THE NEED FOR SPEED

HUNTING DOWN AND FIGHTING AGAINST EMERGING CYBER THREATS

TANIUM™

CONTENTS

EXECUTIVE SUMMARY

The evolution of cyber attacker techniques, skills and tools has far exceeded the pace of those of the cyber defender. Emerging threats continue to wreak havoc on enterprise networks, applications and data. Incident response teams must move faster, but the tools they've been given to do the job aren't fast enough in detecting, remediating and investigating incidents... especially at scale. While the "good guys" spend hours sifting through endless reams of log data, cyber attackers write and install malware that disappears within an hour, before teams can detect and eradicate it, and long after the damage is done.

A new approach is needed: one that enables IT operations and incident response teams to move faster and act smarter, across distributed networks and clouds, across OS platforms, and at scale.

In this paper, we'll explore the current state of cyber security – the good, the bad, and the ugly. We'll examine how Tanium delivers essential capabilities for incident responders to hunt down and investigate threat indicators rapidly and then take swift mitigating actions – within seconds, and at scale. We'll showcase real-world use cases to demonstrate how you can turn the tables on cyber attackers – at less cost, in less time, and more simply than ever before. And better yet, we'll show you how you can fight back.

THE CURRENT STATE OF CYBER SECURITY

The Good, the Bad and the Ugly

There are a number of security principles that have driven the industry for the past several decades. For a little while they worked sufficiently, but the game has changed quite a bit since then. In the abstract, many of these principles make sense. But in practice, the "Good" of these essential security principles have contributed to the "Bad" and "Ugly" place we find ourselves in the current state of cyber security.

Defense in Depth

Defense in depth has been an accepted core principle of cyber security for decades. The "belt and suspenders" concept is rather straightforward. You apply layer upon layer of security controls because no individual layer on its own is sufficient.

In abstract this makes sense. Especially since no single layer of security will work flawlessly 100% of the time. But in practice, it's a different story.

THE BAD: Complexity contributes to tunnel vision

Applying defense in depth in the real world not only results in significant complexity and cost, but often undermines the effectiveness of the security controls it inspired in the first place. In the interest of applying multiple layers of protection, security products have proliferated across endpoints, servers, networks, and databases. Typically these products are aware of only the context in which they find themselves, leaving the IT security professional with the complex work of stitching all of these perspectives together to see a common and unified view of the organization's security posture.

That's where SIEMs[1] come in. While SIEMs can provide that elusive "single pane of glass" visibility, constant vigilance and ongoing investments of time, effort, and resources are required to ensure they remain relevant. Moreover, SIEMs are dependent on the freshness and accuracy of the data they ingest. They're also not designed to remediate[2], adding additional lag time to incident response efforts.

THE UGLY: Isolated security controls

The challenge with defense in depth is that each layer doesn't necessarily build upon the one underneath it. In fact, defense in-depth adds unnecessary logical segmentation when unification and integration would likely strengthen each security layer. Isolated security controls coupled with product proliferation result in compromised security: there are more ways for attackers to find cracks in the crevices between and among the layers. What's more, the business is lulled into a false sense of security due to all of the existing investment, resources, and time deploying and managing individual security products.

[1] *SIEMs are security information and event management tools that take in multiple raw data feeds (typically event logs) from security tools and other systems with the goal of providing IT and security professionals with helpful information about threats in their environment or the state of compliance programs.*

[2] *91% of incidents studied in the latest Verizon Data Breach Investigation Report were discovered by external actors, rather than an internal tool like a SIEM. This provides strong evidence that SIEMs aren't quite living up to their promise of rapid threat detection, not to mention remediation. http://www.verizonenterprise.com/DBIR/2014/*

THE BAD AND UGLY: Sluggish incident response

All of this complexity slows down incident detection, response, and remediation efforts. Cyber attackers know this, and that's why their methods have increasingly evolved to slow and stealthy attacks, that blend techniques and targets. Hiding in and among these layers of complexity provides the perfect breeding ground for exploits, compromise, and data leakage.

Cyber attackers are inserting themselves into smaller and smaller "cracks" than ever before. According to the latest Verizon Data Breach Investigations Report[3], cyber attacks are moving exponentially faster than enterprises can detect and respond.

