



## Company and Market Backgrounder

**“In the Internet Era, firewalls seem increasingly permeable. And businesses would do well to look at ways to watch and control more rigorously what's happening inside the perimeter rather than put their stock in blocking out barbarians with a firewall.”**

"Cracks in the Firewall," *Business Week*, April 9, 2002  
© 2002 The McGraw-Hill Companies, Inc.

eSecurityOnline LLC, an Ernst & Young security software company, is a leading provider of risk management solutions that enable companies to proactively protect their IT assets from external attacks and other security threats. eSO arms CIOs and security executives with the knowledge and tools they need to assess and track the success of their company's security efforts, while communicating security hazards throughout an organization.

As companies elevate security into a core element of corporate strategy, eSO empowers them with an automated and cost-effective operational approach to protecting corporate assets and networks. eSO's patented vulnerability management solutions save companies thousands of hours every year by correlating automated discovery, inventory and assessment processes with an extensive and continuously updated database of verified threats and proven fixes.

**History.** eSecurityOnline was established in July 1999 as an IT security portal for clients of Ernst & Young's global security practice. The portal allowed companies to subscribe to an online vulnerability service that tapped Ernst & Young's database of more than 2,000 verified vulnerabilities.



But as the market for vulnerability management solutions evolved,

so did eSO. In June 2000, the company launched its portal solution to the corporate IT market at large and added a knowledge base of best practices for configuring computer systems, networking devices, firewalls, operating systems and applications. The move made it possible for any company – not just Ernst & Young clients -- to subscribe to eSO's services.

In September 2000, Robin Hutchinson joined the company as CEO. Hutchinson, a veteran of Ernst & Young's eRisk solutions practice, oversaw the company's February 2001 spin-off as a wholly owned subsidiary of Ernst & Young. He also set to work realigning the company's direction beyond its portal focus and driving eSO's efforts to develop eSO Framework™, a multilayered risk management tool that helps companies to develop a comprehensive corporate security posture. The company launched Framework as a hosted solution in August of 2001. Now in its 4.0 release, Framework is popular with major corporations and industry leaders in the financial, telecommunications, entertainment, insurance, health care, chemical and utility industries.



Robin Hutchinson

While rapidly evolving the Framework ASP solution, the eSO management team began working to address increasing market demand for a vulnerability management solution that could be hosted on a company's network. The team recognized that IT managers were caught between conflicting agendas: the increasing need to protect corporate networks from hackers and other threats, and mounting pressure to minimize IT costs. To address these needs, eSO introduced eSO Advisor™, a turnkey appliance launched in October 2002 that brings key features of eSO's popular Framework hosted solution to a scalable and easily deployed package designed to operate behind the firewall.

eSO retains a close and collaborative relationship with Ernst & Young. With its global network of more than 2,400 security practitioners, Ernst & Young is recognized as one of the world's leading innovators in the fields of information security and knowledge management. Security Subject Matter Specialists at Ernst & Young work jointly with eSO security professionals to customize the implementation of Framework or develop specialized content. Working with eSO, Ernst & Young utilizes Framework as a tool for IT risk management while eSO leverages Ernst & Young's capabilities to assist in the evolution of its products. eSO also leverages its vulnerability knowledge base for both its Framework and eSO Advisor solutions.

With more than 60 employees, eSO is headquartered in Kansas City.

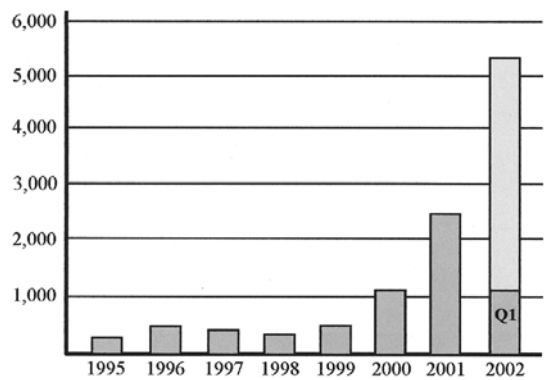
### The Growing Need to Manage IT Vulnerability.

