



# Applied Intelligence for Effective Risk Management

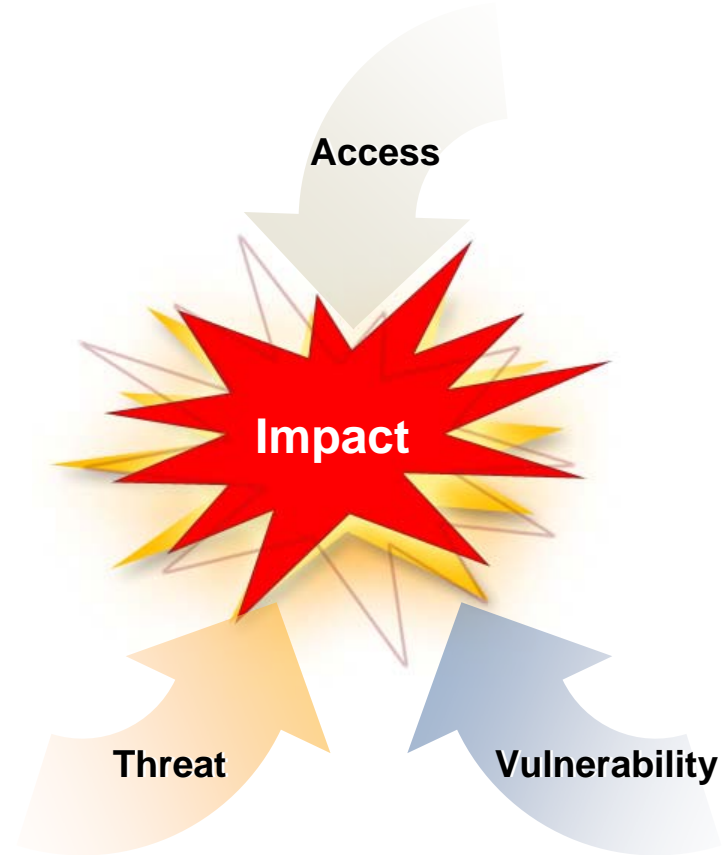


Presented by John Ferguson  
Director of Product Strategy

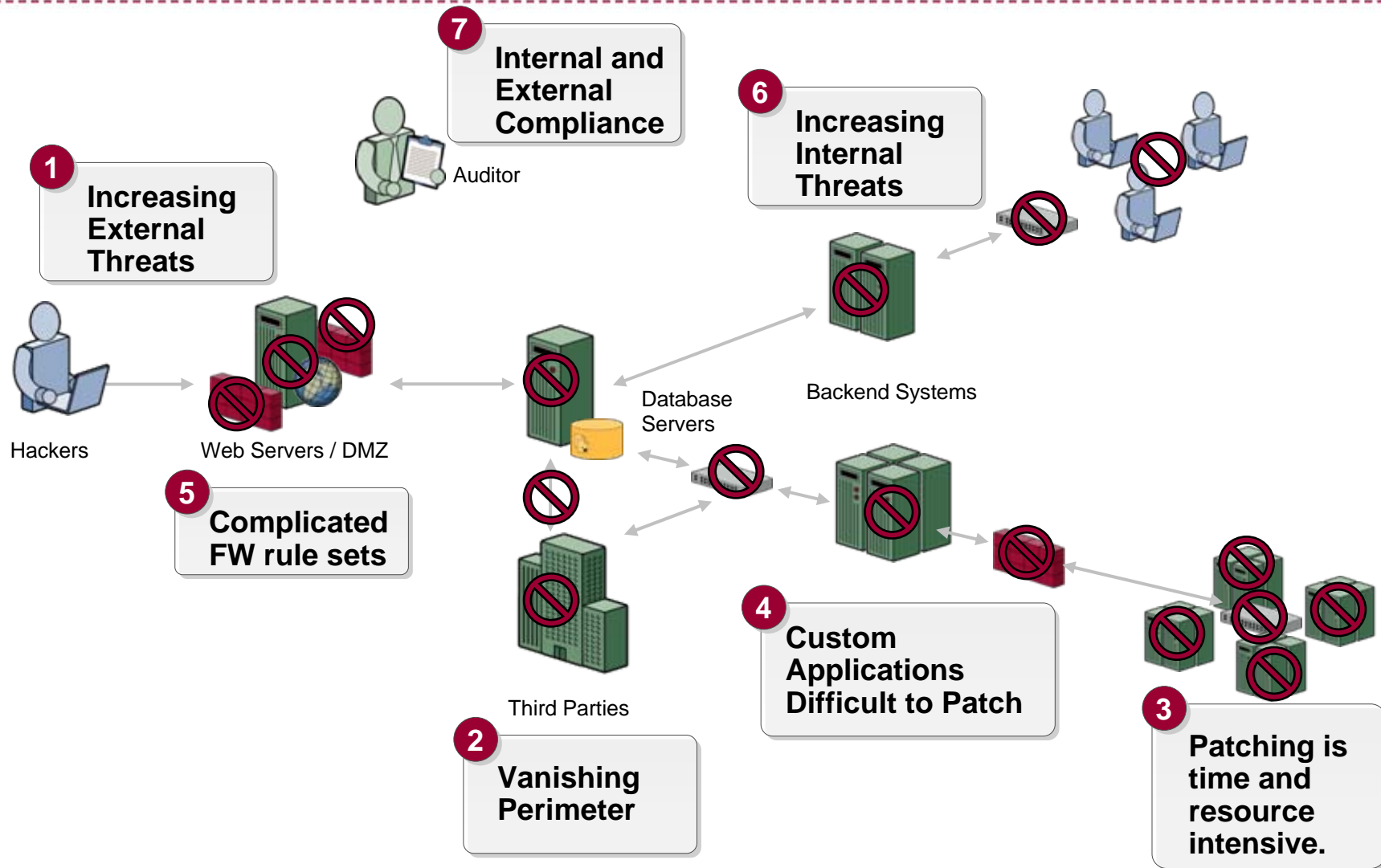
Where it all comes together:

# How Do We View Risk?

- + Risk is the potential harm that may arise from some present process or from some future event
- + We define information security risk as the probability that a threat will exploit a vulnerability and cause an impact
- + Risk Management: A vulnerability is not an issue per se unless a threat exploits it and causes an impact. Risk management therefore ultimately involves minimizing the impacts.