[3] *http://www.verizonenterprise.com/resouces/executivesummary/es_2013-data-breach-investigations_flyers_speed_attacks_en_xg.pdf*

The Bottom Line

The layers of defense that are logical to defenders are not aligned to how cyber criminals plan to attack your network. To be effective, a defense-in-depth security strategy must:

- ☑ Evaluate the real world ways an attacker would infiltrate your defenses and match controls to any areas of exposure.
- ☑ Improve your ability to detect, respond, and recover within seconds of outbreak and at scale.
- ☑ Work reliably and efficiently across large, distributed, and varied networks without impacting operations.

The Rise of "Stand-alone" Cyber Threat Intelligence (CTI)

As the cyber crime war continues to evolve, malware writers and exploit developers are now raising the stakes. For some high value targets, cyber attackers will develop malware variants and morphing code to bypass traditional security controls such as signature-based Intrusion Detection Systems (IDSes) and stateful inspection firewalls (more on the problems with signature-based defenses in the sidebar). Security vendors have risen to this challenge by investing in security research teams while enterprise IT security pros subscribe to dozens of RSS feeds evaluating the latest emerging threats, vulnerabilities, and data breaches.

These advances into understanding attacker techniques and tools are essential for today's advanced persistent threats. Rapid communication of threat information has advanced with the establishment of more sophisticated, standards-based Indicators of Compromise (IOCs) that encapsulate rich descriptions of the threats and incorporate logical and/or conditions between traditional signatures such as file names, registry entries and running processes.

THE BAD: Isolated threat intelligence

Despite these advances, there are many challenges with the current state of the cyber threat intelligence (CTI) ecosphere. While the emergence of standards for IOCs (e.g. STIX, Yara, OpenIOC) has produced machine digestible formats, enterprises lack the support within their security tools to truly unleash the value of CTI. Often the best intelligence remains isolated while potentially preventable attacks continue to take their toll. And while you may be able to integrate threat intelligence feeds with your SIEM tool, IDS, or firewall, they typically still remain isolated from your end-to-end security process.

THE UGLY: Disparity of data

Current CTIs are also "stand-alone" from another perspective. Despite the emergence of standards for IOCs, threat intelligence piles up in diverse, unstructured formats such as alerts from SIEMs, IDSes or emails that must be sifted through carefully, prioritized and translated into actionable intelligence. And without standards with which to measure the quality, relevance or credibility of intelligence sources, it's unclear how to prioritize. Organizations subscribing to multiple sources or participating in crowd-sourced options frequently find themselves overwhelmed and with a signal-to-noise ratio that is too high to be of any value.

> Today's threat landscape requires multiple sources of threat intelligence to be automated in order to be of any real value to the incident responder.

The Problem with Signature-Based Defenses

Custom code, morphing and disappearing malware are examples consistent with the current state of cyber attacks. According to a recent FireEye Report, 75% of unique malware samples were discovered in a single environment in their sample set. In their analysis of 2013 attacks, they found that 82 percent of malware binaries disappear within an hour.

These dynamic attacks go largely undetected by signature-based IDSes that rely on having a specific and static signature for every known exploit. A more dynamic defense tool would be one where you could use more than one variable to query and identify endpoints that may be compromised by these sophisticated attacks. For example, using one or more indicators with flexible analysis (e.g. applying and/or logic) provides a much more agile defense than a 1:1 signature would, considering that these threats are constantly changing.

Source: http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf

THE BAD and UGLY: Lack of automation

The volume of threat intelligence and the rate at which feeds are updated makes it nearly impossible for security professionals to keep up. And once an incident occurs, all attention is pointed to tactical response, recovery, and investigation. Today's threat landscape requires multiple sources of threat intelligence to be automated in order to be of any real value to the incident responder.

The Bottom Line

Incident responders and IT operations teams require integrated, automated, and actionable cyber threat intelligence. Without all three of these capabilities, cyber threat intelligence alerts, notifications, and other manually consumed content actually make life more difficult for the incident responder.

What do we mean by integrated, automated, and actionable?