Corporate CIOs worry more about IT security than any other work-related issue<sup>1</sup>. And with good reason. The number of known vulnerabilities to hackers and other IT threats is growing significantly faster than the average company's ability to patch them. Reported IT vulnerabilities more than doubled in 2001 (see chart at right), and analysts see no signs of slowing.<sup>2</sup>

The problem isn't going away. An estimated 19 million people are believed to possess the skills required to

### Vulnerabilities Are On the Rise

(Number of reported security-related vulnerabilities)



Source: CERT Coordination Center and JP Morgan estimates

<sup>1</sup> Morgan Stanley CIO Survey Series: Release 3.5, Charles Phillips and Ryan Rathman; July 11, 2002

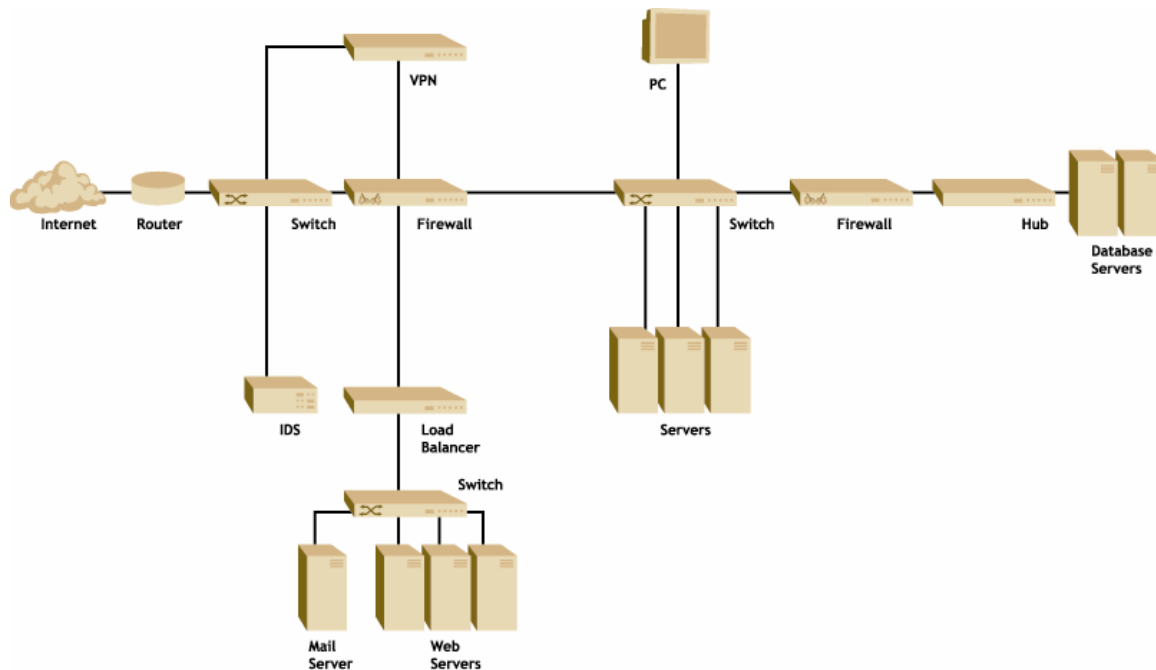
<sup>2</sup> IT Security Industry, *The Weekly Hack*, Issue 84, June 17, 2002, JP Morgan Securities, Inc. Equity Research, P. Sterling Auty II, CFA

engage in malicious hacking<sup>3</sup>. This, too, is a number that is likely to grow as vulnerabilities mount and the knowledge to exploit them spreads throughout the world.

Many analysts believe that coordinated hacker attacks represent the next substantial IT security threat. The worst-case scenarios are nightmarish — a determined coalition of hackers could disrupt 911 service, air traffic control, the power-switching centers that move electricity around the country, rail networks and more.<sup>4</sup> It requires minimal effort to imagine the potential ripple effect on U.S. commerce, which itself was an obvious if indirect target of the terrorist attacks on Sept. 11, 2001.