# Information Security in the Real World = Uncertain Risk



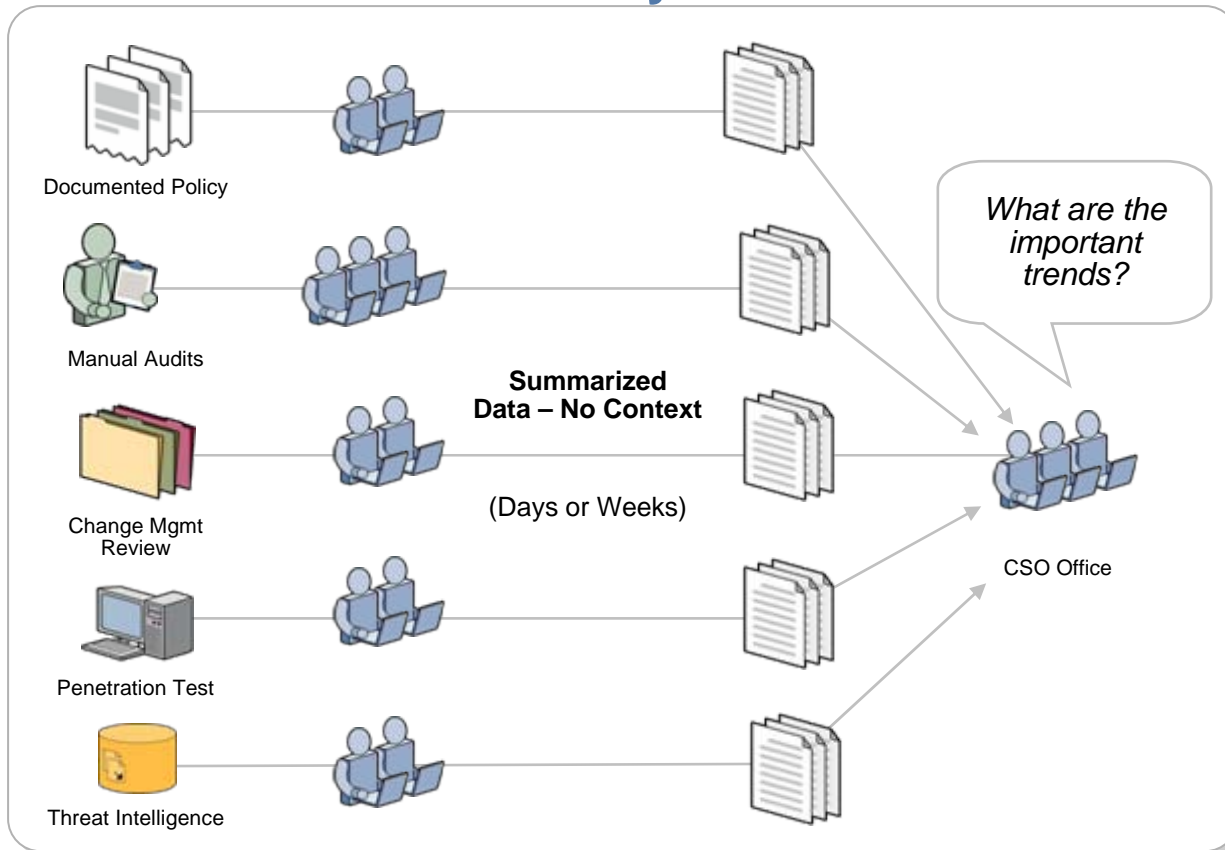
# Is Your Information Security Risk Being Managed?

## *Some questions to ask:*

1. Do you know your current level of risk exposure? Is it improving or getting worse?
2. Can you identify your top security risks including which assets are at risk and top violations?
3. How susceptible are you to the latest worm or virus outbreak?
4. Are you in compliance with your documented security policies?
5. How effective are your security initiatives and investments?

