NNT & CIS Controls Solution Brief

CIS CONTROLS BACKGROUND

The CIS Controls have been formulated to provide clarity and guidance for the bewildering array of security tools and technologies, security standards, training, certifications, vulnerability databases, guidances, best practices and compliance mandates.

The goal is to answer the fundamental questions regarding security:

1. What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program?

2. Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals and guidance to measure and improve?

3. Which defensive steps have the greatest value?

NNT delivers ***Security through System Integrity*** by introducing the essential Critical Security Controls, leveraging intelligent change control technology to track system integrity, and using dynamic policy and baseline management to ensure systems remain secure, available and compliant at all times.

Talk to us to find out more!

WHAT ARE THE CIS CONTROLS?

The vast array of compliance and security mandates out there can leave many organizations confused on where to even start, but NNT believes the best place to start is with the **CIS Controls**. Published by the Center for Internet Security (CIS), these controls help organizations defend against known attacks by condensing key security concepts into actionable controls to achieve better overall cybersecurity defense.

The CIS Controls provide clarity on what organizations ***really need to be focusing on*** in terms of security best practices to help prioritize actions that must be taken to defend against cyber threats. The latest version, CIS Controls V7, keeps the same 20 controls that businesses and organizations around the world already depend upon to stay secure; however, the ordering has been updated to reflect the current threat landscape The latest version breaks down the 20 controls into three specific categories: basic, foundational, and organizational.

CIS CONTROLS CATEGORIES: BREAKDOWN

- **Basic – (CIS Controls 1-6):** Key controls which should be implemented in every organization for essential cyber defense readiness.

- **Foundational – (CIS Controls 7-16):** The next step up from basic – these technical best practices provide clear security benefits and are a smart move for any organization to implement.

- **Organizational – (CIS Controls 17-20):** These controls are different in character from 1-16; while they have many technical elements, CIS Controls 17-20 are more focused mainly on people and processes involved in cybersecurity.

BACK TO BASICS: CIS CONTROLS 1-6

The majority of security incidents occur when basic controls are lacking or are poorly implemented. A study of the previous version of the CIS Controls found that 85% of cyber-attacks can be prevented by adopting the first five CIS Controls alone. NNT solutions alone can help you satisfy the first six CIS Controls.

CIS Controls 1 – 6 represent well known, cybersecurity basics and focus on the fundamentals of securing the infrastructure and monitoring it regularly for changes, including Configuration Management, Vulnerability Assessment, and Continuous Monitoring to know when a new critical vulnerability surfaces or an asset becomes exposed. By implementing CIS Controls 1 – 6 as continuous and evolving processes, organizations significantly reduce their risk while also adapting to today's continuously changing cyber threats and shifting business needs.

NNT & CIS Controls Solution Brief

CIS Critical Security Controls Mapped to NNT Solutions				
CIS Critical Security Control	Change Tracker™ Gen7 R2	FAST™ Cloud	Log Tracker™	Vulnerability Tracker™
Control 1: Inventory and Control of Hardware Assets	■			■
Control 2: Inventory and Control of Software Assets	■	■		■
Control 3: Continuous Vulnerabilility Management	■			■
Control 4: Controlled Use of Administrative Privileges	■			
Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	■	■		
Control 6: Maintenance, Monitoring and Analysis of Audit Logs	■		■	
Control 7: Email and Web Browser Protections	□			
Control 8: Malware Defenses	□		■	
Control 9: Limitation and Control of Network Ports, Protocols and Services	■			□
Control 10: Data Recovery Capabilities				
Control 11: Secure Configurations for Network Devices, such as Firewalls, Routers and Switches	■			
Control 12: Boundary Defense	□			□
Control 13: Data Protection	□	□		
Control 14: Controlled Access Based on the Need to Know	□			
Control 15: Wireless Access Control	□			
Control 16: Account Monitoring and Control	■		■	
Control 17: Implement a Security Awareness and Training Program				
Control 18: Application Software Security	□	□		
Control 19: Incident Response and Management				
Control 20: Penetration Tests and Red Team Exercises	□			

■ Full Coverage □ Partial Coverage

CHANGE TRACKER™ GEN7R2

NNT Change Tracker ™ Gen7 R2 combines industry leading Device Hardening, File Integrity Monitoring, Change & Configuration Management, Security & Compliance Management into one easy to use solution.

FAST CLOUD™ INTEGRITY ASSURANCE

Leverage NNT's cloud-based FAST™ Threat Intelligence to automatically validate file changes as they are detected using the world's largest authoritative file whitelist.

LOG TRACKER™ ENTERPRISE

NNT Log Tracker ™ is a comprehensive and easy to use security information & event log management with intelligent & self-learning correlation technology to highlight potentially harmful activity in seconds.

VULNERABILITY TRACKER™

Identify known vulnerabilities within software and configuration settings before they can be exploited by a cyber attack using Vulnerability Tracker ™.