DATA SHEET

Tanium Software Bill of Materials (SBOM)

Know your software supply chain vulnerabilities in seconds

The Tanium Software Bill of Materials (SBOM) feature utilizes a single Tanium agent to deliver real-time visibility into complex software environments, enabling your organization to make better-informed decisions around managing endpoint risk. After configuring Tanium SBOM, you'll know the details about every software application in your environment, and where any vulnerable packages exist. Ask Tanium SBOM a simple question, and you'll get an answer from across your environment — at scale and in just seconds.

Urgent questions need faster answers

We know that once a zero-day vulnerability has been identified, discovering all the instances on your endpoints using traditional tools can take two weeks or more. To be sure, it's a complex task involving:

- Knowing exactly where the software package is
- Knowing which open-source dependencies, if any, the application uses
- Knowing which version of the software package is running
- Determining whether any other applications use the software package
- Knowing all the above quickly and at runtime

Once a zero-day vulnerability is announced, such as a critical OpenSSL, your leadership will likely ask, "Are we impacted? Do we have software applications that use it? If so, where are they? And how quickly can we remediate them?"

You're on the spot to answer these questions quickly and accurately. But can you?

The average application-development project contains nearly 50 vulnerabilities spanning 80 direct dependencies, according to the Linux Foundation. While indirect dependencies are even harder to find, that's where 40% of all vulnerabilities are hiding.

Gain real-time visibility into complex software packages and better manage risk.

Visibility
Know every software package
With the click of a button, identify all runtime libraries, open-source freeware and software packages.

Control
Enable granular decisions
Make nuanced decisions based on real-time data and your organization's risk tolerance.

Remediation
Take action on your application list
Have flexibility in how you remediate items in ways that best suit your organization.

Shine a light on the darkest corners of your software supply chain. Replace runaway risk with visibility and control.

Know every software component at runtime.

Tanium SBOM currently supports parsing these ecosystems: Java, JavaScript, Python, PHP, Ruby, GoLang-Binaries and OpenSSL Shared Libraries, to help you determine which packages are present.

For example, once you identify Log4j or OpenSSL instances in your environment, you can also determine where it exists across your entire estate using various hunting methodologies. Even better, you can do all this from a single console.

- Be ready when the next vulnerability is reported. You'll have the data to both provide an answer, then fix the problem.
- Maximize your investments in other tools — such as ServiceNow — by pushing granular, accurate and real-time data into their fields.

Fix your software.

Once you get information about where the software packages are and which software applications are impacted, you can adjust that software, such as applying patches as needed.

Make decisions based on both your risk and all the granular endpoint data Tanium gives you. Determine whether you should stop using a device, kill all print spoolers, or just act on the list of known devices.

- Make decisions based on your organization's risk tolerance, and on what you know about your endpoints.
- Determine whether it's best to stop using a device, kill a process or print spooler, or remove an entire application – and be able to measure the impact of each option with granular usage data.

Protect your organization against supply-chain risks.

While we can't know what the next supply-chain vulnerability will be, you will have access to data about how your applications could be impacted. Then you can pivot to remediating the issue from the same console.

- Discover whether you need to stop using a device.
- If necessary, kill all specific processes, such as print spoolers.
- Act based on a list of known devices that are impacted.
- Patch the application.
- Deploy a new version of the application.
- Do all the above in real time.

Tanium Software Bill of Materials is a key component of Tanium's Converged Endpoint Management (XEM) platform.

The Tanium platform offers comprehensive IT operations and security management from a single agent. It delivers complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium XEM provides the visibility and control needed to help you continuously manage your organization's endpoint risk.

Request a demo today

Try Tanium Now

Tanium, the industry's only provider of Converged Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.