# Risk Management Methodology

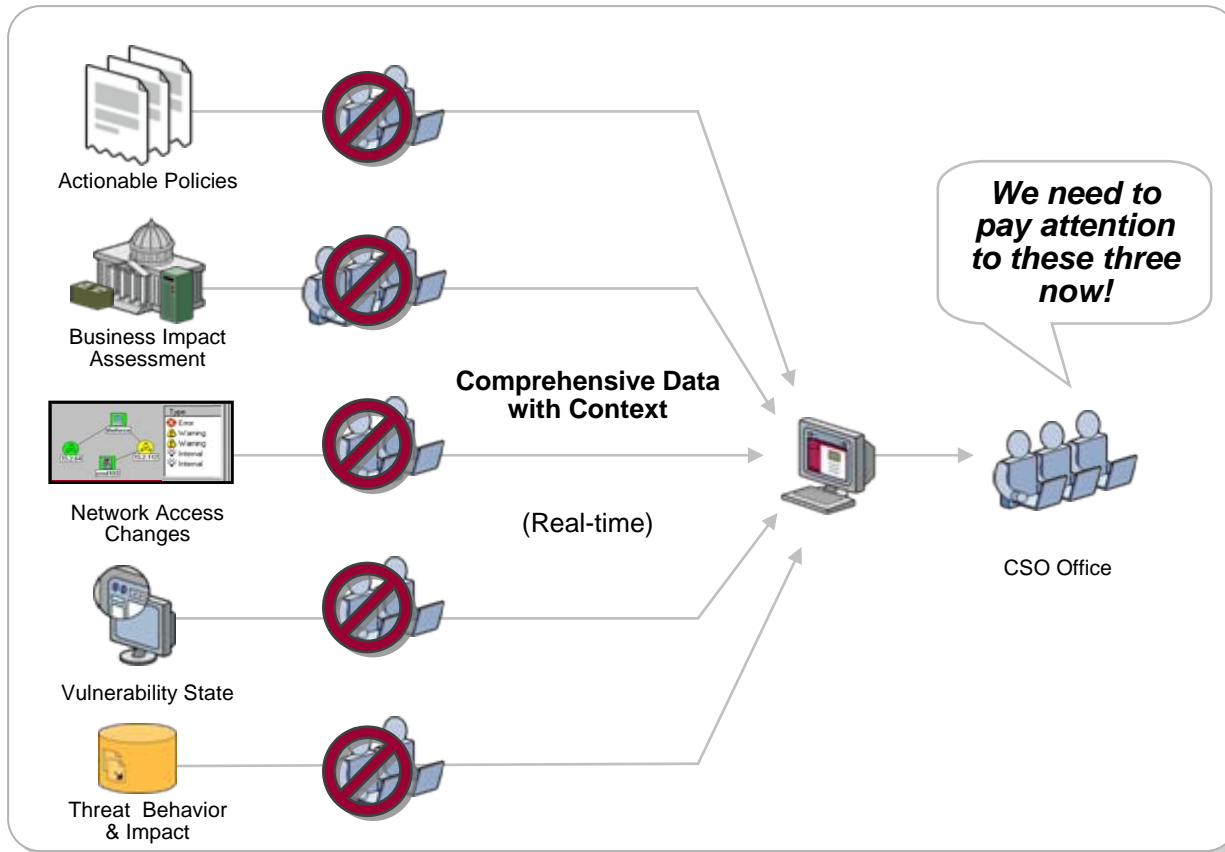
## Today



- + Point in time projects
- + Disparate activities in unconnected silos
- + Extremely labor intensive
- + Multiple outputs with little context
- + Decision-making is extremely difficult and highly reactive

# Risk Management Methodology

## What it Can Be



- + Information gathered in real time
- + Information consolidated from various sources
- + Analysis dynamically generated with minimal labor
- + Consolidated Analysis
- + Better, more proactive decision-making

# A Comprehensive Approach Is Required

## A risk-based approach

- + **Quantifies** asset value to the business
- + **Identifies** likely attack sources and access paths;
- + Helps **Visualize** business-impact view of threats and vulnerabilities
- + **Addresses** compliance requirements with regulations such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, Basel II, etc.

## Effective risk management

- + Integrates security intelligence to **identify** threats
- + Maps risk prioritization based on asset values to **quantify** risk
- + Adheres corporate information security policies, procedures, and standards
- + Allows organizations to **visualize** impact before and after network and system changes and once newly discovered vulnerabilities or threats are identified

# Security Risk Profiling Service Announcement

---

***VeriSign Introduces the first Comprehensive Service to Help Enterprises Identify, Visualize and Quantify Information Security Risks in order to Make Better Operational and Financial Decisions.***

By taking a holistic view of threats, vulnerabilities, network access policies, and potential business impacts, the service allows customers to dynamically generate a risk score including financial impacts, to simulate and model the effects of changes, and to measure compliance with both internal and external policies and regulations.



# VeriSign and SkyBox Security

VeriSign delivers world class services to enterprise customers by leveraging industry-leading technology, trained, experienced experts, structured processes, and unique intelligence.