In addition to these external attacks, internal threats, already on the rise, will become even more problematic in the future. History indicates that some 70 percent of all security incidents originate from internal sources. Yet not every threat involves a concerted effort by employees acting out of malice: Even simple carelessness and a lack of stringent security policies can cost companies untold sums in intellectual property thefts, illegal use of IT resources, hidden “logic bombs” designed to destroy important data, productivity dips and damage to assets. In our precarious environment of downsizing, security control efforts are more important than ever.

The answer isn’t simple, particularly since the corporate firewall isn’t the only point on a company’s network that must be protected. As the diagram below illustrates, vulnerability points exist throughout an organization, and perimeters can be secured around any number of IT assets or categories of IT risk, spanning technology, procedural, and human factors. Technology risks include software flaws and a lack of configuration standards that, when properly implemented, establish policies aimed at protecting IT assets. Procedural vulnerabilities can relate to deployment of security information, tracking of work completion, and auditing of compliance. The human factor, so often overlooked, is just as crucial: IT teams must be knowledgeable about what they need to secure, and how to secure it.



<sup>3</sup> President’s Commission on Critical Infrastructure Protection

<sup>4</sup> Tom Marsh, Chairman, President’s Commission on Critical Infrastructure Protection, September 2001.

For those IT organizations that lack an effective security posture, the costs can be surprising. Among large enterprises, the fully loaded costs of applying a software patch can actually exceed \$1 million.<sup>5</sup> While not all patches are security-related, even a few deployed annually throughout large organizations can result in massive expenditures. Many already understaffed IT departments devote hours every day to surfing the Web and sifting through thousands of vulnerability warnings to try to identify which specific vulnerabilities apply to their assets. These inefficient approaches to managing vulnerability literally bleed resources from an organization, while boosting the cost of owning and maintaining IT assets.

**The Push for Homeland Security.** The problem hasn't gone unnoticed at the federal level. In July 2002, a group of federal agencies and industry organizations released Consensus Baseline Security Settings for systems using Microsoft Corp. Windows 2000. While they are intended to serve as recommendations, some view the move as the first step toward governmental regulation of security standards. The guidelines were developed jointly by the President's Critical Infrastructure Protection Board, the Center for Internet Security, the National Security Agency, the General Services Administration, the National Institute of Standards and Technology, the Defense Information Systems Agency, and the SANS Institute. At the same time, the group released a small vulnerability scanner to check each machine's settings. Most government agencies reported that they plan to implement them and expect their private-sector contractors to follow suit. The release of a vulnerability scanner reflects the group's conclusion that IT security must move away from a threat paradigm toward a vulnerability paradigm.

This is just the beginning. Government efforts to protect cyberspace will be ongoing, and Congress has had to grapple with the difficult task of establishing policy and law that would apply to the country as a whole. To create policy that is inclusive of every type of company – from global organizations with vast US networks and VPNs to small, budget-limited companies that still must protect their patch of cyberspace from security threats – Congress has tried to cast a broad net across multiple factions capable of providing input. Chief among IT concerns is the extent to which companies are willing to share sensitive data so that Congress can craft meaningful security law. And because, by its very nature, lawmaking is a political process, how loud a voice can small- to mid-sized companies expect to have?

It's obvious that companies interested in securing their IT assets may take unnecessary risks by waiting for the government to take action. This is particularly true for smaller companies whose needs may not be sufficiently met by federal policy and legislation. And, in the end, no matter what the government does, IT groups will have to deploy solutions that are available commercially or developed in house. In the short term, government action will do little to change that reality.

**Sizing the Opportunity: The Explosive Growth of Security 3A Software.** With the explosion of proven risks has emerged an industry devoted to combating them. And as IT security moves from a necessary cost center to a core element of corporate strategy – some 80 percent of CEOs recognize security's strategic importance<sup>6</sup> – companies are preparing to commit record expenditure amounts toward risk management solutions.

