Tivoli® SecureWay Risk Manager
Frequently Asked Questions (FAQ)

Questions about Products / Product Line

1) What is Tivoli SecureWay Risk Manager?

Tivoli SecureWay Risk Manager is a new security offering from the Security business unit. Tivoli SecureWay Risk Manager is an e-business security management solution that enables customers to quickly manage threats, such as denial-of-service attacks and other forms of intrusions, across the enterprise. Tivoli SecureWay Risk Manager R1 will become generally available in early Q2 2000.

2) How does Tivoli SecureWay Risk Manger address the complexity of the Internet environment, with the various users, systems and applications?

Managing security in the Internet environment requires the deployment of several point product solutions such as intrusion detectors, scanning tools, Web authentication and access control, solutions. Each of these point products solve a particular problem, are often too complex to administer, are extremely time consuming and require dedicated skilled personnel. Without an integrated security management, it becomes easy of attackers to exploit vulnerabilities in any of these point solutions to render the other point product defenses useless. An integrated security solution is most effective when the firewalls, intrusion detection agents, network security and application security solutions can work together in a coordinated fashion to minimize threats. Tivoli SecureWay Risk Manager addresses this complexity by providing the overall "big picture" view of the security by integrating and managing security events across the different types of security defenses employed within the enterprise.

3) Customers have already deployed Firewalls or Intrusion Detection Systems to manage hacker attacks? Why do they need Risk Manager?

Customers have made significant investments in many point products such as firewalls, intrusion detection systems and application-level security mainly because each point product is best suited to implements a specific security function that is required to implement the overall security strategy. However security is more than firewall or other point product solution. Security is a link with each point product implementing a component of the link. Each component of the security link such as firewalls or intrusion detection systems or application security mechanisms reinforce or complement each other. The overall security is only as good as the weakest link. An integrated security management product such as Risk Manager enables customers to make the most informed security decisions by leveraging the intelligence of the various security links. By centrally correlating intrusions and vulnerabilities across these different components, Risk Manager provides the overall assurance that individual security component reinforce and complement each other and implement the overall business goal of managing risk against information assets.

4) What are the product components in Risk Manager?

Risk Manager includes the following components:

- Pre-Adapter for the RealSecure Network Intrusion Detection System from Internet Security Systems (ISS). The pre-adapter is configured to work with the RealSecure Agent from ISS.
- Pre-Adapter for the Cisco Secure IDS (formerly NetRanger) from Cisco Systems. The pre-adapter is configured to work with the Secure IDS Agent from Cisco.
- New Web Intrusion Detection System (Web IDS). Web IDS is a complete Intrusion Detection System designed for Denial of Service and other forms of Web attacks. Web IDS can be supported on any Web Server but has been explicitly tested and supported on Microsoft IIS, iPlanet Web Server (Netscape Enterprise Server) and Apache Web server

- A set of correlation rules for the pre-adapters and Web IDS. The correlation rules are installed on the Tivoli Enterprise Console (TEC) Server.

5) Are there any pre-requisites for Risk Manager?

Yes. Risk Manager pre-requires the TEC.

6) Does Risk Manager support Firewalls?

Risk Manager does not support any correlation for Firewalls in Release 1. However, Risk Manager leverages TEC as the central console for displaying and reporting alert information. Checkpoint has developed a Tivoli Plus module that enables alert information from Firewall-1 to be sent to the TEC. So, although we do not correlate firewall alerts, the customer still can view Risk Manager and Firewall events on a single console. Tivoli Plus modules are also available for Axent (ESM, ITA) and Symantec Norton Virus that directly send alerts to the TEC. Correlation of these products will be addressed in Release 2.

7) Does Risk Manager include HAXOR?

Risk Manger does not include HAXOR. HAXOR is an intrusion detection system developed by IBM Research.

8) Does Risk Manager support Cross-Site Security?

Cross-Site for Security is an intrusion detection system that is based on HAXOR. Risk Manager will support Cross-Site for security as an intrusion detection system to correlate alerts from. Risk Manager however will not include Cross-Site Security and Cross-Site has to be purchased separately.