- + Global Security Consultants that perform hundreds of annual risk and compliance assessments
- + MSS service and delivery model that dramatically simplifies implementation and ongoing management
- + Unique ability to identify and understand evolving threats including iDefense Security Intelligence
- + Leverages Atlas infrastructure that supports .com and .net
- + Best-in class Security Portal



- + Recognized industry-leading technology with a variety of unique capabilities including:
  - The ability to take feeds from a variety of technologies and vulnerability management tools
  - Sophisticated modeling, simulation, and visualization capabilities
  - Modules designed to track compliance with best standards and with a number of government and industry regulations

# VeriSign Approach to Risk Management

## VeriSign Security Consulting

## VeriSign Managed Security Services

### Policy and Risk Level Baseline

- + Start with Best Practices Policy
- + Add custom policy rules
- + Identify critical applications, connectivity, and business impact values

### Model

- + Proposed network rule changes
- + System updates and changes, e.g. patches
- + Attack simulations and new vulnerabilities
- + Determine new exposures and changes in risk levels

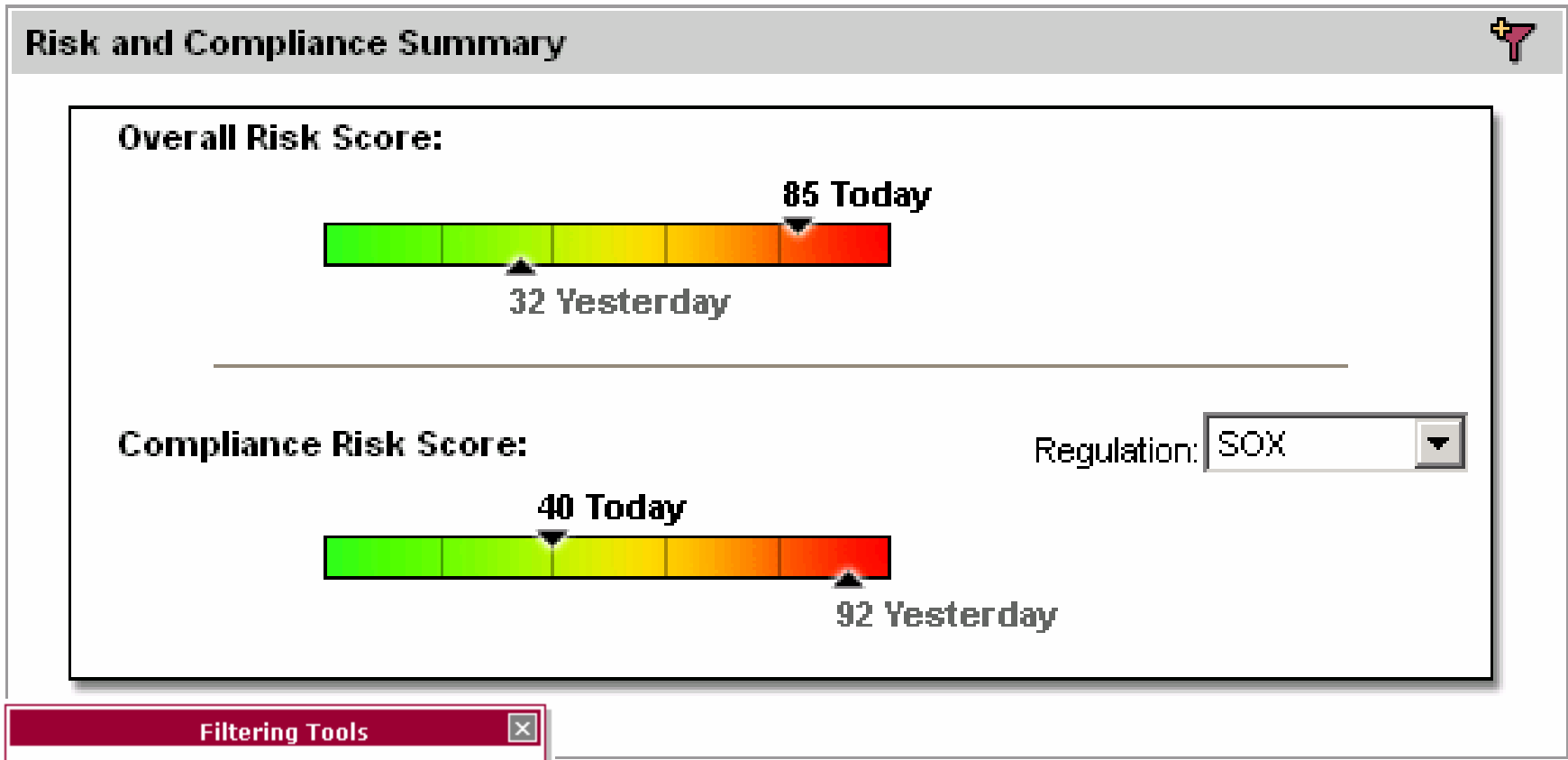
### Analyze Business Risk

- + Link operational changes to potential business impacts
- + Deny or accept risk for compliance reporting and alerting
- + Audit results relative to internal standards and regulatory requirements

