AD-HOC

This level is characterized by reactive firefighting. All network device provisioning, configuration, and updates are completed manually, box by box, and often under duress. Vulnerability remediation is manual, without regard to SLA. Network inventory data is practically nonexistent or, where available, routinely outdated, as they rely upon manual updates. Responding to compliance audits is complicated by information that is incomplete, inconsistent, and in silos, sometimes leading to audit failures which require even more follow-up. Reporting is limited and not standardized. As organizations quickly realize, they cannot stay here long and hope for Network Operations to enable business agility.

INITIAL

Necessity often drives enterprises quickly to Level 2. Here, golden configuration templates and images are introduced, but “automation” means vendor-specific CLI scripts which are costly to develop and maintain for device provisioning and updates. Vulnerability remediation is still manual, as no comprehensive vulnerability management strategy is yet to be in place. Inventory information is found in spreadsheets, but often outdated, as there is no change management integration. Although cursory inventory reporting is available, audit response still requires extensive effort as accuracy of the CMDB is suspect due to manual config efforts. A big risk organizations face is getting stuck here, convincing themselves that their inventory data is “good enough.”

INTERMEDIATE

Policy-driven network configuration and change management (NCCM) applies config templates consistently across the multi-site enterprise and a broad range of vendors and devices, and also facilitates continuous compliance, drift management, and rollbacks. Standardized reporting is used to address both operational and audit needs, and to create real-time compliance summaries and notifications of noncompliance. Automated security scanning is introduced, although vulnerability management is likely still manual and lacks context for backlog grooming. Organizations may have yet to attain a single Network Source of Truth (NSOT) for inventory, as ticketing and change management are still manual.

ADVANCED

Discovery and change management integration reveal dependencies and help prevent rollbacks. Automated configuration drift management and policy-driven compliance enforcement, together with closed-loop ticketing and enrichment, streamline incident response, increasing staff...
productivity and network uptime. Bulk remediation of noncompliance accelerates MTTR and reduces costly rework. Inventory trends and custom reporting inform business decisions. Vulnerabilities are auto mapped to network devices and remediation action; integration of security scanners to NCCM provides context for backlog triage, blind spot detection, and SLA management. Automatically deployed image updates or config changes, to targeted devices or in bulk processing, increases security, uptime, and productivity. As automation accelerates network operational efficiency and security, NetOps staff are increasingly available for higher value work, such as hybrid or public cloud networking, multi-site administration, or exploring enabling technologies (e.g., 5G, SD-WAN, and SaaS).

**INTELLIGENT**

Process orchestration coordinates provisioning and configuration across ITSM, asset discovery, ITOM, and CMDB. AI and ML anticipate needs, proactively deploying or adapting to prevent service outages. Automated asset discovery and dependency mapping inform NetOps decision making within the context of business impact. The CMDB/NSOT is fully trusted as network incident and change management workstreams are process orchestrated with automated vulnerability and drift remediation. The results: reduced errors, rework and costly downtime. Solutions enable cross-functional visibility and collaboration; NetOps are seen as a key enabler of business agility and partner to the business.

**NETWORK AUTOMATION MATURITY MODEL**

For more information, visit [https://www.bmc.com/it-solutions/truesight-network-automation.html](https://www.bmc.com/it-solutions/truesight-network-automation.html)