Tanium for Security Hygiene: Prevent attacks by addressing the root cause

IT Management and Security is fundamentally broken to address Security Hygiene

With more than 200 different products from 125 vendors to solve the top 20 security controls[1], there's not a shortage of tools. Information Security budgets increased 24% from 2014 to 2015, yet the number of security incidents during this time rose 38%[2] . Organizations are building arsenals of defenses yet the intruders are slipping through the digital doors and windows left open by the organization

According to the 2015 Verizon Data Breach Investigations Report, 99.9% of attacks exploited vulnerabilities that had been identified for more than a year, some of them as far back as 1999. Bolstering capabilities to detect and respond to such attacks is important, but it doesn't address the underlying weaknesses that allow them to succeed in the first place. Instead it's a challenge of basic cyber hygiene, from ensuring systems are up to date with the latest patches and software to understanding something as basic as how many computers are on the network.

Do you confidently know the answers to these questions?

- How many authorized and unauthorized software versions do I have installed across my network?
- Are all of my endpoints configured according to best practices and compliant with industry baselines/standards?
- How are we continuously assessing and remediating security vulnerabilities?
- Who has administrative access to my endpoints and do they need that level of access?
- Are my endpoints already compromised with malicious software or unwanted access?

If we don't want to get hacked, we need a new approach to this age old problem

It's obvious that the old approaches aren't working if organizations are still getting had. We see four main flaws with the current stale approach:

1. Out-of-date inventory management tools that only detect assets on the network and take days or weeks to complete the scan.
2. Endpoint security and management tools are often not deployed fully or healthy.
3. Vulnerability management and discovery point tools are limited in their ability to scan endpoints and often only take a sample.
4. Strict change control processes mitigate lack of confidence that take weeks to provide an incomplete view or weeks to collect.

In short, endpoint security hygiene and incident remediation need to go hand-in-hand. If a security operations team can take the post-mortem of a compromise and use it to enhance the baseline security of an environment, organizations will raise the bar for attackers and remain less susceptible to compromise.

How does Tanium enable continuous Security Hygiene?

Tanium's approach to security hygiene is different than the stale point tools in the market place. The current approaches look at the problem from the outside in. How will the attackers get into the network, where are we penetrable and how weak are we? Tanium's approach is inside out. We first identify what needs to be managed and secured within an environment. Organizations can then work to proactively secure every asset with the appropriate endpoint security, patches and security configuration controls. Only Tanium makes the inside-out approach reliable and cost effective - a key deterrent in the past - through unmatched speed, reliability, and completeness.

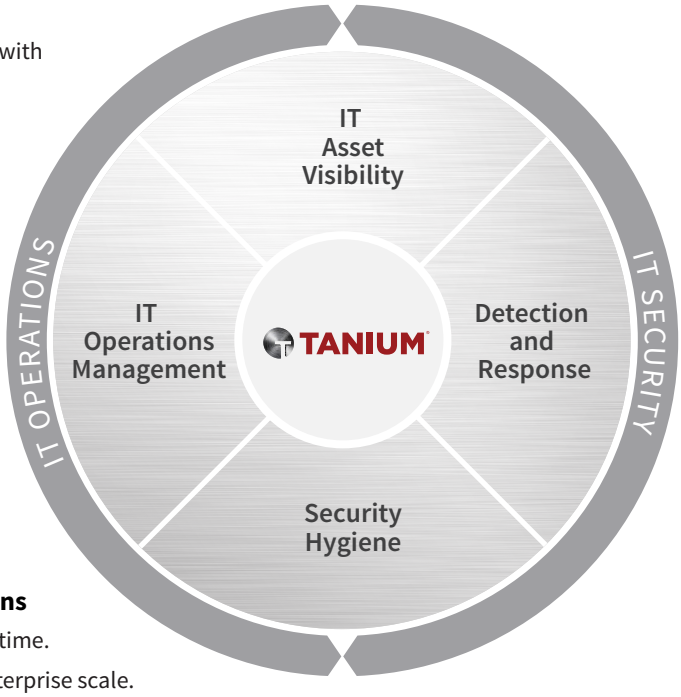
With Tanium Core Platform, customers can ask simple or complex questions about the current state of their networks. With 15-second responses directly from all their endpoints, they can take immediate actions to secure and manage all their assets.

With Tanium Product Modules, customers can extend the value of Tanium platform by replacing siloed point tools that discover unmanaged assets, identify unauthorized software, ensure configuration compliance and speedily patch operating systems and applications. Customers can also simplify their management stack and realize cost savings while increasing security, speed, and agility with a single agent.

[1] SANS Institute CIS Critical Security Controls
[2] PwC 2016 Global State of Information Security Survey

Reduce your overall risk exposure

- Detect unmanaged assets, find and close vulnerabilities in seconds with minimal overhead.
- Reduce the cost and complexity of maintaining an asset inventory.
- Instantly patch all your endpoints to improve compliance.
- Outrun the attackers and prevent future breaches by enabling continuous protections.



Gain game changing efficiency with 15-second visibility and control

- Manage your complex enterprise on-demand and boost productivity.
- Eliminate blind spots created due to costly and siloed point tools.
- Make open system configuration benchmarks actionable at enterprise scale.

Achieve consistency across millions of endpoint configurations

- Ensure administrative controls are on the right systems at the right time.
- Improve security posture by accurately assessing patch levels at enterprise scale.
- Provide confidence that critical security updates can be monitored and mitigated.
- Gather and aggregate assessment results for security hygiene management or compliance audits.

To learn more visit **tanium.com/products**