Recent analyst estimates bear this out: The overall market for IT security will increase from \$14 billion in 2000 to more than \$46 billion in 2005. This represents a compound annual growth rate (CAGR) of 27

---

<sup>5</sup> *IT Security Industry, The Weekly Hack*, Issue 84, June 17, 2002, JP Morgan Securities, Inc. Equity Research, P. Sterling Auty II, CFA

<sup>6</sup> *Morgan Stanley CIO Survey Series: Release 3.5*: Charles Phillips and Ryan Rathman, July 11, 2002

percent – healthy by any measure but dramatic compared to current industry-wide technology growth estimates.<sup>7</sup>

A key driver of this growth is Security 3A (administration, authorization, and authentication) software. Corporations use Security 3A software to manage security within an enterprise, including the tasks of defining security parameters and auditing results. Worldwide revenue for Security 3A software reached \$2.2 billion in 2001, representing 10 percent growth over 2000. IDC forecasts that the Security 3A software market will increase at a 22 percent compound annual growth rate (CAGR) to reach \$6 billion in 2006.<sup>8</sup>

Across all market segments, financial services and infrastructure companies (such as telecommunications providers) claim the lion's share of security software purchases. Recent data shows that the primary reason for security-related investment by companies across industries is to provide increased network access. With downsizing rampant, the ability to instantaneously activate and terminate employee access to network resources, data, and information has become a fundamental requirement. Vast differences in company size and makeup also have an impact on the security solutions they choose. Small companies usually need to protect only a few critical segmented systems. Midsize companies with some distributed systems, linked WANs, integrated enterprise systems, and interactive Web sites attract more visibility and attention, and thus require significant security upgrades to counter a proportional increase in IT risks. Large enterprises with major ecommerce, online sales, and supply chain operations require the most comprehensive security protection to avoid catastrophic system intrusion, compromise, and damage.<sup>9</sup>

**Options for IT Management.** So what can companies do to protect their infrastructures? IT groups need to measure their current and future state of effectiveness against a model that will guide them to a mature vulnerability management process. While recent events have spawned more interest in security, the fundamentals have not changed. People, process and technology are the key areas that must be addressed through good knowledge, effective and efficient deployment, and accountability. It is not enough for a company to merely acknowledge the need for security; rather, it must establish a plan to ensure it can fix vulnerabilities on host systems before they cause pain, while efficiently deploying policy to the people that govern them, and maintaining an accountable process for deployment, testing and repeatability.

But do today's products meet those needs? Point solutions – those designed to handle one or two specific tasks, such as scanning or managing the application of patches – are growing in popularity as companies try to piece together products that will help them establish a comprehensive security posture. But by their very nature, these tools focus solely on limited areas of the security spectrum, and thus require IT security executives to undertake the unenviable task of integrating a variety of point solutions.

Analysts have recognized the shortcomings of this approach. Identifying patch management solutions as a key growth area in the Security 3A software space, JP Morgan Securities analyst P. Sterling Auty writes: “The increasing demand for a patch management solution is great, but we believe it needs to be

---

<sup>7</sup> *The Big Picture: IT Security Software, Hardware, and Services Forecast and Analysis, 2001–2005*: IDC, Brian Burke, Charles Kolodgy, Chris Christiansen, Richard Dean, Allan Carey, and Jason Smolek, December 2001 (IDC Doc. #26311)

<sup>8</sup> *IDC Worldwide Security 3A Software Market Forecast and Analysis, 2002–2006*: IDC, Brian Burke, Chris Christiansen, and Charles Kolodgy, July 2002 (IDC Vendor Views Doc. #27572)

<sup>9</sup> *Internet Security Software Spending Opportunity by Vertical Market, 2000–2005*: IDC, Chris Christiansen, Brian Burke, Charles Kolodgy, and Anna Toncheva, Oct. 2001 (IDC Doc. #25797)

part of a broader solution set; in other words, we view it as a product within a larger product line rather than a product that could sustain a stand-alone solution provider.”<sup>10</sup>

IDC recognizes a similar need; indeed, the research firm predicts that single-point appliances will be most prevalent in lower ends of the IT market until a new class of security appliance is made available for small- and medium-sized businesses. That appliance will result from the convergence of firewall/VPN security appliances with intrusion detection, content security, and policy management capabilities.<sup>11</sup> IDC expects vigorous growth for security appliances that combine hardware and software to administer the overall task of managing IT vulnerability. The market for security appliances alone is expected to swell by 27 percent annually from 2000 to 2005.<sup>12</sup>

