10:00 AM	Information Security Scenario: Towards a Common Defense in CyberSpace			
10:00 AM – 10:15 AM	Networking Break			
10:15 AM – 11:15 AM	Keynote Interview: <i>From Fiction to Reality: Tom Clancy, Best-Selling Novelist</i>			
11:15 AM – 11:30 AM	Networking Break			
11:30 AM – 12:30 PM	Digital Pearl Harbor: Is It Only a War Game?			
12:30 PM – 1:30 PM	Opening Showfloor Luncheon			
1:30 PM – 2:30 PM	Mastermind Government Defenders Panel			
2:30 PM – 2:45 PM	Coffee Break on the Showfloor			
2:45 PM – 3:45 PM	Track Sessions (Tracks A-D run concurrently)			
	TRACK A: Acquiring Information Security	TRACK B: Implementing Information Security	TRACK C: Managing Information Security	TRACK D: Measuring Information Security
	(A1) How to Save \$1 Million Negotiating a Security Software Contract	(B1) Security Architectures for the New Enterprise	(C1) Organizational Structures for Information Security	(D1) Enterprise Liability for Poor Security Practices
3:45 PM – 4:00 PM	Coffee Break on Showfloor			
4:00 PM – 4:45 PM	Sponsor Workshops			
4:45 PM – 5:00 PM	Coffee Break on Showfloor			
5:00 PM – 6:00 PM	(A2) Case Study: Developing Security RFPs in Government	(B2) Compliance with Sarbanes-Oxley 'Corporate Responsibility' Act	(C2) Managing a Computer Incident Response Team	(D2) Measuring Information Security Effectiveness
6:00 PM – 8:00 PM	Corporate Sponsor Showcase Reception			

Color Key:

	Enterprise IT Security Sessions
	Combined/Shared Sessions

Tuesday 3 June 2003

7:00 AM	Registration			
7:00 AM – 8:00 AM	Networking Breakfast			
8:00 AM – 9:00 AM	Vendor Case Study Panels			
9:00 AM – 9:15 AM	Coffee Break on the Showfloor			
9:15 AM – 10:15 AM	Mastermind Panel: Expert Insights and Intelligence on Cyber Threats			
10:15 AM – 10:30 AM	Coffee Break on the Showfloor			
10:30 AM – 11:30 AM	Corporate CIO/CISO Mastermind Panel			
11:30 AM – 1:00 PM	Lunch/Dessert On Show Floor			
1:00 PM – 2:00 PM	Track Sessions			
	(A3) Understanding the Information Security Marketplace	(B3) Implementing Effective Anti-Virus Architectures	(C3) Business Continuity and Disaster Recovery Planning	(D3) Dynamic Trust Models
2:00 PM – 2:30 PM	Coffee Break on the Showfloor			
2:30 PM – 3:15 PM	Sponsor Workshops			
3:00 PM – 3:30 PM	Coffee Break on the Showfloor			
3:30 PM – 4:30 PM	(A4) Technical Security Standards: Do they Matter?	(B4) Security on the Run: Implementing Wireless and Mobile Security	(C4) Case Study: Gartner's CSO on Information Security	(D4) Mad as Hell: Computer Forensics for Dummies
4:30 PM – 5:00 PM	Coffee Break on the Showfloor			
5:00 PM – 5:45 PM	Sponsor Workshops			
5:45 PM – 8:45 PM	Hospitality Suite Event			

Wednesday 4 June 2003

7:00 AM – 8:00 AM	Breakfast with the Analysts			
8:00 AM – 9:00 AM	Track Sessions			
	(A5) Managed Security Services – Market in Transition	(B5) Enterprise Security Architecture for Web Services	(C5) IT Security Management: Fighting Fires and False Alarms	(D5) Measuring Identity and Access Management TCO
9:00 AM – 9:30 AM	Networking Break			
9:30 AM – 10:30 AM	(A6) Intrusion Detection is Dead, Long Live Intrusion Prevention	(B6) Preparing the Enterprise to Combat Social Engineering Attacks	(C6) Case Study: PKI and Smart Cards in the Federal Government	(D6) CyberInsurance Policies: The Measure of Security
10:30 AM – 10:45 AM	Networking Break			
10:45 AM – 11:45 AM	Keynote: Where we Stand on the War on Terrorism: Admiral Stansfield Turner, USN (ret.) Former Director of Central Intelligence			
11:45 AM	Conference Adjourns			

(Agenda subject to change without notice)

TRACKS

(Tracks A-D run concurrently)

TRACK A: Acquiring Information Security

TRACK B: Implementing Information Security

TRACK C: Managing Information Security

TRACK D: Measuring Information Security

Day 1

Monday, June 2

(A1) How to Save \$1 Million Negotiating a Security Software Contract

Frank DeSalvo, Research Director, Gartner

This presentation addresses the specific terms in the licensing agreement that can have a profound effect of the total cost of ownership. Key issues include:

- Why should you be concerned with terms and conditions — not just the price of the software?
- What are the terms that can lower my TCO of security software?
- Where are the ‘Gotchas’ in negotiating a security software license?

