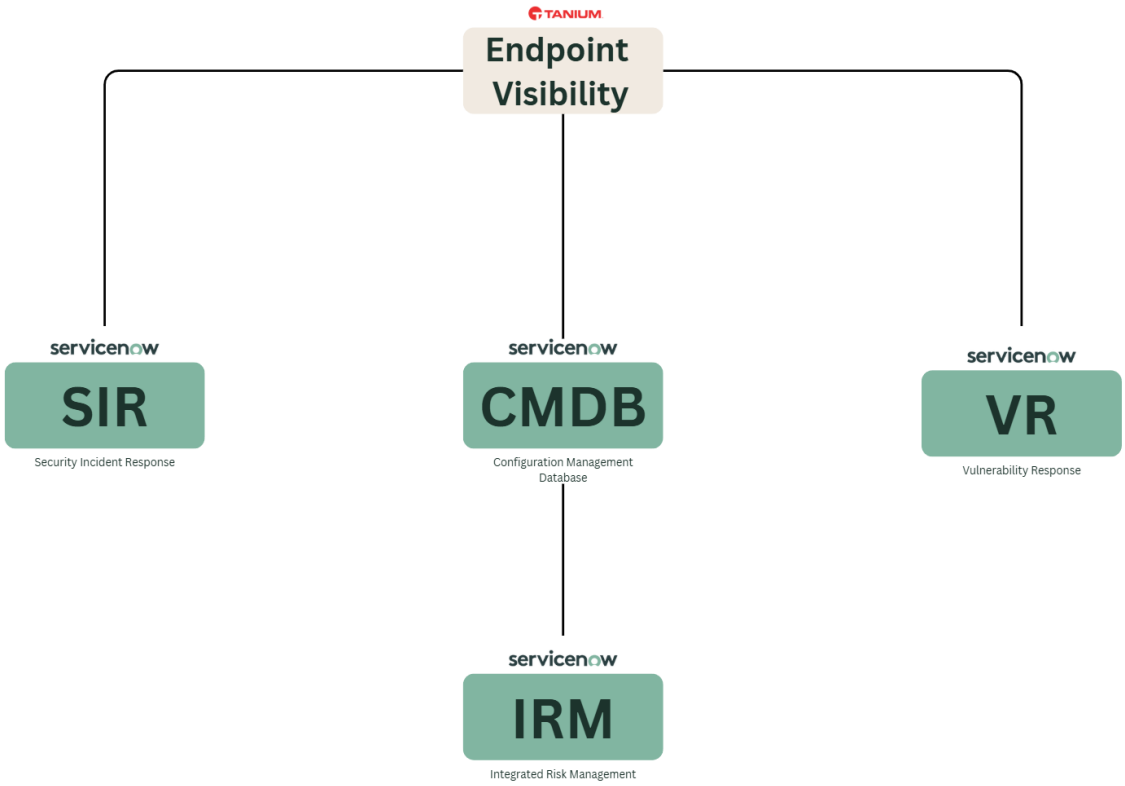


Figure 1 - Example Architectural Diagram

Introduction

In today's environment of rapidly evolving cyber threats, organizations face mounting challenges in balancing protection, compliance, and business agility. Traditional siloed tools no longer keep pace with modern attacks that exploit endpoint blind spots, overwhelm patch management cycles, and stretch audit teams thin.

This white paper provides a prescriptive strategy for combining ServiceNow Integrated Risk Management (IRM), Security Operations (SecOps), and the Configuration Management Database (CMDB) with Tanium's endpoint management and detection capabilities. Together, these platforms create a scalable, automated cybersecurity architecture that reduces risk, accelerates response, and ensures continuous compliance.

Unlike conceptual approaches that remain high-level, this paper lays out specific architectural recommendations, expected quick wins, and case studies demonstrating how organizations have achieved tangible results in as little as 90 days. By aligning Tanium's real-time endpoint visibility with ServiceNow's workflow automation and risk frameworks, enterprises can build a proactive security strategy that is resilient, adaptive, and business-aligned.

Cybersecurity Excellence: ServiceNow SecOps, IRM, & Tanium Endpoint Management

'ike (knowledge) level: Intermediate

Rev July 29, 2025

The Cybersecurity Challenge

Modern enterprises must contend with a rapidly expanding attack surface and a growing list of regulatory demands. Among the most pressing challenges:

1. Blind Spots at the Endpoint: Most breaches originate at endpoints. Without real-time visibility, unmanaged or rogue devices remain unprotected.
2. Threat Volume: Vulnerability disclosures and exploits grow daily. Security teams are overwhelmed with data but lack prioritization tied to business context.
3. Compliance Burden: Regulations such as GDPR, HIPAA, and PCI-DSS require continuous monitoring and evidence. Manual audits create delays and risk penalties.
4. Fragmented Tools: Point solutions for threat detection, vulnerability scanning, and response create silos that delay action.

To overcome these challenges, organizations require unified endpoint visibility, business-context prioritization, and automated workflows that close the loop between detection and remediation.

