Vendor Profile

Tanium's Star Set to Rise on the European Market

Mark Child Duncan Brown

IDC OPINION

Tanium has been an established player on the North American endpoint protection market for some years, but until recently has had only a limited presence in Europe. That is now changing as the vendor builds out its personnel and partnerships in the region. However, organizational presence is only one part of the puzzle: Tanium takes a rather unique approach to protecting its customers' infrastructure and is investing heavily in its technology, extending and enhancing its capabilities to create a compelling and differentiated offering for the market.

IN THIS VENDOR PROFILE

This Vendor Profile looks at the development of Tanium, with a specific focus on its expanding presence in Europe, as well as the development of its solutions portfolio.

SITUATION OVERVIEW

Introduction

The endpoint security market is a crowded field, populated by enterprise-scale incumbents, infrastructure and security platform giants, innovative next-generation disruptors, consumer-segment specialists, mobile endpoint security specialists, and numerous other combinations and variations of the above. To compete in this market, players need to differentiate themselves and provide a unique value proposition, and Tanium has worked hard to ensure it is able to do both of those things.

Company Overview

Tanium was founded in 2007 and has seen strong growth, particularly over the last five years, fueled by successive rounds of financing. The vendor reported $175 million from TPG Growth in 2018, an investment from Salesforce Ventures in June 2020, and a further sale of common stock in October 2020 that generated $150 million. These investments bring the reported total raised by Tanium to more than $900 million and have increased the company's valuation to over $9 billion.

Tanium is growing strongly at a global level: in its financial year 2019, the vendor achieved 50% year-on-year revenue growth, to reach $430 million. The company also grew its workforce by 50% year on year, to around 1,500 employees. According to IDC data, Europe accounted for approximately 10% of that revenue in 2019, and that share is growing.

Company Strategy

Product Strategy

Linear Chain Architecture

Tanium's products are based on a unique approach to asset discovery, called linear chains. A linear chain is a peer-to-peer relationship between entities (typically servers, PCs, and workstations) on a network segment. Rather than a central server polling each entity individually, which is bandwidth-consuming and inefficient, a single request is fed to one entity on the segment and the answer, together with the original request, is passed to the next peer entity in the chain. This process continues to the end of the chain, and the aggregated set of answers is passed back to the originating server.

With some adaptations, this approach works not only in centralized office and datacenter locations but also in distributed environments such as branch networks, and even in cloud deployments.

The benefit of this approach is that complex requests, such as inventory, patch application, and configurations, can be determined in near-real time, providing an up-to-date view of an organization's estate on demand. Results are delivered in seconds, revolutionizing an organization's ability to know its current state – including security posture – at any given time.

Product/Service Offerings

Tanium has developed its product and solution portfolio to address two core areas: endpoint security and endpoint management. This immediately puts it in an interesting space, as there are few endpoint security vendors that also have robust endpoint management capabilities (Ivanti is the closest competitor). With the acceleration of digital transformation (DX), device proliferation, increasing infrastructure complexity, and an expanding attack surface, the ability to provide functions such as patch management and configuration management in concert with threat detection and endpoint security controls can bring considerable benefits to both enterprise operations and security.

Tanium's Platform groups solutions within two main packages – Endpoint Management and Endpoint Security and Risk. Endpoint Management comprises the following solutions:

- Asset discovery and inventory
- Configuration management
- Patch management
- Performance monitoring
- Software management

Endpoint Security and Risk includes:

- Asset discovery and inventory
- Data risk and privacy
- Incident response
- Vulnerability and configuration management

Through these solutions, Tanium aims to provide visibility and control over Windows and macOS devices, as well as servers (e.g., Linux, Unix, Windows), cloud and virtual environments, and containers. Tanium's platform is built to deliver all functions and capabilities from a single lightweight agent (the Tanium agent has a 64kb footprint). The Tanium client provides comprehensive visibility over endpoints, as well as the ability to initiate actions on or for those endpoints, such as patching, compliance, inventory, and incident response.

Tanium's solutions are made up of multiple modules, which constitute the building blocks of the Tanium Platform. While an exhaustive summary of the Tanium portfolio is beyond the scope of this study, notable among the key modules and components are:

- **Tanium Asset:** Maintaining a comprehensive and up-to-date inventory of hardware and software assets across the enterprise environment ought to be a straightforward undertaking for all organizations. The reality is that this can be incredibly challenging, particularly for large enterprises with distributed workforces and infrastructure, huge numbers of devices, and proliferating systems and applications often operated by semi-autonomous business units. Tanium Asset automates and simplifies asset reporting, providing real-time data about IT assets to IT operations teams, regardless of location.
- **Tanium Discover:** Addressing the security truism that you cannot protect what you cannot see, Discover can scan networks with hundreds of thousands of endpoints in real time, to find unmanaged assets in the environment. If unmanaged devices are found, administrators can

either deploy the Tanium agent on those endpoints to bring them under management or block them from the network. This is a key component of Tanium's Endpoint Management approach, the foundation on which it can then enable everything from asset inventory, patching, and configuration management to performance monitoring and software management.