9) Who does Risk Manager compete with?

There is not a whole of competition in this space. eSecurity is one vendor who seem to have centralized management of point products. However eSecurity seems to be focused more on centralized alert reporting rather than any serious correlation of alerts across the different point products.

Vendors such as Axent and ISS are trying to re-position themselves as security management players.

10) What correlation is Risk Manager providing that can't already be done by the IDS's native console? It is my understanding that this is a basic function in any decent IDS already.

Risk Manager provides centralized correlation of alerts and intrusions across distributed IDS sensors and Web IDS. This is fundamentally very different that the correlation capability within the IDS native console. The correlation capability within the native IDS is limited to a historical context in which if the console sees two alerts with identical information (for example, same destination IP) then it flags the console entry differently,

The correlation capability in Risk Manager is vastly different. Network intrusion detection systems work by sniffing the packets on the wire and comparing them to known set of signatures. They do not have any idea if the attack in question really succeeded or not or for that matter even reached the intended target. Web IDS on the other hand is an application-level IDS since it is designed to support Web server attacks. Web IDS knows whether the attack succeeded or not (it does not prevent the attack) and therefore has state information of the attack. The correlation rules take advantage of the state information to present a concise picture of the attack using a single alert with the appropriate severity level. Being able to use state-full alerts from Web IDS in conjunction with alerts from the network IDSes is by itself a clear differentiator in functionality. Other correlation rules are described below.

11) What kind of Correlation do we support in Risk Manager and how does this relate to attacks?

Risk Manager supports two levels of correlation:

- Correlation that is based on common IP and TCP information such as Source IP Address, Source Port, Destination IP Address, Destination Port and the attack signature. This type of common information is available as part of any attack and provides a base-level correlation across the different intrusion detection systems and Web IDS. This type of correlation enables us to identify attacks of the following types
  - A single attack host is systematically attacking many internal hosts within an enterprise
  - Many attack hosts are participating in attacks that may target a single host such as the company's Web server
  - A single host that is scanning or probing for vulnerabilities on a given machine
  - The same attack being targeted on different target machines
- Correlation that is specific to the attack and utilizes attack specific information within the rules.
  - Based on attack specific information the correlation rules enable the console to eliminate alerts from multiple sensors that have not succeeded. This helps in greatly reducing the number of false positives
  - Conditionally upgrade or downgrade the severity of the attack by using inputs from multiple sensors. For example, the Web intrusion detection system would be able to detect Web attacks more precisely than a general purpose network based intrusion detection system. Such information is taken into account by the Risk Manager correlation engine.

12) What correlation is Risk Manager providing that can't already be done by TEC? TEC has been correlating alarms from various sources for years. Why do we need a separate correlation in RM in addition?

Risk Manager does NOT have a separate correlation engine. It uses the prolog rules engine with the TEC to implement its correlation just other Tivoli products do. We have simply added a set of rules and facts for each supported end point within Risk Manager (ISS RealSecure, Cisco Secure IDS and Web IDS) in separate baroc files that installed on the TEC.

13) It is my understanding that Risk Manager R1 will support NetRanger, RealSecure, and IBM's WebWatcher. What is the planned rollout for support of other IDS's such as CrossSite for Security (Haxor), Axent's NetProwler and Intruder Alert, NFR's Network Flight Recorder, NAI's Cybercop, Security Dynamics' Kane Security Monitor, and Tripwire?

There are plans to support Cross-Site for security in a refresh release after Release 1. We are looking at supporting Axent's NetProwler and ITA in Release 2. Axent, today can already send their alerts to the TEC using the Axent Tivoli Plus module. There are no plans to support of yet to support the other products. We are looking at ways to encourage and enable vendors to forward their alerts to TEC in a standardized format that would enable Risk Manager to provide base level of correlation. If you have specific suggestions on these products

14) When will Risk Manager be added to the Tivoli Foundation Demo (or some similar standalone demo package)?

