



Ensure Compliance with IT Security Policies and Protect Against All Classes of Vulnerabilities

Policy Management is a growing must-have for security professionals. IT security staff establish corporate standards to help reduce the risk of attacks from system vulnerabilities. The government is increasingly active in setting rules for corporate and system governance in an effort to protect the investments and assets of online customers. A simple error or deviation from these standards can represent millions of dollars in fines. A simple oversight exploited by a hacker can lead to millions of dollars of damage and irreparable reputational harm.

Catbird's Policy and Trusted Scan Monitor helps organizations ensure that they are in compliance with established IT security policies, monitor new and evolving regulations and perform both OS and application-level trusted scans to protect against all classes of vulnerabilities.

POLICY COMPLIANCE: DETECTION, NOTIFICATION & MITIGATION

An ounce of prevention is worth a pound of cure. Catbird's Policy and Trusted Scan Monitor allows IT managers to take a proactive stance against devastating security attacks. Catbird's continuous monitoring will detect any asset out of compliance with established policies. If a device is found to deviate from corporate guidelines, Catbird immediately notifies appropriate IT personnel with actionable intelligence. Staff can then make the best choices about the next step, including mitigating potential security or regulatory risks through Catbird's Penalty Box – a built-in ability to quarantine the out-of-compliance host. Through the Penalty Box, the compromised device will cease to be a threat to the rest of the organization, giving IT staff the opportunity to evaluate and remediate. Logging, reporting and tracking of the alerts and response taken is available to auditors and managers as a demonstration of proactive compliance.

TRUSTED SCAN

Many vulnerability scanning solutions monitor only external ports. But security threats can originate from inside of the network, just as they can originate from external hackers. Catbird's continuous Trusted Scan monitoring complements Catbird's External and Internal Intelligent Vulnerability Monitoring with a comprehensive check of all classes of vulnerabilities.

BENEFITS

Monitors for Corporate Best Practices Determines whether corporate policies are being followed and alerts IT personnel when exceptions are discovered.

Comprehensive Protection for all classes of vulnerabilities Including software defects, unnecessary services, unsecured accounts, misconfigurations, incorrect patch levels and backdoors.

Eliminates false positives and guesswork Credentialed scanning means IT administrators are guaranteed accurate information as monitor logs into machine itself.

Continuous and Automated Protection Instant notification upon any violation of corporate policy. CIOs and auditors secure in their knowledge that network security infrastructure stays in compliance at all times.

Ensure Compliance with IT Security Policies and Protect Against All Classes of Vulnerabilities

The Policy and Trusted Scan Monitor rounds out a security profile by providing full vulnerability threat protection— including ones that require credentials to proceed. Examples of risks detected by Catbird include outdated software on client PCs, OS patch levels and application-level vulnerabilities for the most popular programs, such as browsers, IM and search engines.

Catbird's continuous monitoring instantly alerts IT staffers if an OS or application vulnerability is detected. Corporate policy would determine whether Catbird's Penalty Box quarantine mechanism is warranted to neutralize the device and prevent risk to the rest of the network. All alerts, data and actions are logged to an auditable file for use by IT managers and auditors.

Catbird's Policy and Trusted Scan Monitor is easy to setup. Leveraging Active Directory or single administrative domain configuration, multiple machines can be tested via a single login. This eliminates the need for multiple logins to scan multiple machines.

POLICY AND TRUSTED SCAN COVERAGE AREAS:

Policy Checks Detects, notifies and mitigates upon a violation of a corporate PC out of compliance with established policies. Examples include password policy, guest account policy, audit file logging status, Windows registry checks and non-authenticated system shutdown.

Vulnerability Checks Detects, notifies and mitigates upon detection of over a hundred application-level vulnerabilities. Coverage includes vulnerabilities in the most popular programs including Google, Quicktime, McAfee, Skype, VERITAS, Mozilla, Firefox and Real.

Patch level Checks Detects, notifies and mitigates upon detection of outdated software on client PCs. Corporate policy would determine whether user needs to upgrade to current patch levels for improved security.

The Catbird Difference

CONTINUOUS

All Catbird technology is based on a simple principle: security is a continuous process. Continuous protection ensures that new 'best practices' policies, vulnerabilities and patch levels are detected immediately, 24x7, 365 days a year.

COMPREHENSIVE COVERAGE

Goes beyond traditional policy-compliance scanning to include vulnerabilities, misconfiguration and patch-level aging on a range of Windows operating system and application-level services. Complements Catbird's broad suite of security and performance services.

FULLY AUTOMATED

All Catbird technology is fully automated. Monitoring and protection occur automatically.

NO CLIENT TO INSTALL

Full protection provided without hassle and expense of installing software on each covered machine.

COST-EFFECTIVE

Catbird's "more for less" coverage is a fraction of the cost of its competitors.