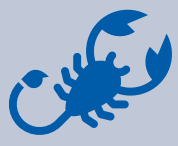
Architectural Recommendations

A prescriptive architecture for integrating ServiceNow and Tanium includes the following pillars:

1. Unified Endpoint Visibility & Asset Context

- Deploy Tanium as the system of record for endpoint data, including hardware, software, configurations, and vulnerabilities.
- Sync Tanium's endpoint data into ServiceNow CMDB to create a real-time, accurate asset inventory.
- Leverage ServiceNow Dependency Views to link incidents and vulnerabilities to critical services, ensuring business context drives prioritization.

2. Closed-Loop Incident & Threat Response



- Configure Tanium threat detections (e.g., suspicious processes, malware indicators) to automatically generate incidents in ServiceNow Security Incident Response (SIR).
- Enrich incidents with CMDB context, threat intelligence, and severity scoring to prioritize effectively.
- Automate playbooks using ServiceNow Flow Designer and IntegrationHub:
  - Isolate compromised endpoints
  - Deploy immediate patches or configuration fixes
  - Validate remediation success and update IRM risk registers

3. **Vulnerability Response & Risk Prioritization**

- Integrate Tanium vulnerability scans directly with ServiceNow Vulnerability Response (VR).
- Use CMDB data to assign criticality, ensuring vulnerabilities tied to core systems receive priority.
- Automate Tanium patching commands triggered by ServiceNow VR workflows, enabling SLA-based remediation.

4. **Compliance & Risk Automation**

- Feed Tanium compliance telemetry (e.g., CIS benchmarks, encryption status) into ServiceNow IRM indicators.
- Automate evidence collection for audits, reducing manual preparation by 50–70%.
- Map endpoint compliance data against ServiceNow IRM frameworks (ISO, NIST, HIPAA) for continuous readiness.

5. **AI/GenAI-Driven Assistance**

- Use ServiceNow's AI/GenAI to summarize incidents, suggest workflows, and provide contextual recommendations.
- Apply predictive analytics to anticipate emerging vulnerabilities and guide patch prioritization.

Quick Wins (Realized in 90 Days)

Organizations adopting this architecture can expect measurable benefits within the first three months:

- 50% faster vulnerability remediation through closed-loop Tanium + ServiceNow VR workflows.
- 60% reduction in audit preparation time with automated evidence capture.
- 30–40% lower Mean Time to Resolution (MTTR) for endpoint threats using automated incident isolation.
- 95%+ real-time accuracy in CMDB asset data, eliminating blind spots in risk and compliance tracking.
- Greater analyst efficiency, with AI/GenAI reducing manual triage and ticket noise by up to 40%.

Case Study Examples

Case Study 1: Global Pharma Organization
Challenge: Thousands of unmanaged endpoints created compliance risk.
Solution: Tanium populated ServiceNow CMDB with real-time endpoint data, integrated with IRM for risk tracking.
Outcome: Achieved zero audit gaps in FDA inspection and reduced audit prep by 65%.

Case Study 2: Retail & Consumer Goods Company
Challenge: Patching cycles stretched from weeks to months, exposing critical vulnerabilities.
Solution: Tanium vulnerability data flowed into ServiceNow VR, prioritized using CMDB criticality. Automated patch deployment executed through Tanium.
Outcome: SLA compliance for remediation improved from 40% to 90% within 3 months.

Case Study 3: Financial Services Provider
Challenge: Threat detection fragmented across tools, leading to 5-day MTTR.
Solution: Tanium threat intel integrated with ServiceNow SIR, orchestrating response via IntegrationHub.
Outcome: MTTR reduced to under 48 hours, dramatically lowering risk exposure.

Case Study 4: Healthcare Provider
Challenge: Manual compliance reporting delayed HIPAA audits and risked penalties.
Solution: Tanium compliance telemetry fed directly into ServiceNow IRM for continuous monitoring and automated reporting.
Outcome: Audit readiness achieved year-round, reducing audit prep effort by 70%.

Conclusion

A prescriptive, integrated architecture leveraging ServiceNow IRM, SecOps, and CMDB with Tanium endpoint management provides not only stronger cybersecurity, but tangible business outcomes.

By uniting endpoint visibility with enterprise workflows:

- Threats are detected and contained in real time.
- Vulnerabilities are prioritized by business impact and resolved automatically.
- Compliance evidence is continuously collected, reducing risk of penalties.
- Risk management is no longer reactive but continuously aligned to business priorities.

This approach allows organizations to quickly realize value—often within 90 days—while building toward long-term resilience. For enterprises seeking to modernize security operations, the combined ServiceNow and Tanium solution represents a future-ready foundation for cybersecurity excellence.

Cybersecurity Excellence: ServiceNow SecOps, IRM, & Tanium Endpoint Management

'ike (knowledge) level: Intermediate

Rev July 29, 2025

About Mana'o Pili↘

Mana'o Pili is a Hawai'i based technology consulting firm specializing in business automation through ServiceNow. Mana'o Pili provides its customers with individualized solutions. We reject the notion of one-size-fits-all solutions. Instead, we partner with you to craft a tailored plan that aligns with your unique needs, budget, and objectives. Our approach focuses on optimizing your existing platform while minimizing customization and reducing technical debt.

Here at Mana'o Pili, we treat our customers as 'ohana (family), listen closely to your challenges and deliver tailored attention with exceptional service.