- **Integrated –** Threat intelligence should be integrated holistically throughout your incident response process and overall toolset. CTI content should be integrated into your security tools like IDS, Firewall, SIEM, and AV but also your systems management infrastructure such as patch management, configuration management, and software distribution. Recovery speeds up when you don't have to stop to switch tools.
- **Automated –** Automated hunting for Indicators of Compromise (IOCs) against your existing environment (platforms, applications, devices, and other variables) provides the speed you need for effective hunting and defending. Once an IOC discovered, it's essential to implement remediation tactics at scale. The most important capability for the incident responder is to ask any question of the environment, because threats are constantly morphing, and your attack surface area is changing at the same time.
- **Actionable –** The goal is to see CTI content that's relevant for only the devices, applications, and platforms that are on your network. If it's not relevant, it's not actionable. In addition to relevance, the CTI content should provide enough intelligence to make it actionable. But it doesn't end there. In today's complicated enterprise networks, it's not only knowledge that matters but also agency. Pursue a CTI strategy that enables a path to execute defensive tactics, like automated detection and remediation, not just security research for its own sake.

The most important capability for the incident responder is to ask any question of the environment, because threats are constantly morphing, and your attack surface area is changing at the same time.

Network-centric Security Mindset

Despite the fact that we've all agreed the perimeter disappeared years ago, we still suffer from this legacy mindset. Network security investments continue to grow at a faster rate than other segments of the security industry. Building stronger and taller walls between an enterprise network and public networks like the Internet may make you feel like you're doing something to secure your enterprise. The problem lies in the failure to recognize that the rules of the game have completely changed.

With the rise of cloud computing, virtualization, and an increasingly mobile workforce, enterprise IT security teams would significantly benefit from moving their focus, attention, and investment from a network-centric perspective to a data-centric one. To be honest, the idea that an attacker will always follow the path of the choke points you've set for him is naïve.

The reason that most organizations have not moved to a data-centric security model is because they have never had access to tools that are able to operate with the same speed, precision and control on endpoints as they do on network devices. After all, the scale of the problem is so large, and the amount of information you need is detailed, voluminous, highly unstructured and constantly changing.

The legacy database technology that powers most security and systems management tools cannot keep pace with the amount and diversity of endpoint data to process. Even worse, this technology wasn't designed to support ad-hoc and unstructured questions. And yet, immediate answers to ad-hoc and unstructured questions are precisely what today's incident responder needs. Emerging threats are customized per industry, per target. They morph as they move through networks. The ability to ask any question, receive answers in seconds, and then execute remediation seconds later is what's needed to fight back.

That's exactly what the Tanium Platform delivers.

The Need for Speed

The ability to maintain a hold on the data and the hundreds of thousands of devices where it lives (and moves between) lies in one key factor: speed.

Up until recently, there hasn't been a way to "reach out and touch every endpoint" on a network (or cloud for that matter) in any degree of expediency to be useful to IT security operations. A database scan initiated from your systems management tool or the latest vulnerability report might find a few weak links, but it won't likely find them all in seconds. Or enable you to fix them seconds later. And yet, that's the speed at which malware moves through your network.

That's why this level of speed is essential for the incident responder, but remains elusive when relying upon traditional client-server architectures and legacy databases.

[4] *A Forrester Research Survey found that 46% of respondents intended to increase their network security investment in 2014. The survey also found that network security claims the largest single portion of the overall IT security budget. Source: http://www.zdnet.com/network-security-spending-to-surge-in-2014-7000024948/*

To be honest, the idea that an attacker will always follow the path of the choke points you've set for him is naïve.

The Bottom Line

It's much easier to apply security controls to choke points on a network because there are so few of them and they're relatively static. Unfortunately, this approach is no longer sufficient to combat today's sophisticated and dynamic threats.

Staying Ahead

To stay ahead of emerging threats, incident responders and IT security teams should consider a data-centric security model. And to keep pace with the speed of these attacks, IT security teams need a tool that can touch every endpoint in seconds to:

1. Find out information about its configuration and the data it holds.
2. Make any necessary changes to protect that data.

Additionally, this data-centric friendly tool must also work across skinny networks with high latency across geographically disperse areas without impacting operations. Sounds impossible, but it's not. Keep reading.

TANIUM EMERGING THREAT DEFENSE

The Essential Tool for the Incident Responder

When it comes to successfully defending against today's dynamic attacks, a revolutionary approach to incident response is sorely needed. IT security pros and incident responders need to find and fix exposures faster than ever before, across mixed networks and systems, without compromising precision or control. And all of this must happen without breaking the budget, or the network.

