

## Continuous Risk Assessment and Vulnerability Prioritization

Organizations invest millions in IT security technology and resources yet are unable to determine the risk exposure of critical assets; or whether or not the risk level is increasing or decreasing. In addition, organizations have tens of thousands of vulnerabilities throughout their IT infrastructure yet they cannot quickly or accurately prioritize which vulnerability should be dealt with first; or how to best mitigate these exposures.

Security professionals are overwhelmed by the number and diversity of vulnerabilities. Manual risk assessment and vulnerability prioritization processes are inefficient and labor-intensive. Quantifying risk and business impact on a continuous basis remains an elusive goal. Finally, remediation is often broadly applied because it is impossible to understand the complex matrix of security controls, policies, and vulnerabilities.

Skybox's Risk Exposure Analyzer continuously quantifies risk and prioritizes vulnerabilities by taking into account business logic, network and security configuration, threats, and vulnerabilities. Using a fraction of the resources, security professionals can understand and analyze the business impact of threats, simulate attacks on the network, and simulate the most cost-effective remediation alternatives.

## Business Problem

- Tens of thousands of unmanageable vulnerabilities exist
- Level of risk exposure is unknown and nearly impossible to identify
- Vulnerability prioritization process is manual and highly subjective
- Difficult to identify which portions of the network are vulnerable to attack
- Difficult to measure or justify security investments
- Inability to quickly evaluate which countermeasures to use
- Escalating cost due to labor-intensive and inefficient manual processes

## Value Proposition

The Risk Exposure Analyzer automates the risk assessment and mitigation planning process. This is accomplished through continuous assessment and quantification of risk and prioritization of vulnerabilities taking into account business logic, network configuration, threats, and network access policies.

The Risk Exposure Analyzer provides users with a unified, consistent and quantified view of security risk for the entire IT network. Risk exposure is reduced through an automated and proactive risk assessment process. More confident and accurate decisions can be made by determining which threats pose the greatest potential harm to the business. In-depth analysis enable users to determine the safest and most effective countermeasure to deploy. By doing so, the organization can quickly respond to strategic business initiatives.

## Why Skybox Security?

*"One version of the truth."*  
- Reuters

*"Risk exposure window is reduced by 95%."*  
- USAID

*"Allows us to carry out a measurable, repeatable, and predictable risk assessment and mitigation planning process."*  
- EGG Bank

*"By visualizing threats quickly and efficiently, we realized a full ROI in a year and a 300% ROI in three years."*  
- Credit Suisse

*"We now have more answers than questions."*  
- Barclays Capital

*"Once you have it, you realize you can't live without it."*  
- Standard Chartered Bank

*"Skybox could completely change the vulnerability assessment landscape and become the dominant vendor in the world."*  
- Forrester

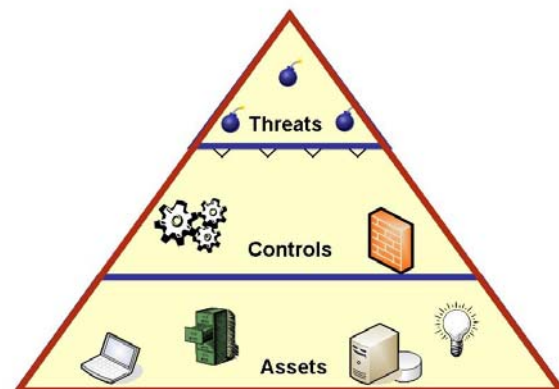
## Why Should You Care?

- Predict and eliminate exposures before the attack occurs
- Comply with regulatory and best practice requirements (SOX, PCI, FISMA, NIST, etc.)
- Reduce resources for on-going assessment and remediation work
- Provide risk metrics and benchmarks to management team

# Risk Exposure Analyzer

## Key Features

- Continuously updated virtual model of the IT infrastructure
- Normalized view of all threat, vulnerability, assets and control data
- What-if analysis—predicts risk behavior and business impact
- Business impact and risk metrics reports are generated in minutes
- Built-in ticket generation system and remediation status tracking
- Customizable reporting for management, auditors, and IT operations
- Automated vulnerability prioritization
- Supports most major information sources and devices: AlterPoint, BigFix, Check Point, Cisco, eEye, HP, ISS, Juniper, McAfee, nCircle, Nessus, Nortel, Opsware, Qualys, Symantec



## Benefits

- Accurate, continuous, and automated risk assessment process
- Simulate, visualize and analyze all attack paths and scenarios
- Overall reduction of security risk exposure
- Prioritized action plans for optimal remediation—based on network and business context
- Visibility into the risks that are detrimental to the organization
- Considerable time and labor reduction through automation of manual processes

## How It Works

Implementation of Skybox Security's Risk Exposure Analyzer is a six step process that will ultimately optimize the visibility and productivity of existing security layers.

**Step 1: Central Repository of Intelligence**—All corporate security related information is automatically collected and collated into the system. Sources include threat profiles, network configurations, asset classifications, and vulnerability data from network or application-level scanners.

**Step 2: Virtual Security Model**—Based on the above information, a virtual model of the entire IT infrastructure and its security profile is created causing no disruption to the live network. All collected information is normalized to simplify information sharing and analysis.

**Step 3: Attack Simulation**—Attacks on the system are simulated to calculate all possible access routes from each threat to critical business assets, capturing all vulnerabilities. Control weaknesses and accessible ports are highlighted. The likelihood of a successful attack, and the resulting impact on the business, is calculated.

**Step 4: Risk Analysis**—Risk exposure is calculated and results available in minutes. A risk value is assigned and aggregated based on individual assets, group of assets, business units or network segments.

**Step 5: Remediation Planning and Ticketing**—Remediation is automatically prioritized and ranked by risk level and is grouped by logical and/or geographical units. Countermeasure solutions are presented for each risk exposure. Remediation projects can be assigned to the network operations team responsible for provisioning configuration changes through a built-in ticketing.

**Step 6: Reporting**—Reports are tailored for the different audiences that will be utilizing them (examples; executives, security team, IT operations, and auditors).

