Tanium Risk and Compliance – Robust endpoint security and compliance assured!

Value Proposition:

Tanium Risk & Compliance is part of a single, unified platform to manage risk and compliance at scale. It provides complete visibility into your endpoint risks and incidents of non-compliance, gives you the data you need to remediate exposures, and lets you consolidate multiple point solutions into a powerful platform. With Tanium, you will:

- Continuously monitor for vulnerabilities, sensitive data, and lateral movement risk across your entire estate in real time and at scale
- Prioritize remediation actions using issue severity, endpoint context, and peer comparisons
- Increase efficiency while reducing the chance of suffering a costly breach or regulatory fine

Ideal Customer Profile:

For Prospects/Customers who:

Had to deal with a security incident that involved exploitation of a vulnerability or compliance violation

Are concerned about risks from software supply chain (SBOM)

Need vulnerability and compliance coverage for servers and workstations

Have a C-Level strategic focus on improving security posture

NOT for Prospects/Customers who:

Have significant network, database, or web application scanning needs and are not willing to use a different product to address those needs.

Competitive Differentiators:

- A single solution that empowers SecOp and compliance teams to optimize their data security and risk efforts
- Provides a greater ability to slashes MTTR with integrated VM & Remediation than the competition
- The only VM solutions that swiftly discovers and remediates CVEs in third party software libraries – at runtime
- Fortifies compliance for all your endpoints with unparalleled efficiency and scalability!
- Reduces your attack surface by effortlessly finding, identifying, prioritizing and remediating sensitive data – all on a single platform

Compelling Stats:

93% of security professionals say vulnerability management is “very important” or “critical”

70% say their vulnerability management program is only somewhat effective (or worse)

On Average it takes 271 days for security teams to address just 13% of their known vulnerabilities

Customer Benefits:

Risk mitigation

Identify and address security vulnerabilities before they can be exploited by malicious actors.

- Find and address CVE across all endpoints
- Detect and address supply chain vulnerabilities
- Easily find and remediate sensitive data at rest

Operational efficiency

Optimize IT operations via integrated remediation on a single platform.

- Integrated remediation
- Feed vulnerability and compliance data into CMDBs such as ServiceNow

Enhanced visibility and reporting

Effectively see and trust prioritized vulnerabilities and compliance gaps.

- Automatic prioritization of vulnerabilities including CISA KEV
- Real-time risk data from managed and unmanaged endpoints

Modules Included in this Solution:

- **Comply:**
  - Continuous vulnerability and compliance assessments to evaluate and mitigate risk
- **Reveal**
  - Detect sensitive data at-rest on endpoints utilizing the speed and scale of Tanium
- **Integrity Monitor**
  - Satisfies compliance requirements and promotes proper change control via real time file and registry monitoring

TANIUM

Tanium Risk and Compliance – Robust endpoint security and compliance assured!

Discovery Questions:

- What are your goals & priorities specific to risk and compliance management across your endpoint estate?
- What groups are involved in the endpoint risk and compliance management process?
- What data compliance and regulatory requirements do you have to meet?
- How many different tools do you use for vulnerability management and remediation? Which tools?
- What tools and processes do you employ to maintain data compliance today?
- How do you drive consensus around gaps and what needs to be prioritized for remediation cross your organization?
- Can you identify and remediate software supply chain or SBOM vulnerabilities embedded in 3rd party libraries in your production software?
- What are the bottlenecks or barriers you encounter – is it the ability to identify and find CVEs and compliance gaps or is it change control/maintenance windows/coordination?
- How do you report on the status and effectiveness of your vulnerability & compliance management program to executives and the BoD?
- Which systems rely on accurate endpoint state data to make decisions? Which are your most valuable?

Objection Handling:

Objection:

What about endpoints that don't have a Tanium client?

Answer:

With Comply 2.0 - we can leverage the Discover modules NMAP capabilities to discover and enumerate other devices on net and surface any CVE's associated with those devices.

Objection:

Qualys, Tenable, Rapid 7 cover all vulnerability and compliance use cases for us - really similar to what Tanium does.

Answer:

Managing vulnerabilities and compliance gaps is more than just scanning your environment. You also need to consider how quickly and accurately you can remediate. Tanium enables you to find the vulnerabilities and compliance gaps that your existing tools find, but also fix them in seconds.

Objection:

My Qualys, Rapid7, BigFix is a platform that offers compliance, vulnerability, remediation, patching, endpoint detection and response, and even endpoint protection.

Answer:

You have many tools to help your teams monitor and remediate across the enterprise but with all those point solutions it's difficult for them to work together seamlessly.

With our platform, organizations can consolidate their disparate data from different point solutions into one unified view—allowing them to remediate across their environment without switching tools.

Common Use Cases:

- Maintain an accurate picture of all endpoint risk in your environment:
  - Scan all of your endpoints for vulnerability and compliance risks in minutes — not days or weeks — without creating significant network strain
  - Gather risk data from both traditional, managed endpoints
- Remediate risks across your entire environment as soon as they are found:
  - Seamlessly pivot between risk assessment and remediation by unifying IT operations, security and risk teams within a single dataset and platform
- Ensure regulatory and industry compliance:
  - Aggregate real-time scan data to improve preparation for audits and compliance assessments
- Take a risk-based approach to prioritizing and remediating vulnerabilities:
  - Quickly decide which CVEs to remediate first

Key Competitors:

Qualys

Requires a network tap, real-time scanning is resource intensive, use a 3rd party patch tool.

Tenable

No real-time remediation, need to switch tools to take action, scanning scheduled to lessen impact on environment.

Rapid7

Rapid7 scans can take a considerable amount of time ~30-40 minutes for each scan

TANIUM