## VeriSign iDefense Security Intelligence Services

## VeriSign Managed Security Services

# Question 1a. Do you know your current level of risk exposure?



**Filtering Tools**

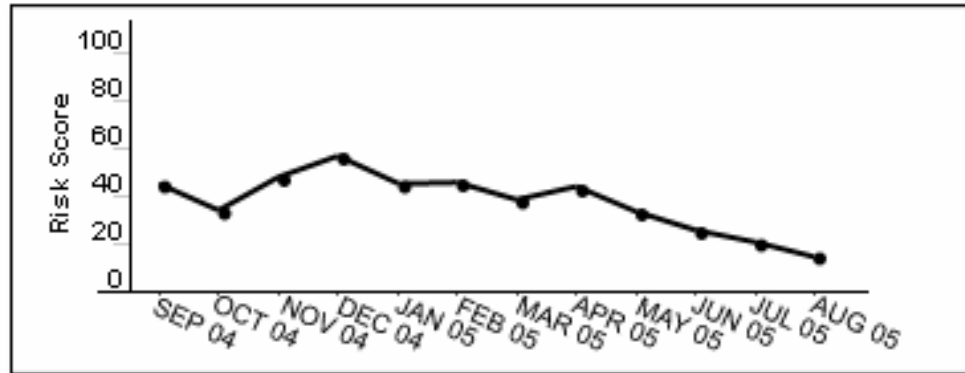
Filter: All

Compare Today with: Last Month

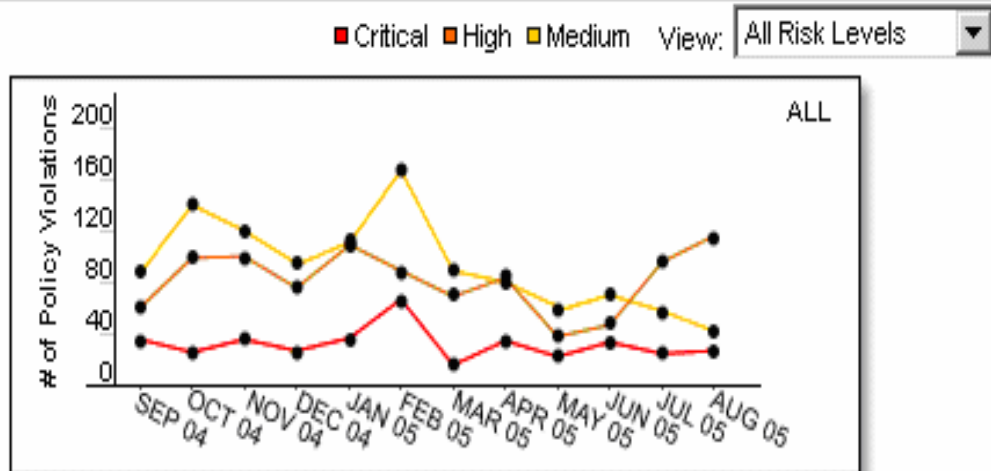
**Apply**

# Question 1b. Is it improving or getting worse?

Risk Score Trend



Policy Violation Trend



## 2. Can you identify your top security risks?



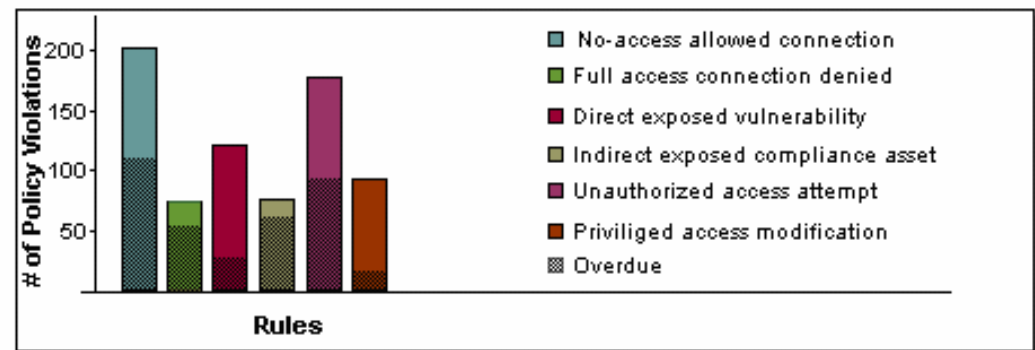
### Top Risk Contributors



Asset	Risk Score
Firewall Systems	98
Production DB	97
Web Servers	95
Customer Data Store	94
DYNAMIC-UDP	76
Deny protocol	44
ICMP	41
Outbound NETBIOS	38
NETBIOS SMB-DS	37
Inbound TCP	12