This is great news for companies who today face the many headaches associated with collecting and implementing multiple point solutions. A recent survey of CIOs found that IT executives are increasingly drawn to integrated solutions: Sixty percent of CIOs surveyed report they are consolidating the number of technology suppliers to their companies. Of those, more than half (57 percent) prefer the simplicity of dealing with fewer vendors, specifically citing the technological complexity of integrating solutions from multiple vendors. And then there is the issue of the financial health of those companies that supply point solutions, which typically are launched by venture capital-backed start-ups. The same CIO survey found that more than half of the IT executives questioned say their companies are more closely scrutinizing the financial stability of their suppliers – something not likely to change in the current business environment.<sup>13</sup>

**The eSO Option.** Early in its history, eSecurityOnline recognized the need to integrate crucial risk management tools and knowledge into solutions that allow companies to design, implement and monitor a comprehensive corporate security posture. Over time, that philosophy has fueled the development of an entire line of eSO risk management solutions: the ASP-delivery of Framework™, and the turnkey appliance delivery of eSO Advisor™. In all of its offerings, eSO leverages extensive Ernst & Young vulnerability data and configuration standards. Only eSO products employ constantly updated security knowledge aggregated and verified by more than 2,400 Ernst & Young security specialists.

eSO solutions are modeled on the Vulnerability Management Maturity Model (VM<sup>3</sup>). VM<sup>3</sup> is based on helping companies understand how they deal with knowledge, deployment and accountability challenges related to securing their IT environments. It defines three levels of growth and provides a company with the means to evaluate where they stand. Companies can develop a more mature security posture by mastering these three key aspects of IT security:

- **Knowledge:** Because security threats change hourly, the availability of constantly updated information is an important driver of success for IT security efforts. Yet most companies today surf the Internet or subscribe to services that deliver unfiltered and unverified vulnerability reports and virus alerts. Useful security knowledge must be delivered in a way that can be

---

<sup>10</sup> *IT Security Industry, The Weekly Hack*, Issue 84, June 17, 2002, JP Morgan Securities, Inc. Equity Research, P. Sterling Auty II, CFA

<sup>11</sup> *The Big Picture: IT Security Software, Hardware, and Services Forecast and Analysis, 2001–2005*: IDC, Brian Burke, Charles Kolodgy, Chris Christiansen, Richard Dean, Allan Carey, and Jason Smolek, December 2001 (IDC Doc. #26311)

<sup>12</sup> *Return of the Black Box: Firewall/VPN Security Appliances Unleashed*: IDC, Chris Christiansen, Nora Freedman, and Charles Kolodgy, June 2001 (IDC Doc. #24797)

<sup>13</sup> *Morgan Stanley CIO Survey Series: Release 3.5*: Charles Phillips and Ryan Rathman, July 11, 2002

deployed throughout an enterprise. And most valuable of all is information that is specifically relevant to a company's own IT assets.

- **Deployment.** Developing good security knowledge is a great starting point for limiting risks exposed by misconfiguration of systems, the existence of inappropriate code, or the absence of policies that govern people and their behavior. However, without a responsive, repeatable deployment process, good becomes obsolete. Using a tool that is built to interact with a knowledge management database and assign asset specific tasks is the next step. If companies have this tool, they address the process and have a mechanism to understand where gaps occur in their battle against threats. They will be able to extend the scope of their security coverage beyond the systems that protect them, while extending the knowledge to IT administrators who configure and manage the serving systems.
- **Accountability.** The ability to track what changes have been made to computer systems and determine if an employee has read and acknowledged a policy is step one in the accountability stage. Step two is extending governance to include an entire critical infrastructure, made possible by the feasibility of an automated engine. Lastly, companies must measure compliance to the process by conducting reviews of actual systems to ensure a correlation of the discovery process with the actual record of inventory, as recorded in a tool. The old adage of "test first and then fix" is being replaced with "fix first and then test." It uses testing as a means of accountability and assurance.