(B1) Security Architectures for the New Enterprise

Ray Wagner, Research Director, Gartner

Enterprise architectures are evolving to support a wide range of business functions over a broad set of constituents. Web services, wireless applications, content management and other technologies are enabling architectural evolution, but each has its own security risks. Key issues include:

- What new business styles and new applications are driving the new enterprise architectures?
- What security patterns can be implemented to reduce risks in business?
- How can enterprises develop a security architecture that supports a balanced risk portfolio?

(C1) Organizational Structures for Information Security

Roberta Witty, Research Director, Gartner

The growing focus on managing information security is challenging most organizations to figure out who should manage it, what should be managed, where it should reside within the organization, and how much should be spent on securing enterprise assets. Key issues include:

- What does a successful information security organization look like?
- Who should staff the information security organization?
- What are the spending patterns for a successful information security organization?

(D1) Enterprise Liability for Poor Security Practices

Ben Wright, Esq., Attorney and Founding Author
“The Law of Electronic Commerce”

Increasingly, courts and government policy makers expect corporate users and providers of information systems to maintain security. Key issues include:

- How can enterprises be held accountable for hackers and malicious code?
- What is the potential for enterprise “downstream liability” if the entity has poor security?
- What are the methods for limiting legal exposure to the risks associated with sharing information about security vulnerabilities?

(A2) Case Study: Developing Security RFPs in Government

Bill Spornow, Chief Information Security Officer,
Georgia Student Finance Commission

A case study where luck ran out and a serious security breach received media attention. The case presents details on requirements, war stories and the development of nearly two dozen security RFPs. Key issues include:

- How will enterprises organize for information security?
- Which solutions are best for solving enterprise information security problems?
- How should enterprises evaluate competing offers from a variety of security providers?

(B2) Compliance with Sarbanes-Oxley ‘Corporate Responsibility’ Act

Ben Wright, Esq., Attorney and Founding Author
“The Law of Electronic Commerce”

This presentation includes analysis of cases such as the criminal prosecution of Arthur Andersen for destroying records, the pressure under the privacy laws to secure digital records and the implications that computer forensics has for corporate record retention/destruction policies. Key issues include:

- What is the conflict between laws requiring record destruction and those that forbid it?
- What is enterprise liability under the new “corporate responsibility” Sarbanes-Oxley legislation?
- Why do electronic records render traditional records management practices obsolete?

(C2) Managing a Computer Incident Response Team

Rich Mogull, Research Director, Gartner

This presentation examines the process of justifying and creating a Cyber Incident Response Team (CIRT) and how such a team can be used to mitigate risks. Key issues include:

- How should a CIRT be structured?
- What skill sets are needed to build an effective CIRT?
- What is the role of third parties in providing forensics and services to enterprises that have suffered from a cyber-crime?

(D2) Measuring Information Security Effectiveness

Colin Buckley, Senior Research Analyst,
Measurement, Gartner

By measuring costs, service-levels, and best practice adherence against a relative measure of risk, Gartner’s TCO methodology offers a consistent, meaningful framework for managing and communicating information security effectiveness. Key issues include:

- What non-technical models can help organizations consistently measure security efficiency and effectiveness?
- How can enterprises highlight security improvement opportunities through comparisons with other organizations?

- How can organizations objectively communicate their information security successes and opportunities, and justify needed resources?

Day 2

Tuesday, June 3

(A3) Understanding the Information Security Marketplace

John Pescatore, Vice President, Gartner

This presentation predicts how the information security market will change over the next 3 years, recommends strategic and tactical investment strategies, and identifies the key characteristics of marketplace winners. Key issues include:

- How will the information security marketplace shake out between now and 2007?
- What elements of the information security marketplace are mature enough for safe investment, and which are speculative?

(B3) Implementing Effective Anti-Virus Architectures

*Richard Stiennon, Research Director, Gartner
Arabella Hallawell, Research Director, Gartner*

The presentation presents Gartner's Magic Quadrant of AV products, discusses the potential for malware as a terrorist threat, and examines multi-headed worms that bypass e-mail and tunnel through enterprise gateways. Key issues include:

- How is the viral threat scenario changing and what are AV vendors doing to combat these threats?
- What improvements are being made in anti-viral signature response times?
- What new anti-viral defense mechanisms are evolving?

(C3) Business Continuity and Disaster Recovery Planning

Roberta Witty, Research Director, Gartner

This presentation focuses on best practices in business continuity planning, including scope, approach, technologies and services. Key issues include:

- How will enterprises mitigate risks of business process downtime?

- What tools, technologies and processes will enterprises employ to protect critical applications and business processes?
- How will the market for business continuity services evolve?

(D3) Dynamic Trust Models

Richard Mogull, Research Director, Gartner

As technology enables the real-time economy, the network-enabled enterprise and virtual value chains, it impacts the way we develop and manage relationships. This session demonstrates how to implement "dynamic trust," as the foundation for risk management. Key issues include:

- How has technology impacted my internal and external business relationships?
- How does the drive toward a "real-time economy" and virtualization expose me to more risk?
- How can I manage these risks and implement "dynamic trust" with today's services and technologies?