Legacy client-server architectures, single-purpose security products, emerging endpoint threat detection and response tools, signature-based detection, and other traditional approaches all fail to hit the mark. They are too slow, too complicated, too imprecise, and increasingly unreliable at scale. Not to mention the fact that they're very expensive to deploy and manage over time.

Tanium transforms threat detection and response by overcoming the speed bumps and visibility gaps inherent in defense in depth. By automating and integrating cyber threat intelligence, and delivering precise and granular endpoint threat detection and remediation at network speeds, Tanium delivers the speed, scale, and simplicity that incident responders need to hunt down and defend against emerging cyber threats.

Rich Endpoint Data at Network Speeds

By applying automation to the threat detection, analysis, and remediation process, Tanium allows incident responders to react to incidents within seconds, reducing cost and risk at the same time. As we mentioned in the previous section, a defense in depth strategy in practice results in complicated layers of products that don't work together, slowing down incident response and leaving blind spots in your security infrastructure.

While many of these single purpose tools or "layers" have provided some insight into emerging threats, they fail to provide the end-to-end coverage necessary to detect and recover from these threats.

Today's incident responders need technologies that can capture granular endpoint data across distributed networks, within seconds, and without impacting operations. Pivoting from one piece of data to the next needs to happen in seconds to zero in quickly on the threat, its impact, and its scope. Additionally, once issues are discovered, remediation needs to happen just as quickly. At scale, and again, without impacting user productivity or network performance. And Tanium is the only solution available that can deliver on that promise.

Tanium transforms threat detection and response by overcoming the speed bumps and visibility gaps inherent in defense in depth, delivering the speed, scale and simplicity that incident responders need to hunt down and defend against emerging cyber threats.

Customer Spotlight: Altering the Time Scale with Tanium

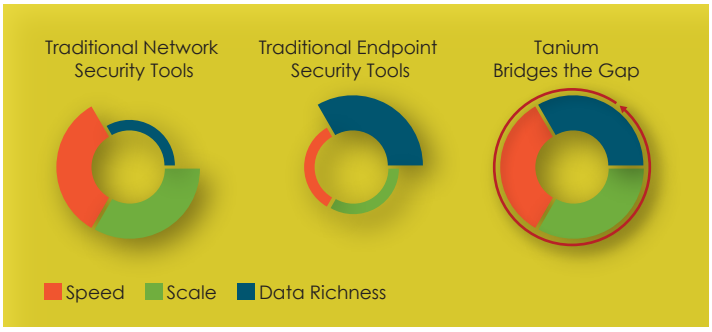
The IT security team at a large global retailer was concerned that they might be vulnerable to the same malware that was used to steal data from UPS[5]. When they tried to use their existing toolset to scan for systems that were vulnerable, they weren't able to verify the vulnerable systems with certainty, and each scan was taking a few days to complete. They quickly installed Tanium, and were able to determine in seconds which of their 100,000 machines were vulnerable. Seconds later, those 20,000 machines were issued patches, and all machines received the correct DAT files for their AV system to identify the malware. Additionally, as soon as new machines came online, they automatically received the updated DAT file from the peers in their network. Tanium altered the time scale for this IT team by enabling them to move from days to seconds.

The following table compares Tanium's capabilities with established classes of tools attempting to close the current gap in endpoint threat detection and response for the distributed enterprise.

	ANOMALY BEHAVIOR DETECTION	THREAT INTELLIGENCE DETECTION	INCIDENT RESPONSE	FORENSICS AUTOMATION	REMEDIATION
TANIUM	●	●	●	●	●
ALTERNATIVE TOOLS:					
SECURITY LOGGING & ANALYTICS	●	○	○	○	○
ENDPOINT FORENSICS	○	○	◑	●	○
NETWORK FORENSICS	○	◑	◑	●	○
SANDBOX FORENSICS	●	●	○	●	○

Based on a resilient, linear peer-to-peer communications topology[5], Tanium bridges the speed and visibility gap between network security and endpoint data, by providing deep endpoint data at network speeds. No matter what the OS or where the endpoint resides, Tanium provides instantaneous threat detection with rapid remediation at scale.

Tanium bridges the operational security gap with rich endpoint data and precise control, at network speed and scale.



[5] More information can be found on Tanium's linear peer-to-peer communications topology in the "How it Works" section of this paper.