© Copyright 2001 and 2002 eSecurityOnline LLC

### eSO Framework™

eSO Framework™ is a multi-layered risk management tool for enterprise customers. Each layer defines the people and processes necessary to manage an expanding scope of control over critical infrastructure. Provided to customers as a managed service via a classic ASP model, the key components of eSO Framework are built around the company's VM<sup>3</sup> methodology.

eSO Framework *Knowledge Components* include:

- **Knowledge.** Framework simplifies the process of creating and maintaining policies. Companies can choose to either import current organizational standards or customize template policies and procedures based on Ernst & Young's best practices and regulatory guidelines. Policies can also be defined for, and viewed by, specific business units, IT assets or risk groupings. This component also allows users to search, view and edit policies according to granted access privileges. Furthermore, eSO Framework delivers security policies throughout the enterprise for security awareness training by giving employees content that is specific to their role.
- **Configuration Standards.** Configurations are continuously monitored and confirmed by Ernst & Young. These configuration standards constitute one segment of the E&Y/eSO knowledge base. Each baseline standard describes the risk of not implementing the controls, along with step-by-step audit and implementation procedures enabling consistent deployment of systems throughout the enterprise. These configurations are also classified by risk through confidentiality, integrity and availability, allowing organizations to apply the correct standards to a specific IT asset. Baseline configuration standards are further expanded by sets of specific configuration standards relevant to intended use—these additional configuration standards address specific recommendations for web servers, mail servers, database/file/application servers, remote access servers, security servers/devices, and workstations.
- **Vulnerabilities.** A vulnerability management process is powered by an eSO Research Team that monitors, validates and tracks a growing knowledge base of thousands of vulnerabilities and associated fixes. By tracking vulnerabilities through technologies and service pack levels, eSO Framework provides granular information and alerts specific to an organization's environment.

eSO Framework *Deployment Components* include:

- **Workflow.** To mitigate IT risks across an enterprise, an organization and its management must be able to assign and track the completion of defined tasks. eSO Framework allows companies to complete this by building tailored workflow processes. Management also is able to view workloads across the enterprise, while providing daily task lists to those responsible for mitigating risk. When tasks are completed, employees update the implementation status, progress notes and compliance to produce a record of actions taken. Customizable reports keep management apprised of the overall risk posture of the organization's IT assets.

eSO Framework *Accountability Components* include:

- **Administration.** Best practices for mitigating IT risks require that an organization define and measure the effectiveness of its operational processes, structure, guidelines and parameters. Organizations are provided with a tangible means to implement, manage and measure these procedures, which are normally too complicated and immense to accomplish. The Framework has the ability to break down this complex problem into smaller components by identifying organizational structures, users and roles, workflow parameters, policy structures and risk classification, which are then used within the Framework as an overlying process around the entire solution.
- **Security Audit.** eSO Framework provides the tools necessary to carry out effective internal audits through predefined technology assessment procedures. Using these procedures, security auditors, managers, system administrators and data owners can generate compliance checklists on an asset or asset group, allowing them to determine their company's current state of security compliance.

- **Reporting.** The key to effective IT risk management and decision making is having access to real-time information regarding risks across the enterprise. With eSO Framework, risk stakeholders can view information on demand through standard and ad hoc reports. Users can create, execute and save queried reports on information at the enterprise, business unit or asset level. These reports provide instant snapshots of an organization's security and IT risk posture.