(A4) Technical Security Standards: Do they Matter?

Greg Young, Associate Director, Consulting, Gartner

Many government standards organizations "certify" compliance of security products with technical standards. Although such testing is important, limiting product evaluation to certified products might lead to inappropriate selection. Key issues include:

- Which of several security specifications are most relevant to enterprises in their vendor and product evaluations?
- How can non-government organizations use "protection profiles" and "security targets" to evaluate information assurance products?
- How should information security product providers ensure the continuing certification of their products as they go through generation evolution?

(B4) Security on the Run: Implementing Wireless and Mobile Security

John Pescatore, Vice President, Gartner; John Girard, Vice President, Research Director, Gartner

Mobile and wireless devices bypass firewalls, open networks to new risks and allow sensitive information to be clipped on to employees belts. The evolving standards appear wanting and often at cross purposes. Key issues include:

- What will be the most significant obstacles to the deployment of VPN technologies through 2006?
- What strategies and tactics will prove best for managing mobile TCO?
- What will be the typical support and security problems experienced by remote users?

(C4) Case Study: Gartner's CSO on Information Security

Michael Zboray, Chief Security Officer, Gartner

In this session we examine how Gartner itself has identified, prioritized and mitigated risks within the context of a fixed budget. We will discuss lessons learned in the areas of implementation and operation and review Gartner's plan to improve risk management. Key issues include:

- How will enterprises arm themselves to address increasing information security risks?
- How can you outsource and be safe?
- What best practices will information security organizations adopt to avoid potential legal liability and safeguard intellectual assets?

(D4) Mad As Hell: Computer Forensics for Dummies

Bill Spernow, Chief Information Security Officer, Georgia Student Finance Commission

This presentation demystifies computer-based forensic analysts. Discussion pivots on policies and procedures, staffing, investigative issues, forensic techniques, commercial tools, court testimony, sources of training and support, emerging technical challenges and the costs of developing computer-based capabilities.

Day 3

Wednesday, June 4

(A5) Managed Security Services — Market in Transition

Kelly M. Kavanaugh, Senior Analyst, Gartner

Enterprises have begun to recognize the value of outsourcing day-to-day security tasks such as monitoring firewalls and intrusion detection systems. Key issues include:

- What does consolidation mean for the managed security market, and who will be the dominant vendors?
- What are the key criteria for choosing a managed security services provider?
- What do enterprises that turn to managed security look for?

(B5) Enterprise Security Architecture for Web Services

Raymond Wagner, Research Director, Gartner

This presentation looks at several examples of how Web services are secured, the standards involved, issues of trust, and what the implications of Web services are for the rest of an enterprise security program. Key issues include:

- How are Web services secured?
- What are the relevant technologies and standards and what is their state of development?
- What are the security implications of Web services deployment for the rest of your enterprise?

(C5) IT Security Management: Fighting Fires and False Alarms

Mark Nicolett, Vice President, Research Director, Gartner

The IT security operations group is overwhelmed with security event and alert data from sensors, network devices, servers and applications. The challenge is to find the burning security problems amidst the din of false alarms. Key issues include:

- What are the security operations issues that IT security management technologies attempt to solve?
- What are the functional characteristics of an effective IT security management product?

- Which vendors provide the most effective IT security management products today, and what is the future of the emerging IT security management market?

(D5) Measuring Identity and Access Management TCO

Roberta J. Witty, Research Director, Gartner

In this presentation we discuss how user account and privilege administration can be better managed, and discuss the relationships between directories, single-sign-on and employee provisioning. Key issues include:

- How will the changing technical environment affect security administration requirements?
- What best practices and strategies should enterprises adopt to ensure a well managed and secure user administration facility?
- What tools, technologies and products will enterprises employ to manage user accounts and privileges?

(A6) Intrusion Detection is Dead, Long Live Intrusion Prevention

Richard Steinon, Research Director, Gartner

A sea-change in security defensive mechanisms is rapidly causing IDS to be relegated to a niche play. Enterprise protection and intrusion prevention will finally provide a better security posture for the enterprise. Key issues include:

- How will inline-network intrusion detection allow the first network intrusion prevention solution?
- At what point should an enterprise outsource for intrusion detection and prevention services, and when should the function be kept in house?
- Who are the market leaders in intrusion detection/prevention services and what is their strategy?

(B6) Preparing the Enterprise to Combat Social Engineering Attacks

Rich Mogull, Research Director, Gartner

This presentation focuses on the human side of security, with specific strategies and actions that enterprises need to take to limit the effectiveness of social engineering attacks. Key issues include:

- How is social engineering used to breach security?
- What specific techniques can be used by enterprises to limit their vulnerability to social engineering?
- How can organizations coordinate their physical/organizational security with their information security efforts to limit their vulnerability to social engineering?

(C6) Case Study: PKI and Smart Cards in the Federal Government

Tim Polk, PKI Program Manager for NIST

Will the government be able to demonstrate ROI and improve security when few commercial PKI projects have done so to date? The speaker, the PKI Program Manager for the National Institute of Standards and Technology, is in a good position to assess the situation. Key issues include:

- What government agency applications will use PKI to its full potential?
- How will the Federal Bridge Certificate Authority work to cross-certify entities?
- What lessons can commercial enterprises learn from the Government's PKI and smart card programs?