We are currently working on demo capability (at least a screen cam demo for the short-term)

15) What actual "risk management" functions does Risk Manager do? From what I can tell, it does IDS alarm correlation and reporting. This is not "risk management" in the way that the term is widely understood in the IT security industry (which is closely related to risk analysis).

First of all, to manage risk requires a clear understand of what the risk is and where the risk is coming from before you implement risk management techniques. With Release 1, Risk Manager provides a better management tool that enables the security analyst to get a better handle on what things are happening. Since Risk Manager is based on TEC, we can leverage the TEC's capabilities for actions in response to certain alarms. These actions are specific to the customer environment and needs to be developed by the customer or obtained through services as these actions could have unintended consequences. For example

an analyst may want to change the firewall filter to deny access to a certain port from a certain source address.

With Release 2 we would address the need to provide a risk management response on things or actions an analyst can initiate to mitigate the risk. We need to understand how customers are using this tool to have built-in capability to support risk management actions.

16) What platforms will RM run on initially? Future platforms?

Risk Manager pre-adapter for ISS RealSecure : Windows NT 4.0

Risk Manager pre-adapter for Cisco Secure IDS: Solaris 2.7

Risk Manager Web Intrusion Detection System:
Apache: 3.1.12 (AIX/NT) 3.1.9 (Solaris); Netscape ES 4.1 (Solaris/NT) 4.0 (AIX); Microsoft IIS 4.0

Platforms: Windows NT 4.0 SP5, Solaris 2.7, AIX 4.3.3

Future platform support would include support for Linux

17) What mechanism is used to communicate between Risk Manager and downstream IDS? Between Risk Manager and TEC? Is this a proprietary protocol or open? Is the traffic encrypted, authenticated, etc.?

Architecturally, Risk Manager pre-adapters source their alerts from the IDS database (which is installed on the third-party IDS console.). The IDS database has the aggregated alerts from all of the IDS sensors that have been deployed (Risk Manager does not interfere with the communications between the third-party IDS sensor and the third-party IDS console). The pre-adapters take the alert data and send it to the TEC using the capabilities of the LogFile Adapter. The communications between the LogFile Adapter and the TEC is mutually authenticated using security services of the framework.

18) What is the basis for determining that alarms are related? Is there some sort of expert system technology or is it strictly based on customer-defined rules?

The correlation rules and the fact base were derived from the work done by IBM Zurich. It is not based on customer defined rules.

19) Does Risk Mgr scan the packets in the LAN? like a Sniffer? I thought not, but looking at the announcement it looks like it does. I thought it was a manager for scanning tools. If it does not scan packets in the LAN, what is Haxor used for?

Risk Manager does not include native network functionality. This is the job of ISS or Cisco Secure IDS. Risk Manager DOES include a native Web IDS capability. Similar to how network IDS sniffs network traffic, the Web IDS parses Web Server log files in real-time and maintains has an exhaustive list of Web attack signatures. Please refer to the question on HAXOR.

20) When will Risk Manager be available?

Release 1 will be available May 31st 2000.

21) Do we have a list of scanning tools managed by Risk Manager?

Risk Manager does not support any scanning tools in Release 1.

22) How is Risk Manager priced?

Risk Manager is based on a Managed Server pricing model. Under this model, Risk Manager is priced as following:

Tier 1 Servers: 140 points; Tier 2 Servers: 280 points; Tier 3 Servers: 2800

Example:

A customer decides to deploy Risk Manager to secure the customer's extranet. The customer has 4 IDS agents on Tier 1 servers and 6 Web servers deployed on Tier 2 servers. (Note that the Risk Manager pre-adapter is installed only the console/database machine, not on the individual sensors. The console database has the aggregated alerts from the 4 different IDSes and so the value pricing model accounts for this as 4 managed servers.)

4 IDS agents on Tier 1 servers count as 4 Managed servers:	4 X 140 =	560
6 Web Servers on Tier 2 servers count as 6 Managed Servers	6 X 280 =	1680
Total Points:		2240