Business Unit A

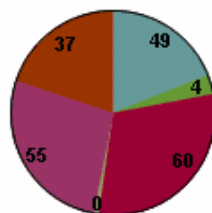
### Policy Violations



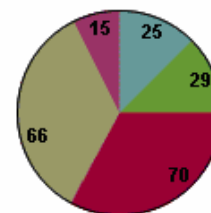
Business Unit A - 45 Firewalls

# 3. How susceptible are you to the latest worm or virus outbreak?

## Exposed Vulnerabilities Report

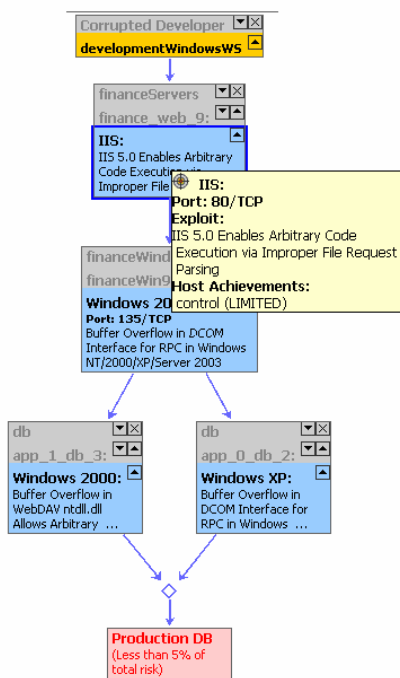


- Direct
- Indirect
- Potential
- Excluded
- Unknown

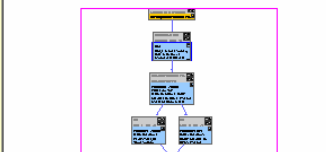


- Critical
- High
- Medium
- Low
- Info

Severity	Exposed		Not Exposed				Total
	Direct	Indirect	Inaccessible	Potential	Excluded	Unknown	
Critical	8	0	16	0	1	0	25
High	0	4	8	0	15	2	29
Medium	14	0	10	0	26	20	70
Low	20	0	18	0	13	15	66
Info	7	0	8	0	0	0	15
<b>Total</b>	<b>49</b>	<b>4</b>	<b>60</b>	<b>0</b>	<b>55</b>	<b>37</b>	<b>205</b>