(D6) CyberInsurance Policies: The Measure of Security

Vincent Oliva, Vice President, Research Director, Gartner; Arabella Hallawell, Research Director, Gartner

What are the regulatory and legal risks of poor security, and how can those risks be mitigated through cyber insurance policies. The costs of implementing security controls in order to receive such insurance defines the costs of remediating the risks. Key issues include:

- When does it make sense to evaluate cyber security insurance policies, for what types of coverage?
- Who provides cyber insurance policies and what are the costs?
- How much should enterprises spend to reasonably insure good enough security?

Sunday 1 June 2003

4:00 PM – 6:00 PM	Pre-Event Registration	
5:30 PM – 6:30 PM	Pre-Conference Tutorials:	
Complimentary!	(T1) PKI, Digital Signatures	(T2) Internet Security 101
	(T3) Enterprise Security Strategies for Windows	(T4) Rule Sets in Firewalls

Monday 2 June 2003

7:00 AM	Registration
7:00 AM – 8:30 AM	Continental Breakfast
8:30 AM – 9:00 AM	Welcome and Introductions
9:00 AM – 10:00 AM	Information Security Scenario: Towards a Common Defense in CyberSpace
10:00 AM – 10:15 AM	Networking Break
10:15 AM – 11:15 AM	Keynote Interview: From Fiction to Reality: Tom Clancy, Best-Selling Novelist
11:15 AM – 11:30 AM	Networking Break
11:30 AM – 12:30 PM	Digital Pearl Harbor: Is It Only a War Game?
12:30 PM – 1:30 PM	Opening Showfloor Luncheon
1:30 PM – 2:30 PM	Mastermind Government Defenders Panel
2:30 PM – 2:45 PM	Coffee Break on the Showfloor
2:45 PM – 4:15 PM	Concentration 1: Authentication, Biometrics, Identification (SECTORS 1-5 run concurrently)
	Transportation Energy, Utilities and Water Banking and Financial Services Telecommunications and Information Services Vital Health, Safety, and Emergency Services
4:15 PM – 4:30 PM	Coffee Break on the Showfloor
4:30 PM – 6:00 PM	Concentration 2: Intrusion Detection, Response and Prevention, Viruses and Forensics (SECTORS 1-5 run concurrently)
	Transportation Energy, Utilities and Water Banking and Financial Services Telecommunications and Information Services Vital Health, Safety, and Emergency Services
6:00 PM – 8:00 PM	Corporate Sponsor Showcase Reception

Color Key:

- SECTOR 5 Sessions
- Combined/Shared Sessions

Tuesday 3 June 2003

7:00 AM	Registration
7:00 AM – 8:00 AM	Networking Breakfast
8:00 AM – 8:45 AM	SECTOR 5 Sponsor Workshops
8:45 AM – 9:15 AM	Coffee Break on the Showfloor
9:15 AM – 10:15 AM	Mastermind Panel: Expert Insights and Intelligence on Cyber Threats
10:15 AM – 10:30 AM	Coffee Break on the Showfloor
10:30 AM – 11:30 AM	Corporate CIO/CISO Mastermind Panel
11:30 AM – 1:00 PM	Lunch/Dessert On Show Floor
1:00 PM – 2:30 PM	Concentration 3: Coordinated Crisis Response (SECTORS 1-5 run concurrently)
	Transportation Energy, Utilities and Water Banking and Financial Services Telecommunications and Information Services Vital Health, Safety, and Emergency Services
2:30 PM – 3:00 PM	Coffee Break on the Showfloor
3:00 PM – 3:45 PM	SECTOR 5 Sponsor Workshops
3:45 PM – 4:15 PM	Coffee Break on the Showfloor
4:15 PM – 5:45 PM	Concentration 4: Security and Privacy (SECTORS 1-5 run concurrently)
	Transportation Energy, Utilities and Water Banking and Financial Services Telecommunications and Information Services Vital Health, Safety, and Emergency Services

Wednesday 4 June 2003

7:00 AM – 8:00 AM	Breakfast with the Analysts
8:00 AM – 8:45 AM	Birds-of-a-Feather: Opportunity to network based on common interests in areas that include industry, professional title and role, and specific security-related topics.
8:45 AM – 9:00 AM	Networking Break
9:00 AM – 10:30 AM	Concentration 5: Government's Role in the National Defense of Cyberspace
	All Sectors – Combined General Session
10:30 AM – 10:45 AM	Networking Break
10:45 AM – 11:45 AM	Keynote: Where We Stand on the War on Terrorism: Admiral Stansfield Turner, USN (ret.) Former Director of Central Intelligence
11:45 AM	Conference Adjourns

(Agenda subject to change without notice)

