Tanium Comply

Perform industry-relevant compliance checks and vulnerability scans on demand

Zero-day vulnerabilities

Very few attacks exploit endpoints using advanced malware or zero-day vulnerabilities Instead, the most common opening is simple operating system or application misconfiguration. Most organizations have invested in point tools to address these issues, but those tools were built for an era with fewer endpoints and less complexity. Traditional compliance tools simply can't keep up.

At a Glance

Assess all endpoints against industry benchmarks and get up-to-date results on demand

Prepare for audits by aggregating assessment results

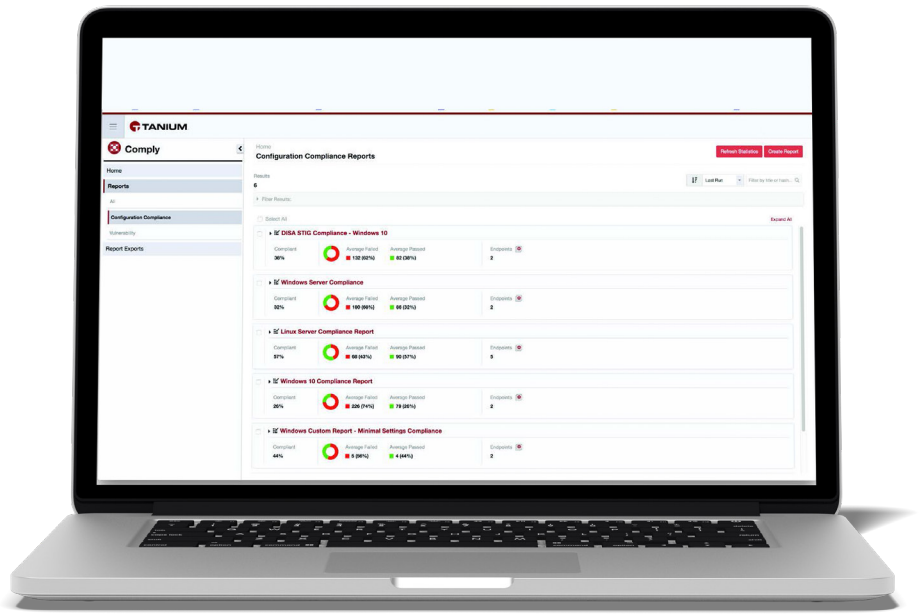
Support corporate mandates around proactive security across desktops, laptops, and servers

The Tanium difference

Tanium Comply conducts vulnerability scans and evaluates benchmarks and vulnerabilities against operating systems, network configuration, password policy, file permissions, and other standard security configurations. With data from Tanium Comply, organizations can improve overall security hygiene and simplify preparation for industry compliance audits.

Key Features

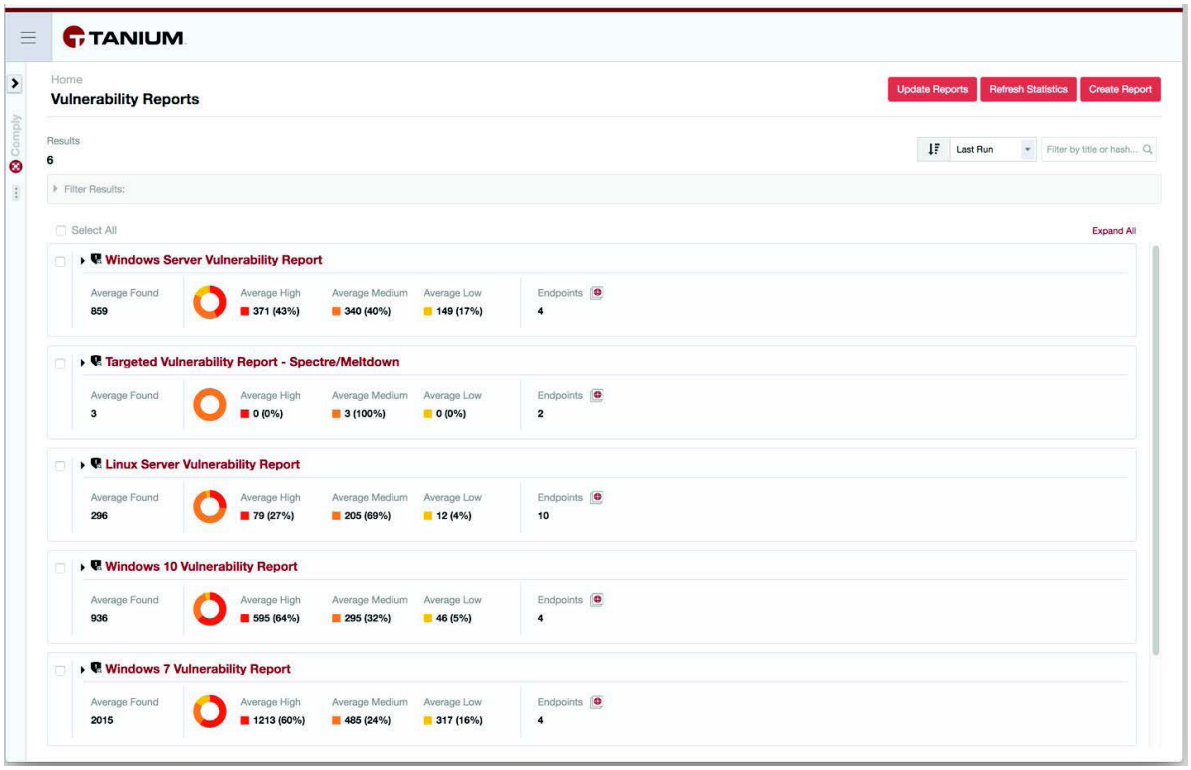
Evaluate endpoints against industry-standard benchmarks Tanium Comply works with standard, unbiased security configuration benchmarks and vulnerability definitions. These standards fulfill the system configuration hardening and vulnerability scanning portions of industry regulatory requirements and support corporate mandates around proactive security across desktops, laptops, and servers.



Run configuration compliance reports against established benchmarks.

Scan for vulnerabilities on demand

Check hundreds of thousands of endpoints for vulnerabilities. Tanium Comply supports the Open Vulnerability and Assessment Language (OVAL), the Common Vulnerabilities and Exposures (CVE) database and custom checks.



Run configuration compliance reports against established benchmarks.

Simplify audit preparation

With Tanium Comply, IT teams can gather assessment results from all systems and organize them so they are easy to present during an audit or during routine security hygiene inquiries. Organizations can use Tanium Comply to fulfill configuration hardening and vulnerability scanning portions of industry regulatory requirements, including PCI, HIPAA, and SOX.

Tanium platform power

Tanium Comply is built on top of the Tanium platform, which gives organizations complete visibility and control over their endpoints. The Tanium platform is designed to deliver all IT operations and security services—including asset inventory, file integrity monitoring, patching, threat detection and response, and more—from a single agent.

About Us

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With theunprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations

TANIUM