AUTOMATED, INTEGRATED, AND ACTIONABLE CYBER THREAT INTELLIGENCE (CTI)

As we mentioned earlier in this paper, CTI content is at its most valuable when it's automated, integrated, and actionable for your organization. Tanium optimizes the investment in your security ecosystem and CTI subscriptions, by enabling you to focus on only those IOCs that are relevant to your organization. With its IOC Funnel, Tanium can take in multiple feeds from a variety of CTI sources, and use that data to detect emerging threats across distributed networks within a matter of minutes. In fact, Tanium supports a wide variety of IOC formats including: OpenIOC, STIX, and YARA.

With this integrated capability, incident responders and security analysts can easily import thousands of standardized IOCs, as well as share these IOCs and any results of instantaneous IOC scans. Tanium evaluates and translates IOCs into optimized sets of questions, allowing multiple IOCs to be evaluated within a single scan, reducing operational impact and accelerating threat detection. Once these threats are identified, Tanium enables automated remediation at scale, no matter how large, distributed or varied the environment.

Tanium's IOC Funnel overcomes the limitations of traditional and static signature-based defenses, by ingesting and processing rich details about threat indicators, including applying "and/or" conditions to traditional signatures such as file names, registry entries, running processes, and other dynamic variables. This approach accommodates the varied and dynamic aspect of today's blended threats, as well as maximizes the effectiveness of existing security investments.

Tanium's unparalleled speed with asking questions at scale and getting rapid answers powers the iterative nature of the incident response process. By accelerating the ability to evaluate the results of IOC scans, incident responders can quickly pinpoint compromised systems, containing outbreaks before they spread out of control. Security analysts can quickly fine-tune IOCs to filter out the bad ones that produce too many false positives. Once the initial incident has been contained, security analysts can run scheduled scans of IOCs for future threat identification. Additionally, IOC scan results can easily be integrated with existing security information and event management systems (SIEM) for historical analysis and reporting.

Not only does Tanium enable CTI to be actionable, but it also accelerates the implementation of those actions faster than any other tool available.

Customer Spotlight: Racing Against Time with Tanium

A large global retailer was struggling to pinpoint and resolve a malware outbreak they discovered in one of their South American offices. Out of 15,000 endpoints connected to that office, they guessed that 2,000 were infected, and their IT security team struggled to contain the outbreak. They were in a race against time, and their existing toolset had a stalled engine.

They had two key operational challenges working against them. First, this was a new piece of malware, which meant they were waiting for an updated DAT file from their AV vendor. And the other was the highly constrained, highly latent network links connecting them to the region. Their existing solution wasn't flexible enough to evaluate IOCs containing mutexes to identify infected machines, so they turned to Tanium.

With Tanium, they were able to verify the infected machines, quarantine them, make registry repairs to roll-back the threat temporarily and then push out an updated DAT file once it was released from their AV vendor. With their existing remediation solution, pushing out a 150MB file across those constrained network links would have failed. Thanks to Tanium's resilient, linear peer-to-peer topology, each DAT file reached its destination without error. Tanium also automated a forced AV re-scan to put these protections into place immediately. Additionally, as new machines came online, they automatically received the updated AV DAT file from their peers, saving network bandwidth, and eliminating future windows of vulnerability.

Tanium's unparalleled speed with asking questions at scale and getting rapid answers powers the iterative nature of the incident response process.

ITERATIVE, AD-HOC Q&A DRIVES AGILE INCIDENT RESPONSE

Customer Spotlight: Speedy Pivoting Leads to Success

A global financial services firm has long recognized the benefits of running their IT security team members through Red Team vs. Blue Team exercises. They know that the best way to discover their own security weaknesses is to have their best and brightest take a turn at playing the role of an attacker, as part of the Red Team.

During their latest exercise, the Blue Team defenders had a new tool in their arsenal – Tanium. Using Tanium, they were able to pivot quickly from question to question thousands of times faster than ever before. Each question returned answers in seconds, enabling them to zero in on the compromised systems with just a few pivots, and implement remediation minutes later. This was the first time that a Blue Team ever successfully defended against a simulated attack, and the last time they'll ever think about trying this competition without Tanium in their toolbox.

One thing that's true about incident response is that you never know what you'll need to know when a serious data breach occurs. But it's a universal truth that you'll have a LOT of questions once you first discover a potential threat, compromise, or exposure. In fact, at the start of an investigation, you'll have far more questions than answers, and each new answer will of course produce even more questions. Pivoting from data point to data point, or from one "clue" to the next, is the way incident response gets done. The quicker you can pivot, and the faster you can ask and get answers to iterative, unstructured questions[7], the quicker you can fix the problem.