Participating **SECTOR5™** Presenters

AlGeBRS, Ty R. Sagalow, EVP, COO
Allfirst, John Walsh, VP and Information Security Manager
AMS, Matthew Dezee, VP, Digital Government
Arlington County Government, Vivek Kundra, Dir, Infrastructure Technologies
Ameren, Robin Goatey, Process Measurement Specialist/IT Coordinator for Power Operations
Avaya, Ken Pfeil, Senior Security Consultant
B.I.T.S., Catherine A. Allen, CEO
B.I.T.S., John Carlson, Senior Director
BearingPoint, Art Ehuan, Manager
Cisco, Ken Watson, Senior Manager, Critical Infrastructure Assurance Group
Cisco, Lance Hayden, Strategic Consulting Manager
Computer Associates, John Sabo, Business Manager
Computer Sciences Corp., Ronald L. Dick, Director, Information Assurances Strategic Initiatives
Cooley Godward LLP, Randy V. Sabett, Attorney
Credant Technologies, Dwayne Mann, CTO
ECommSecurity, Phyllis Schneck, VP, Enterprise Services
EDS, Mike Hulley, President
Federal Express, David Zanca, VP, Information Security and Business Continuity
FORTINET, Ken Xie, Founder, President & CEO
Foundstone, Kevin Mandia, Director of Computer Forensics
Foundstone, Stuart McClure, President & CTO
Freight Transportation Security Consortium, Drew Robertson, Director
G-Log, Steven Gaines, VP, Marketing
IBM, Lois McKeon, VP
Intel, Mark N Blatt, Manager, Health Strategies
Internet Security Systems, Patrick Gray, Director
Intrado, Stephen Meer, Co-Founder, CTO, VP
I/O Software, William Saito, President & CEO
Mazu Networks, Jim Melvin, President & CEO
Merrill Lynch, David LaBianca, VP, Information Security and Privacy
National Security Corp., Mark Hardy, CISSP, CISA
NOL Group/APL, Limited, Cindy Stoddard, CIO
Northrop Grumman, Robert Brammer, VP & CTO
Oracle, Mary Ann Davidson, CSO
Partners Healthcare, Scott Rogala, Corp Mgr, Network Engineering & Security
Patchlink Corp, Sean Moshir, CEO
Privacilla.org, James Harper, Editor
Prudential, Kenneth Tyminski, Chief Information and Security Officer
QinetiQ Trusted Information Management, Peter Stephenson, Director of Research
Remedy, Doug Mueller, Co-Founder
RSA Security, Bill McQuaid, SVP, Authentication Products Division
S1, Al Kirkpatrick
Sabre Laboratories, Bob Offutt, Senior VP
SAIC, Bettina M. Stopford, Senior Program Analyst
SAIC, William J Marlow, SVP
SCANA, Andy Bowden, Security Director
SecureLogix, Lee Sutterfield, President
SecureWave, Dennis Szerszen, Consultant
Southeastern Pennsylvania Transportation Authority, Ralph Menzano, CIO
Symantec Corporation, Lawrence Dietz, Director, Market Intelligence
Top Layer, Joe Magee, CSO
Unisys, Steven Vinsik, Senior Solutions Specialist
Unisys, Sunil Misra, CSO
UPS, Jim Flynn, Director of IT Security
Verizon Federal Network Systems, Bruce Fleming, CTO
Vocent Solutions, Chuck Buffum, CEO & Co-Founder
Whale Communications, Elad Baron, CEO

For an updated list of speakers visit sector5.biz



S.1 Transportation



Concentration 1

Authentication, Biometrics, Identification

How can transportation workers most effectively be identified and authenticated, beyond TWICS, into other key industry sectors: rail, ports and maritime, hazardous material trucking? What technologies and practices will assist carriers to develop trusted shipper programs in foreign ports? What is keeping trusted traveler biometric programs from more rapid adoption? When and how will computer-aided passenger profiling systems (CAPPS) be enhanced?



Concentration 2

Intrusion Detection, Response and Prevention, Viruses and Forensics

What new IT tools and methodologies are emerging for intrusion detection? How can you prevent attacks or theft of vital supply chain data in shared web portals? How effectively can RFID and other technologies prevent and/or detect tampering with cargo containers on ships, trains, and trucks?



Concentration 3

Coordinated Crisis Response

Do you have effective plans in place to recover supply chain information loss? What are the cost/benefit tradeoffs of business continuity processes? How often do these plans need to be tested, validated, updated? Under what conditions should shippers, assembly plants and merchants increase safety stock levels to cover possible attacks?



Concentration 4

Security and Privacy

What level of controlled ID and physical access monitoring will transportation workers accept? Will airline passengers trade some privacy for “preferred traveler” status? What degree of database-linked profiling will the public tolerate? What specialized security controls are needed for web cargo portal access?



S.2 Energy, Utilities and Water

✳ Concentration 1

Authentication, Biometrics, Identification

How can field and operation center energy workers most effectively be identified and authenticated, within energy operations centers and between SCADA and field operations? How should company operations with other operations entities be authenticated and authorized? What technologies and practices will assist utilities to develop trusted relationships with other critical infrastructure providers, such as telecommunications, government, – etc.? How do we protect SCADA systems the communication, command and control mechanism of the energy infrastructure? Are these systems targets by increasing their capabilities? What are the latest trends and directions in SCADA security?