**Skybox ID:** SBV-00262  
**CVE:** CVE-2000-0886  
**Discovery method:**  
**Scanned by:**  
**Severity:** High  
**Host Achievements:** Control (LIMITED)  
**Description:**  
 IIS 5.0 allows remote attackers to execute arbitrary commands via a malformed request for an executable file whose name is appended with operating system commands, aka the "Web Server File Request Parsing" vulnerability.



# 4. Are you in compliance with your documented security policies?



## 1. Access Policy Compliance - Summary

Number of Rules in the scope: 22.

Policy success rate: 86% of the rules are compliant with Policy (19 rules out of 22).

Total number of Policy violations: 3 Rules.

Number of critical Policy violations: 0 Rules.

Number of Access Queries: 0 Rules.

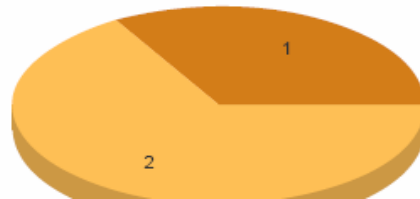
Last calculation time of the Policy: Thu Oct 20 14:36:08 EDT 2005.

## Access Policy Violations

### Access Policy Rules by Compliance



### Access Policy Violations by Importance



The screenshot displays the Windows Firewall console. The left pane shows a tree view of policies, with 'Restrict NetBIOS' selected under 'Public Policies'. The right pane shows the rule's configuration for the 'Live' profile. The rule is applied to 'Internal Networks' (192.168.1.0/24) and specifically targets '137-138 (UDP)' and '139 (TCP)'. The 'Details' pane shows the rule's scope: source IP ranges (0.0.0.0-9.255.255.255, 11.0.0.0-99.255.255.255, 100.0.1.0-100.0.255.255, ...), source services (1-65535/UDP), and inbound rules (9 (Access) - Allow, 2 (NAT) - Translate). The destination IP is 100.2.0.15, which is translated to 192.168.1.5.

## 5. How effective are your security initiatives and investments?

### Security Risk Profiling Summary

Last Risk profile Update: 10:56 am, 08/13/03

Total System Host Assets: 1000

Total Network Assets: 12

Business Value: \$100M

Business Risk Impact: \$5M

Assets at Medium Risk : 4

Critical Risk

High Risk

Medium Risk



# Security Risk Profiling Service

*The service leverages industry-leading technology from Skybox Security and includes:*

## **Automated IT security modeling**

- To gain a complete network view that includes location of assets and all associated access paths.

## **Simulation and Visualization**

- To understand the impact of and better prepare for potential threats.

## **Business impact analysis and risk metrics**

- To help quantify the financial and operational impacts to help prioritize activities.

## **Early warning analysis**

- To immediately identify and understand the impact of threats as they emerge.

## **Regulatory compliance risk management**

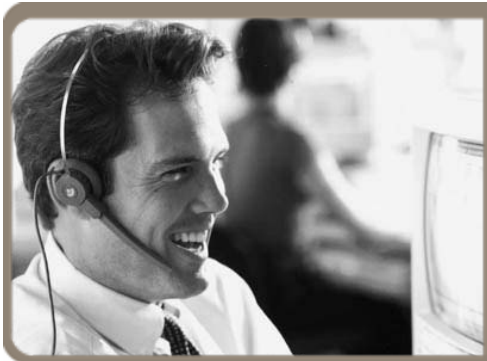
- To understand whether you are in compliance with internal policies and external regulations.

# Managed Security Approach

## GLOBAL SECURITY CONSULTING



## SOLUTION DESIGN & IMPLEMENTATION



## 24x7 SECURITY MONITORING



## THREAT & VULNERABILITY RESEARCH