Typically, you won't be able to predict what sorts of questions you'll have during an investigation so you need to be able to ask any question. Since you can't predict which systems attackers will target or when, you need to be able to ask any endpoint, any question, any time.

Tanium simplifies and accelerates incident response by enabling IT security teams to ask any question - in basic English – about their endpoints, no matter what OS or where these endpoints are located, and receive answers in seconds. What's more, IT security teams can automate remediation actions across hundreds of thousands of endpoints, around the world, minutes later.

[7] There are of course some basic, general questions you'll always want to be able to answer about your security posture. Things like "who is connecting to my network" or "which user accounts have privileged access" or "who has Microsoft Office installed". Those are good questions, and you need answers to them, but they are not the ones that pop up during real-world investigations and incident response. Thankfully, you can use Tanium to answer any of these questions as well. And you'll get answers just as quickly.

Since you can't ever predict which systems attackers will target or when, you need to be able to ask any endpoint, any question, any time.

TANIUM OVERVIEW AND HOW IT WORKS

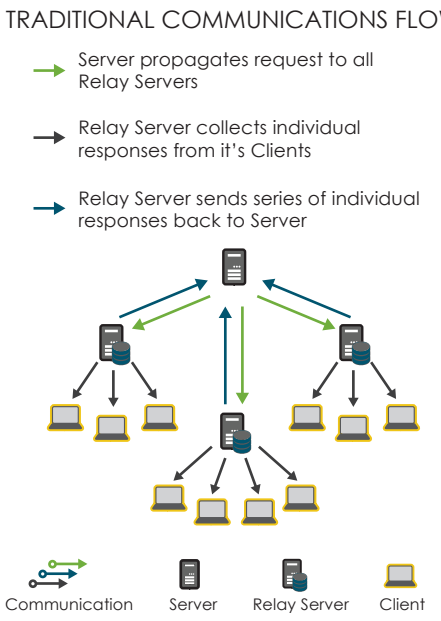
Tanium breaks through the limitations of legacy technologies to deliver the "next generation" of endpoint threat detection and response capabilities required by the distributed enterprise. Tanium provides instant command and control - at scale - across some of the largest enterprises in the world. Based on a resilient linear peer-to-peer topology, Tanium is able to deliver unparalleled speed, precision and control so that IT security pros and incident responders can respond and remediate threats in seconds, and at scale.

Only Tanium lets you ask virtually any question of any endpoint at any time and pivot through 10's of 1000's of potential analytical positions within seconds. And no scripting is required. So you get complete visibility – even into the hidden corners of your enterprise where emerging threats hide, wait for the next opportunity to bypass one of your defense layer and "slip sideways" to gain an increasingly dangerous foothold deep in your corporate network.

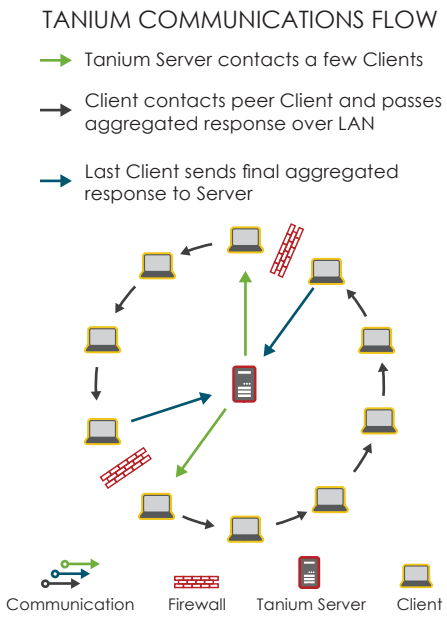
Unlike other enterprise technologies, Tanium doesn't rely on a centralized, hierarchical server infrastructure to provide data collection, aggregation, and distribution functionality. Tanium is based on an incredibly efficient, linear peer-to-peer architecture designed for fault tolerance, transient endpoints, and the global WAN segments typical of today's enterprise.

