



CONTROLLING AND MONITORING CHANGE



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

The majority of system outages occur from a breakdown in the change control process; the ROI on solidifying this process can be significant.

Minimize Risk and Downtime with Change Management Controls


Challenges

Organizations continue to face an ever-growing and dynamic landscape of security threats that are becoming more targeted and malicious in nature. Recent attacks are no longer being launched en masse: rather they are focused and sophisticated, with a clear directive to defeat tactical, reactive security technologies that are in place at an organization. Whether an attack targets a network, an endpoint device, a sensitive business application, or even a database, it is important for any organization to have visibility into how these systems are being used and by whom in order to protect against a catastrophic event such as a security breach, system outage, risk event, or compliance violation that results from an unintentional or unauthorized change to these systems.

Organizations have little visibility into the effectiveness of their change management controls across their IT infrastructure. When change controls are not effectively managed and monitored, the impact of this can be devastating. Initially, reduced availability across key corporate, financial, and customer systems can occur if unauthorized changes or software updates are made, even if these are non-malicious in nature. These activities can affect key functionality, or even bring down complete systems. As systems must then be taken offline to mitigate a security issue or simply back out the unauthorized change, this can cause a dramatic loss of revenue as capital expenditures are increased to resolve the issues, and customers cannot access revenue-producing systems.

Second, change management controls are a foundation of many regulatory compliance standards and requirements, including Sarbanes-Oxley and PCI-DSS. Many organizations rely on manual processes or point technology solutions in an attempt to react to change requests and activities across their environment. Reliance on manual controls and reactive processes to validate that unauthorized changes did not occur is extremely ineffective and can leave a company exposed to significant undue risk. In addition, these inefficient, manual processes lead to increased compliance and operational costs to test, validate, and report on change management requirements.

Finally, ineffective change control processes can directly lead to the breakdown of an overall security management program. Overall risk exposure is increased as new vulnerabilities are introduced across IT, financial, and operational systems, and systems require more frequent and updated patches to mitigate these vulnerabilities. Without direct oversight and monitoring of change controls across every system, device, and application, organizations cannot holistically protect against internal or external security and risk issues occurring throughout their environment.



Manual change control processes, assessments, and reporting leave organizations exposed to the unauthorized changes that occur between assessments. Automated enforcement delivers continuous protection against any unauthorized change.

Solutions

Every desktop, server, application, network device, and database must be in scope for any change control solution. If changes are not effectively managed across all of these, companies will remain exposed to possible security breaches and increased risk. An effective change control solution is engineered around three key processes: automated assessment, real-time monitoring, and continuous enforcement. By aligning these key processes, organizations can ensure that any change in their IT environment is authorized, overall system availability is maintained, and the effectiveness of their compliance and security programs is increased.

Automated assessment

Change control assessment capabilities enable you to quickly and effectively authorize and manage appropriate system changes, while also preventing unwanted changes across key systems. Initially, system image comparison diagnoses and reports on changes between deployed system images and “known” good, or gold-standard, images. Next, change reconciliation improves compliance through integration with current change management systems and policies to streamline workflow and change management processes. And finally, automated reporting and alerting enables real-time assessment and analytics of how any change may impact the stability of the IT environment, the state of regulatory or policy compliance to change requirements, and overall risk exposure.

Real-time monitoring

Monitoring enables you to maintain constant visibility into change requests across a controlled environment, ensuring that system uptime and compliance levels are maintained. Database activity monitoring capabilities automatically discover database instances across your network and continuously monitor them for any unauthorized change request. Ensuring that all database changes are monitored delivers high availability for your users across key applications. Integrity monitoring improves the overall state of compliance by enabling real-time monitoring and centralized management of file and configuration changes. This can reduce the overall level of compliance violations for unauthorized changes and improve the effectiveness of change management and reporting processes. Policy tracking capabilities directly improve security by ensuring that changes are managed per policy requirement, minimizing the impact from any ad hoc or unauthorized change.

Enforcement

A change control solution must be able to automatically enforce change policies across any system, application, network device, or database to ensure overall system availability and compliance. System availability levels are maintained through virtual patching and memory protection capabilities, which help prevent operating system and database attacks. The ability to prevent unauthorized changes helps maintain effective levels of compliance by eliminating unknown or unapproved system changes. Finally, dynamic whitelisting improves the overall level of system security by preventing all unauthorized software from running on your desktops and servers.

Best Practices Considerations

- Ensure change control processes cover desktops, servers, networks, applications, databases
- Invest in automated capabilities to assess, monitor, and enforce
- Leverage dynamic whitelisting to ensure applications and system remain compliant and secure
- Continuous monitoring of all change requests can help prevent system downtime, compliance violations, and increased risk exposure
- A single management platform pulls together all change control process and policy information, delivering a more efficient and effective change management program
- Centralized management of security, compliance, and change control process significantly lowers total cost of ownership

Value Drivers

The value drivers for controlling and monitoring change really reside in an organization's ability to manage and make changes to the core IT environment that are controlled and deliberate. This is achieved by:

- Demonstrating that patching can be accomplished at scheduled intervals instead of turning them into fire drills, while still maintaining a strong security posture and reducing the personnel time, QA, testing, and rollouts related to critical device management
- Addressing the question, "Are we secure?" through continuous monitoring and thus ensuring greater protection and the ability to demonstrate regulatory compliance with greater ease
- Preventing the exploitation of sensitive structured data stored in databases and avoiding the pitfalls that other organizations have encountered because of database breaches

Related Material from the Security Connected Reference Architecture

Level II

- Protecting the Data Center
- Obtaining Benefit from PCI
- Protecting Information

Level III

- Protecting Databases
- Identity Management and Trust
- Protecting Intellectual Property
- Protecting Customer/Patient Records and Information

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.

About the Author



Dave Anderson is Senior Director of Security and Risk Management for McAfee, responsible for the global product marketing strategy for the McAfee risk and compliance business unit. Dave has nearly 20 years of global experience in information security, risk management, and strategy at leading enterprise technology and services companies, including SAP, ArcSight, KPMG, and VeriSign, where he has developed market and product solutions that integrate risk, compliance, security and strategy into unified governance and risk frameworks. Dave's experience includes implementing and delivering IT governance solutions based on COSO, CobiT, ISO 27001, and ITIL standards. Dave has been published in multiple leading industry and technical journals and is a frequent speaker on risk management, corporate governance, and security strategy. Dave holds an MBA from Duke University, specializing in global management and strategy.

dave_anderson@mcafee.com