✳ Concentration 2

Intrusion Detection, Response and Prevention, Viruses and Forensics

Do open versus proprietary SCADA systems provide any more or less of a target for potential attackers? As SCADA systems continue to adopt open standards, and use other critical infrastructures such as the Internet and office and field wireless technology for remote station operations and mobile operations, how do we protect, detect and recover these systems from attack? What IT/security tools and methodologies are most effective and which ones are emerging for intrusion detection? What are the most effective means of protecting infrastructure that is geographically widely distributed? How do we protect the physical assets (eg, physical monitoring, biometrics) of the energy infrastructure – what's missing, what are the current problems and potential solutions?

✳ Concentration 3

Coordinated Crisis Response

How broad should crisis response planning be? Local, regional, national, inter- or intra-CIP? Do we have effective plans in place to protect the entire energy delivery, supply chain? What are the most critical elements of the supply chain and are the control mechanisms of this supply chain adequately protected and is information loss or disruption critical to the reliable operation of the critical infrastructure? What are the cost/benefit tradeoffs of business continuity processes? The energy industry provides the raw energy that sustains the operation of many of the other CIP's. Do we have/need a coordinated crisis response mechanisms between CIPs?

✳ Concentration 4

Security and Privacy

Has the deregulation of the electric utility industry, and the separation into Genco, Transco, and Distco, and ISO elements created new security issues for the industry? What is the effect on CIP? Has the market been made less secure by financial deregulation and the new interactions between the parties? How do we provide privacy for business transactions while still maintaining a reliable operating environment? What is the role of the various marketplaces in managing the privacy of the participants in the marketplace vs. maintaining the security of the marketplace?



S.3 Banking and Financial Services

✳ Concentration 1

Authentication, Biometrics, Identification

How can financial service providers authenticate and identify external clients and suppliers without jeopardizing their trusted relationship reputation but still assure and demonstrate effective verification routines? What technologies and practices will assist financial service providers in identifying and authenticating internal and external users? Is biometrics gaining popularity and acceptance among financial customers?

✳ Concentration 2

Intrusion Detection, Response and Prevention, Viruses and Forensics

Who's knocking at the door of financial service providers' systems? What practices and frameworks provide early detection of intrusive activity? What technologies assist in the determination, incident evaluation, prevention and response to intrusion? What patterns or behavioral activities help FSPs understand false versus positive intrusions?

✳ Concentration 3

Coordinated Crisis Response

What procedures should be in place to coordinate an effective message to your customers and internal staff if a crisis occurs? What determines a crisis? What relationships should FSPs create for backup and processing? What is the cost and benefits trade off of business continuity approaches?

✳ Concentration 4

Security and Privacy

How should FSPs provide security and still maintain customer privacy? How do you balance your security vs privacy message with your consumer base? Should physical and virtual security have common leadership? What role can technology support in balancing the security/privacy dilemma?



S.4 Telecommunications and Information Services

Concentration 1

Authentication, Biometrics, Identification

How can users of information and network services be authenticated as services move desktop, servers, and data centers to incorporate fixed, circuit switched systems to incorporate wireless, mobile, and packet-based access? How will multi-vendor information users integrate with service providers authentication systems in a multi-carrier environment; who is minding the ship? How can the pressure to maintain security costs be balanced against the growing complexity of identity and access management tools?

Concentration 2

Intrusion Detection, Response and Prevention, Viruses and Forensics

How can user systems and connected data and voice service provider's infrastructure be protected from intrusion and denial-of-service attacks? What new tools and techniques are available? How far is the responsibility for such protection shifting from systems and servers, towards the network infrastructure and "in the cloud" security services?

Concentration 3

Coordinated Crisis Response

How can critical information and network resources be maintained in disaster scenarios? How can enterprises assess the likelihood and impact of different types of disaster? What techniques and tools are available to build resilience into "infocom" infrastructures, and to recover when the worst happens?

Concentration 4

Security and Privacy

What responsibilities do enterprises and telecommunication service providers have for protecting the increasing quantities of personal and business information that are transported and stored on their infrastructures? Can we expect increased government regulation of privacy? What tools and techniques are available to enterprises to maintain privacy of their own and their customer's information?



S.5 Vital Health, Safety, and Emergency Services

Concentration 1

Authentication, Biometrics, Identification

Information is key to mitigating disasters. However, the same information that can save lives and be used to destroy when in the wrong hands. How can authentication and the associated technologies ensure the right information reaches the right people and only the right people?

Concentration 2

Intrusion Detection, Response and Prevention, Viruses and Forensics

If government networks are carrying critical information, the information must be protected, sometimes at any cost. Tracking, identifying, and neutralizing cyberterrorists is and must be a top priority.

Concentration 3

Coordinated Crisis Response

Disasters, both natural and contrived, will happen. Often, people and businesses look to the first responders to forestall the effects and to begin rescue and recovery. In order to do so, they must be the best prepared to recover. How can projects like CapWIN help with cyber attacks?