Through a lightweight and optimized agent, Tanium distributes management intelligence and data directly to the computing devices themselves. This key innovation results in radically faster, more accurate, scalable, and more adaptive security than traditional solutions. Delivering the highest value at the lowest TCO, a single Tanium server can manage over 500,000 endpoint devices, resulting in a level of resilience and efficiency not possible with alternatives. The following diagrams highlight these key architectural differences.

TRADITIONAL COMMUNICATIONS FLOW



TANIUM COMMUNICATIONS FLOW

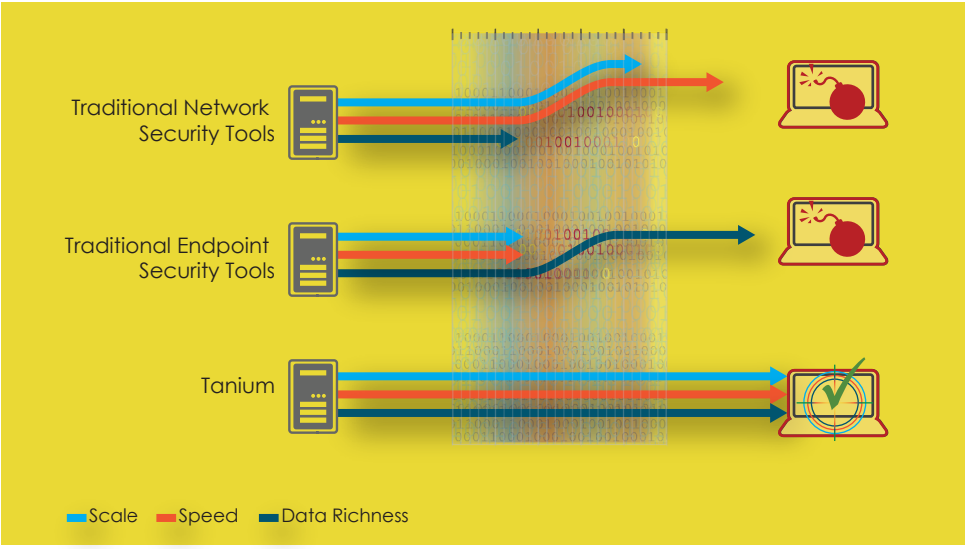


THE KEY TO SPEED: TANIUM'S LINEAR P2P ARCHITECTURE

It's important to spend some time explaining how this architecture works under the covers, since it's the key to Tanium's unparalleled speed. The Tanium Client is installed locally to each managed computer, and periodically contacts the Tanium Server to register and gather details about neighboring computers on the network. Based on this information, the Tanium Clients automatically identify the best peer devices from which to receive and to forward data.

Clients are then able to keep the network intact through aggressive routing around Clients that are removed or are unable to communicate effectively, fast addition of new Clients that come online, and the ability to utilize the Server to "reflect" around network-level blockages such as firewall blocks in core backbone routing. The result of the process can be imagined as a "ring" of Clients, with each Client having a single peer Client that is feeding information to it, and a different Client to which it is feeding information. A Tanium linear peer ring can scale to hundreds or thousands of Clients.

Because of extensive optimization in the Client communications architecture, allowing single messages to be transmitted to hundreds of thousands of clients in a matter of seconds, the linear peer to peer rings can deliver any new piece of information—to every Tanium Client in the environment in less than a minute, regardless of the network scale. Furthermore, because the messages being transmitted through the rings are quite small, the platform can answer approximately 100 questions per second without any appreciable load on the server, the assets themselves or the network infrastructure.



TANIUM PLATFORM COMPONENTS

Accessed through a web-based console, the Tanium platform relies on two primary components to ask virtually any question of any endpoint and then deliver actions based on those answers. Within seconds.

- **Sensors –** Sensors are simply scripts written in a variety of non-proprietary languages. Tanium customers can easily customize these for any ad-hoc questions they have, and capture the answers globally, across OS platforms, in seconds. Tanium delivers over 800 core sensors out of the box. And since most sensors contain multiple data points and many can be combined, filtered, sorted, and parameterized from a simple natural language UI, Tanium literally lets you ask an infinite number of questions out of the box without ever having to write even a single script.
- **Packages –** Packages are the actions that you want to take in Tanium. They are composed of commands that you want to issue, as if you were sitting at the command-line of the machine, and any files that need to be distributed for those commands to run, including tools, patches, application updates, new software, or service packs.