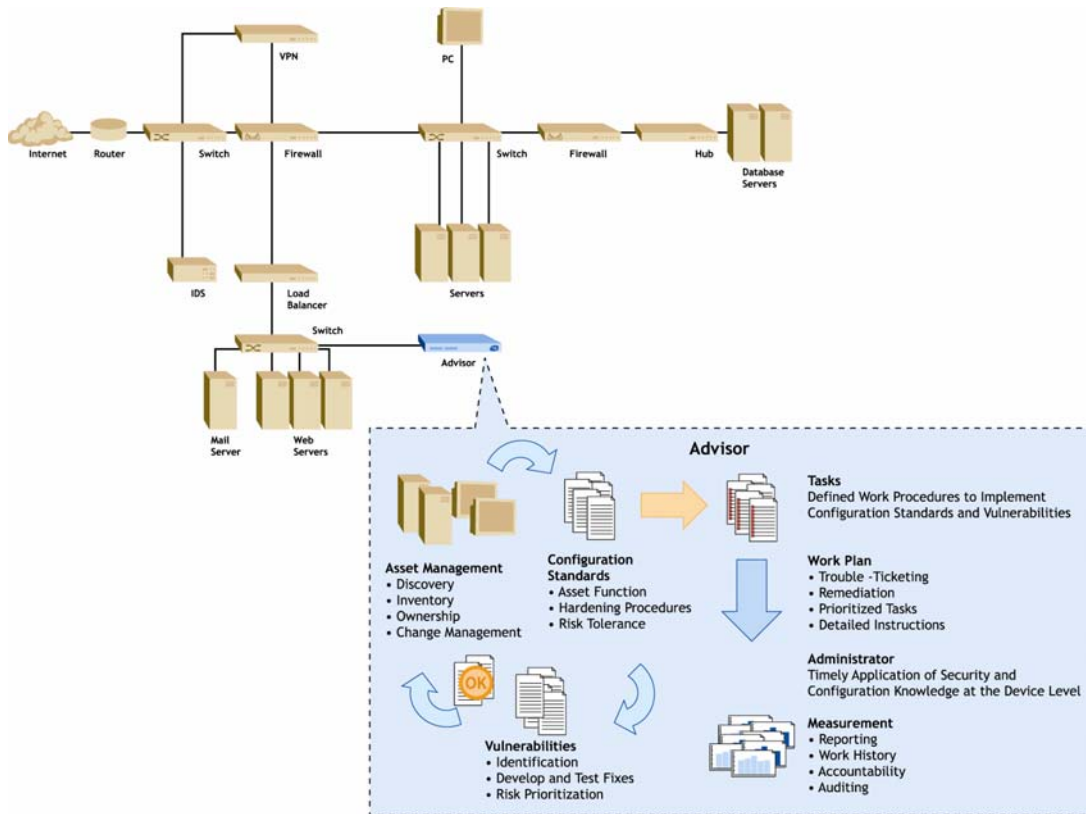
#### eSO Advisor™

To address the increasing demand for a vulnerability management solution that can be hosted on a company's network, eSO developed eSO Advisor™. eSO Advisor (Asset Discovery and Vulnerability Intelligence System with Onsite Repository) is a turnkey appliance that brings select features of eSO's Framework™ hosted solution to companies seeking a scalable, easily deployed package designed to operate with asset profile information behind the firewall. eSO Advisor allows companies to quickly and affordably establish a robust and easily manageable corporate security posture, while reducing the cost of owning and maintaining their IT assets.

eSO Advisor is the first vulnerability management product that helps enable organizations to automatically assess and manage security risks likely to impact their specific IT assets. eSO Advisor also allows companies to track their progress in protecting their environment from attacks. In addition, eSO Advisor is the IT security industry's only appliance to leverage vulnerability information from more than 2,400 Ernst & Young security specialists.

Targeted at companies of any size, eSO Advisor:

- Correlates automated discovery, inventory and assessment processes with an extensive and continuously updated database of verified threats and proven fixes;
- Automatically surveys and inventories a company's network of IT devices and assets, and deploys Ernst & Young knowledge to create a prioritized list of security risks correlated with a company's devices and mission-critical software.
- Helps security personnel to immediately attend to the most potentially damaging vulnerabilities using keystroke-by-keystroke instructions.
- Can be implemented anywhere within a client's network.
- Can be clustered via eSO Director™, eSO Advisor tool's management console, so IT managers can more efficiently evaluate and update multiple eSO Advisor systems to protect larger networks.