Concentration 4

Security and Privacy

One of the fundamental questions for the public sector is how is the public's right to know balanced with the individual's right to privacy? As technology advances, so do the opportunities to use and misuse private information. How will HIPAA influence privacy and the need for a secure infrastructure?

All Sectors

Concentration 5

SECTOR 5 Combined Session: Government's Role in the National Defense of Cyberspace

The National Strategy to Secure Cyberspace, released in February 2003, has elevated the issue of a common defense in cyberspace, while endorsing a less active government role in protecting cyberspace from attacks from terrorists and criminals. This concentration will examine the many implications of this new plan. How should the government collaborate with the private sector? What will be role of the new Department of Homeland Security? Will there be government funding for any initiatives? What standardization of reporting will be required?

These and other questions will be tackled in a joint session of the five Sectors.

For speaker, session and sponsor updates visit gartner.com/us/itsecurity

Premier

Ernst & Young's Security & Technology Solutions (STS) practice is part of the firm's global Technology and Security Risk Services group, which is comprised of more than 2,000 professionals with world-class capabilities in minimizing risk and maximizing the security and controls of IT systems. Ernst & Young assesses, designs, implements, and operates independent security solutions that help enable businesses to achieve their critical business goals. The practice is comprised of security and risk professionals drawn from Fortune 500 companies, the federal government and various military agencies, including the National Security Agency, the U.S. Air Force and the U.S. Navy. Further information on Ernst & Young's security practice can be found at ey.com/security.



Guardent, headquartered in Waltham, Mass, is one of the largest, privately held, managed security service providers. Guardent combines managed security services with vendor independent consulting to provide better information security at a lower operational cost than can be achieved through an organization's internal staff. The company's flagship offering, Guardent Managed Security ServicesSM, is based upon an open service delivery platform that makes it possible to deploy any combination of commercial or open source security technologies, including NetScreen, Check Point, Cisco, ISS, IP Tables, Snort and Nessus.



Oracle Corporation (Nasdaq: ORCL) is the world's largest enterprise software company, providing enterprise software to the world's largest and most successful businesses. With annual revenues of more than \$10.8 billion, the company offers its database, tools and application products, along with related consulting, education, and support services. Headquartered in Redwood Shores, Calif, Oracle is the first software company to develop and deploy 100 percent Internet-enabled enterprise software across its entire product line: database, server, enterprise business applications, and application development, and decision support tools. For more information about Oracle visit our website at oracle.com.



Platinum

BMC Software. With user information spread across various data stores such as applications and operating systems, securely and efficiently managing today's IT environment is a nightmare. BMC Software's CONTROL-SA manages your disparate environment through a single console, dramatically reducing your security administration costs while enhancing your security. CONTROL-SA's open architecture is foundational for your future identity management initiatives.

IBM is the world's largest information technology company, with more than 80 years of leadership in business innovation. IBM offers a wide range of research technology, encryption hardware, platform security, Internet applications, security management, and consulting services enabling customers to take full advantage of the new era of secure e-business. Visit ibm.com/security.

KPMG LLP is the accounting and tax firm that has maintained a continuous commitment throughout its history to providing leadership, integrity and quality to the capital markets. The Big Four firm with the strongest growth record over the past decade, KPMG offers clients the scale, global reach, industry insights, and multidisciplinary range of services they demand. Our highly skilled Information Risk Management professionals help clients maintain control of their business, while minimizing systems-related risk. They have the knowledge and experience to help organizations maintain security, reliability and availability of

crucial technology systems — while maintaining appropriate controls and growing their business.

MessageLabs is a leading international Managed Services Provider (MSP) specializing in managed email security services. Its revolutionary portfolio of services enables customers to be protected from threats such as viruses, unsolicited mail, and pornography, which are all intercepted before they reach the customers' network boundaries. For further information, go to messagelabs.com, or email: info@messagelabs.com

Microsoft. Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software — any time, any place and on any device. microsoft.com

NetContinuum is the leading provider of all-in-one web security gateways — enterprise-class web security appliances designed to secure applications and protect against Web attacks. Founded in 1999, NetContinuum is funded by blue-chip venture capital firms and investors. For more information, please visit netcontinuum.com or call 408 961 5600.

Oblix Inc. is a leading developer of identity-based security solutions for e-business networks. The company's flagship product, Oblix NetPoint, is an enterprise identity management and Web access control solution that

provides an identity infrastructure for an entire e-business environment. Based on a Web services architecture, Oblix NetPoint includes rich identity management functionality and provides access control with single sign-on to enterprise applications. This combination significantly lowers IT costs for organizations conducting business on the Web.