A lightweight and scalable infrastructure enables the delivery of the above content. This includes the Tanium Server, a multi-purpose Client, a web-based Console, and an optional Zone Server to reach all endpoints no matter where they roam.

Tanium Server – An application server in the traditional sense, the Tanium Server manages client registrations, provides Clients with environmental perspective, signs Sensors (questions) and Packages (actions), and performs other security configuration tasks.

Tanium Client – Once installed on each managed device (Windows, Mac, Linux, and Unix), the Client initiates traffic between itself and the Tanium Server (registration), between itself and its peer Clients (neighbors) to exchange and answer questions and distribute packages which have a valid signature.

Tanium Console – A web-based application to easily ask questions, display answers, and take actions based on the security configuration of the Tanium Server.

Tanium Zone Server – An optional component, the Zone Server enables roaming devices to remain in contact with the Tanium Server. A small, lightweight service, the Zone Server is typically installed to one or more existing devices within an organization's DMZ. As long as the remote computer has an Internet connection, the Tanium agent can answer questions and perform targeted actions as if it were connected to the network.

TANIUM EMERGING THREAT DEFENSE

To kick-start their incident response program, organizations may choose to implement Tanium Emerging Threat Defense, a solution pack of IR-specific Sensors, Packages, Dashboards, and other product extensions such as the SOAP API, IOC Funnel and the Connection Manager to integrate with your existing security ecosystem for complete threat detection, analysis and response.

Key Benefits of Tanium Emerging Threat Defense

SOAP API – Using the SOAP API, an organization can expose the full functionality of the Tanium Console to any other system that can issue a SOAP request and consume the response. The query and action events deployed through the SOAP API provide the same role-based restrictions as users working directly from the console, so visibility and management can be carefully controlled even when integrated into external systems.

Tanium IOC Funnel - The Tanium IOC Funnel was developed to allow security analysts to import IOCs easily and use Tanium's speed and precision to evaluate hundreds or thousands of IOCs on all of the endpoints in a large enterprise. The IOC Funnel can convert multiple IOCs into an optimized set of questions. This optimization minimizes the overhead of IOC scans and allows Tanium to evaluate multiple IOCs efficiently in a single scan to accelerate incident response.

Tanium Connection Manager - The Tanium Connection Manager provides a flexible and powerful framework to automate the integration of Tanium with other systems within the enterprise, as well as interactions with other APIs and services. Through a simple interface that requires no scripting, administrators are able to "string together" rich endpoint data surfaced through simple Saved Questions with one or more connections to back-end systems, data processing tasks, or other services. This simple framework empowers teams to easily share endpoint context with out of the box connectors to SIEMs such as Splunk, HP ArcSight, and IBM QRadar, discover and compare new behavioral data to threat feeds, drive new data to big data analytics tools, or share audit and inventory data with CMDBs. This ability to easily link together configurable Connectors allows the Connection Manager to provide an extensible engine to automate security response activities and work-flows, accelerating and empowering security and operations team's analysis, response, and verification efforts.

SUMMARY

When it comes to cyber security, it's an arms race between the attackers and the defenders. Those who will be successful in protecting an enterprise's data will be those who can move as quickly as possible - whether that's in identifying the initial threat, or recovering from an incident.

With Tanium, incident responders can hunt down, investigate, and recover from incidents within seconds, reducing risk and cost – no matter how large, complicated or distributed the network. This level of speed and agility is absolutely essential to protect networks, systems, and data from the latest cyber attacks.

NEED MORE INFO?

Please contact us today at sales@tanium.com. We'll provide more information on how Tanium can help you rapidly hunt down and fight against emerging threats for a truly revolutionary approach to IT operations and security. You can also find product overview videos and other resources on our website at www.tanium.com.

ABOUT TANIUM

Tanium was founded in 2007 by a team with extensive experience providing security solutions and systems management capabilities to Fortune 500 customers. Having worked closely with some of the largest, most carefully managed enterprises in the world, Tanium's founding team understands the specific challenges and constraints that must be addressed to keep large network environments running smoothly.

Tanium allows enterprises to manage, secure, and maintain the endpoints across their entire network. It enables enterprises to ask questions in plain English; identify and diagnose problems as they occur; and instantly interrogate, update and secure nodes.

1625 Shattuck Avenue, Suite 200 Berkeley, CA 94709
info@tanium.com www.tanium.com

91514-SWP