Key eSO Advisor features include:

- **Auto-discovery.** Automatically surveys devices connected via specific IP address ranges, in most cases retrieving, to the extent possible, the device name, MAC address, qualified domain name and operating system. eSO Advisor can assess up to six “Class C” IP ranges, and can address vulnerabilities even on devices with dynamically assigned IP addresses.
- **Auto-inventory.** Identifies installed technologies and applications on targeted devices storing the asset information locally
- **Auto-update.** As often as users wish, eSO Advisor automatically updates its vulnerability database from the Ernst & Young knowledge base.
- **Multi-user work list.** A single and customizable list of prioritized tasks can be shared among multiple users for maximum efficiency in patching IT vulnerabilities.
- **Audit assessment.** Allows IT managers to generate audit reports correlating vulnerabilities with work history status.
- **Flexible device support.** Supports up to 254 assets on a single appliance, and seven eSO Advisor users, five of whom can be concurrent.
- **Support for major platforms.** Can automatically inventory devices using the following operating systems: HP.UX, Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows XP, Red Hat Linux, and Sun Solaris.
- **Unique appliance package.** eSO Advisor combines eSO-developed security software with Ernst & Young data for delivery on an Intel hardware platform.

**eSO Market Strategy.** With the debut of eSO Advisor, eSO is evolving its market strategy to bring its solutions to a larger global customer base through a broadly dispersed indirect channel.

**Management.** eSO benefits from a diverse group of senior managers whose drive, expertise and vision create a unique competitive advantage for the company.

*Robin Hutchinson, President and CEO.* Robin Hutchinson joined eSO in 2000 to oversee a dramatic expansion in the company's focus: first from a security portal to a provider of host risk management solutions, and now as a leading provider of packaged vulnerability management products. At eSO, Hutchinson draws from more than 15 years of experience in the security, eCommerce and technology industries to oversee the company's day-to-day operations and chart its strategic direction. Hutchinson's background as a managing partner at Ernst & Young's Innovative Solutions Group Practice spans both technical and entrepreneurial roles: As a technologist, he has developed and implemented security methodologies and strategies for Fortune 500 clients; as an entrepreneur and manager, he has identified and pursued high-revenue potential initiatives, including venture investments, new practices, and go-to-market plans. He also has taken two companies public during his tenure as a senior executive with ASG Technologies, Secure Computing Corporation, Border Network Technologies and Health Systems Group. Hutchinson earned a bachelor's degree from McMaster University.

*Kevin Price, Chief Financial Officer.* With more than 20 years of experience as a financial decision-maker in the networking, software and Internet industries, Kevin Price heads all of eSO's financial planning, execution and operations. An Ernst & Young partner, Price also has extensive experience in mergers and acquisition consulting, public and private offering transaction consulting and assisting numerous companies with IPOs. Before joining the eSO management team, he was an audit partner for Ernst & Young, serving clients in various technology industries. Price has a bachelor's degree in Accounting from Illinois State University.

*John Giubileo, Vice President, Products and Services.* John Giubileo is responsible for eSO's product development, infrastructure support and research and development endeavors. For more than 12 years, Giubileo has built, managed and secured large enterprise networks in both the commercial and government sectors. He also has a strong background in a variety of security areas, such as encryption, firewalls, authentication protocols, Intrusion Detection Systems, Virtual Private Networks and Public Key Infrastructures. Prior to joining eSO, he was director of managed security services for Sprint Corporation. Giubileo holds a bachelor's degree in Computer Science and Industrial Management from California University of Pennsylvania.

*Ken Hammond, Vice President, Business Development.* Ken Hammond brings to eSO unique venture capital experience from eVenture, a construction company where he served as president, director and chief operating officer. Hammond's negotiating and relationship-building skills play into his role at eSO, where he is responsible for establishing strategic partnerships in targeted verticals and security related industries. A technology industry veteran, Hammond also has a strong background in commercial process architecture, enterprise solutions, application development, business analysis and process mapping. His other industry experience includes five years with Black & Veatch's Information Technology subsidiary, BV Solutions Group. He holds a bachelor's degree in Civil Engineering and a master's of business administration in management from Rensselaer Polytechnic Institute.

###

© Copyright 2002 eSecurityOnline LLC. All rights reserved. All eSO products or services mentioned herein are the registered or unregistered trademarks and service marks of eSecurityOnline, LLC. All other trademarks or service marks are the property of their respective holders and are hereby acknowledged.

Press Contacts:

eSecurityOnline, Monte Beery, 816.480.5186; monte.beery@ey.com  
Catapult Partners, for eSO: Theresa Campbell, 916.419.0281; [theresa@catapultinc.com](mailto:theresa@catapultinc.com)

Last Updated: October 2002