PricewaterhouseCoopers' Security & Privacy Practice is the world's leading provider of security and privacy solutions to Global 2000 organizations. Our Enterprise Security Business Model[®] is the industry's first comprehensive guide to help organizations identify, create, capture and sustain the value of security. Through this innovative framework, companies can leverage security to gain competitive advantage. PricewaterhouseCoopers is an acknowledged industry leader in the areas of security strategy, privacy, Identity Management, threat and vulnerability management, and incident response. pwcglobal.com/security or 1 800 639 7576

RSA Security Inc. With thousands of customers around the globe, RSA Security (NASDAQ: RSAS) provides interoperable solutions for establishing online identities, access rights and privileges for people, applications and devices. Built to work seamlessly and transparently in the complex environments of thousands of customers, the Company's comprehensive portfolio of identity and access management solutions - including authentication, Web

access management and developer solutions - is designed to allow customers to confidently exploit new technologies for competitive advantage. RSA Security's strong reputation is built on its history of ingenuity and leadership, proven technologies and long-standing relationships with more than 1,000 technology partners.

SilentRunner is the market leader in a new generation of network security and forensic analysis products that cost-effectively solve the challenges involved in uncovering, analyzing and investigating the theft, misuse and abuse of corporate information resources and meeting new information assurance regulations.

TruSecure is the leading Managed Security Services Provider (MSSP), offering the only fully integrated, enterprise risk management services on the market. TruSecure's unique blend of proactive risk reduction with real-time security management, monitoring and response assures continuous security of critical business information assets.

Waveset, a leading provider of identity management solutions, enables the real-time enterprise with an integrated suite of management applications that improve enterprise security while maximizing the efficiencies of critical business and IT processes. With a proven ROI track record for Fortune 500 organizations, Waveset delivers real business value through innovative solutions that give you a competitive advantage.



Premier

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce network operating costs. The comprehensive security offering from Cisco combines a management framework, hardware devices, identity services, software functionalities, and applications into a single, secure infrastructure. The integration of this wide range of security technologies into all Cisco products along with world-class service, support, and training, allows security for voice, video, and data to be embedded throughout the network for small businesses, large organizations, and service providers. cisco.com



Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to enterprises, individuals and service providers. The company is a leading provider of client, gateway and server security solutions for virus protection, firewall and virtual private network, vulnerability management, intrusion detection, Internet content and e-mail filtering and remote management technologies as well as security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries. For more information, please visit symantec.com



Unisys Corporation Threats to the security of your operations. It's not a question of "if" there are gaps, but a matter of "where." Unisys helps you identify the gaps in your security plans and procedures.

Our full set of security solutions do more than protect your network, they protect your entire business. The Unisys Zero-Gap Security PlanningSM approach holistically addresses security in five risk areas: Identity, Privacy, Collaboration, IT Infrastructure Protection and Business Continuity. What makes Zero-Gap Security Planning unique is that it addresses these five risk areas across an organization's four security segments: physical, operational, financial and cyber. unisys.com/services/security



Platinum

Avaya Inc. designs, builds and manages communications networks for more than 1 million businesses worldwide, including 90 percent of the FORTUNE 500®. Focused on businesses large to small, Avaya is a world leader in secure and reliable Internet Protocol (IP) telephony systems and communications software applications and services. For more information visit the Avaya website: avaya.com.

Computer Associates is a worldwide leader in security with its eTrust security solutions and delivers to global organizations including 99% of Fortune 500. Its eTrust brand provides comprehensive enterprise security management, and delivers a holistic view of the security infrastructure.

Network Associates, Inc. is a leading supplier of network security and availability solutions. Network Associates is comprised of three product groups: McAfee Security, delivering world-class anti-virus and security products; Sniffer Technologies, a leader in network availability and system security; and Magic Solutions, a leader in innovative service management solutions.

QinetiQ Trusted Information Management, Inc. For over fifty years, QinetiQ has delivered innovative security solutions, research, and technology to international organizations. Specialty areas include: global threat analysis; corporate governance; security governance; forensics; education; research and development; managed services; and attack resistance/prevention. QinetiQ's comprehensive, proactive security solutions enable organizations to reduce the "risk" in "risk management".

Sun Microsystems. Since its inception in 1982, a singular vision — "The Network Is The Computer™" — has propelled Sun Microsystems, Inc. (Nasdaq: SUNW) to its position as a leading provider of industrial-strength hardware, software and services that make the Net work. Sun can be found in more than 170 countries and on the World Wide Web at sun.com.

VeriSign, Inc. (Nasdaq: VRSN), is the world's largest and industry leader provider of Internet trust services, supporting government, business, and consumer e-commerce activities. VeriSign offers a wide range of solutions in areas such as e-authentication, access management, PKI, validation, payment and domain names registration services to enable everyone, everywhere, to use the Internet with confidence.



SECTOR 5 Sponsors

IT Security Summit Business Suite Sponsors

Blockade Systems

Bluefire Security Technologies

Business Layers

Clearswift

Configuresoft

Courion Corporation

Credant Technologies

Decru

Entercept Security Technologies

e-Security

Foundstone

GuardedNet

Intellitactics

Internet Security Systems

IntruVert

Lancope

Mphasis

M-Tech

nCircle Network Security

Neoteris

Netegrity

NetIQ

NetScreen

Network Intelligence

NFR Security

Nokia

Northrop Grumman

OpenService

Qualys

Radware

Sanctum Inc.

SecureWave

Security

Sourcefire

SPI Dynamics

Stratum8 Networks

Symark Software

Trend Micro

Tripwire

Media Partners