- **Tanium Enforce:** Enforce is a key component of Tanium's Configuration Management solution, which is part of both the Endpoint Management and Endpoint Security and Risk packages. Enforce allows customers to manage and secure end-user, server, and cloud endpoints from the Tanium console. Key capabilities of Enforce include Windows policy management, application control (including both blacklisting and whitelisting), firewall management, antivirus management, drive encryption, and remediation enforcement (including remediation of compromised endpoints, enforcing desired state, and continuous endpoint monitoring to prevent repeat compromise).
- **Tanium Impact:** New in 2020, Impact is a visualization and management tool to address access rights and relationships across the enterprise. Impact maps privilege interdependencies in order to uncover potential lateral movement pathways caused by complex directory structures and inadequate privilege management processes. Impact allows customers to visualize, contextualize, and prioritize overly permissive administrative rights, leveraging a quantitative assessment of asset risk. These can then be remediated through the Tanium Platform.

Another major development in 2020 was the launch of Tanium as a Service. This negates the need for a central on-premises server, with all queries being handled from a cloud-based server. An agent on each endpoint is still required.

In 2020, Tanium also rolled out **Blue Star**, a complete rebuild of its user interface (UI). Prior to Blue Star, the vendor had not invested in its UI for a few years, which naturally leads to erosion of performance and user experience as components and capabilities are added or evolve over time. For end users, simply taking too many clicks to reach an objective represents inefficiency and can cause frustration. Tanium extensively reviewed its old UI and, with Blue Star, updated every single page of its Platform. Key content is always "above the fold" (i.e., immediately visible) on every page, and all key information is on the home page — which is also customizable. The UI has two main dropdown menus: Modules and Admin. It is important not to show information and then leave the user at a dead end, so everything is clickable. For example, administrators can click "Unmanaged Network Interfaces" and it shows them all in the Discover module. Blue Star also includes a query tool, Explore, which uses natural language processing, and a Quick Links function that is customizable and works within individual modules.

As Tanium strives to expand its customer base in the midmarket, it will increasingly serve organizations with limited security teams that need intuitive tools — and more help. The vendor has focused on ensuring that behaviors and controls are as consistent as possible across all modules. Among the next steps planned for development of its UI are the addition of trend evaluations and visualizations to all modules, as well as the possibility to add components for individual modules to the homepage as needed.

In 2021, Tanium will launch its risk module. This builds upon Tanium Impact, which determines key relationships between entities and the organization (e.g., the CEO's PC) and Tanium Reveal, its e-discovery module. Risk measures are mapped primarily onto the National Institute of Standards and Technology (NIST) framework, but General Data Protection Regulation (GDPR) and Center for Internet Security (CIS) controls are also supported. The ability to determine security status in near-real time and to determine priorities in a timely fashion will add substantial value to organizations with complex infrastructures. A key challenge for such firms is to answer such simple questions as: Have the latest patches been applied to my entire estate and can I prove this to an auditor? With Tanium's risk module, organizations will be able to answer this question in seconds.

Business Strategy

Partnerships and Alliances

- Tanium as a Service is available on the **AWS** Marketplace.
- Tanium has an established integration with **Cisco**, via the latter's pxGrid platform, to provide automated threat control and containment. Through integration of Cisco's Identity Services Engine (ISE) and Tanium's endpoint agent, the companies are able to provide dynamic access control for endpoints and ensure continuous compliance.
- Tanium has also integrated its unified endpoint management platform with **Cloudflare Access** to secure access to corporate devices and applications.
- In August 2020, Tanium announced a partnership with **Google Cloud** to help organizations secure their increasingly distributed business operations. The new offering, an integration between Tanium Threat Response and Chronicle, Google Cloud's security analytics platform, enhances Tanium's ability to detect and investigate advanced persistent threats (APTs).
- In November 2020, Tanium announced a partnership with **IBM** to enable security and compliance monitoring for hybrid cloud environments, particularly for heavily regulated industries such as healthcare, financial services, and government. Previously, IBM had been a competitor for Tanium with its IBM BigFix endpoint management platform, but with the divestiture of that asset in 2019, it opened the door for cooperation with Tanium. Together, the two companies aim to provide a consistent approach for real-time visibility, security, and compliance in hybrid cloud environments.
- A new key focus for Tanium is IT service management (ITSM). In this respect, it is building a partnership with **Salesforce**, to capitalize on Tanium's ability to provide visibility into IT assets and performance. Salesforce can provide insight into employee activity within their organization using its Work.com IT service management tool, while Tanium can speed up the remediation cycle for technical problems.
- In February 2020, Tanium and **vArmour** announced a global strategic partnership to improve visibility and control for enterprise applications. vArmour specializes in Continuous Application Relationship Management, which simplifies complex processes of modeling and managing enterprise applications. vArmour's solutions allow enterprises to baseline application communications, scope security boundaries, and orchestrate policy enforcement.

In May 2020, Tanium launched its Partner Advantage (TPA) Program. This program is still in its early stages and has been kept simple to enable quick traction with potential partners. The Partner Advantage Program is for resellers/VARs. Tanium also has a separate managed services provider (MSP) program that sits under the umbrella of TPA and has operated in Europe, the Middle East, and Africa (EMEA) since March 2020. This will be globalized in 2021. There is no restriction on how many endpoints an MSP can service, although 15,000 is a good example of where MSPs can really be effective.

Market Positioning

Customers

Tanium has a strong focus on very large business customers. Key customers in EMEA include leading companies in retail, automotive, consumer goods, fashion, pharmaceuticals, utilities, manufacturing, insurance, banking, government, and many other sectors. More broadly, Tanium claims to have half of the Fortune 100 among its customer base, as well as all six branches of the U.S. Armed Forces, underlining its ability to serve very large and complex enterprise environments.

FUTURE OUTLOOK

Challenges and Opportunities

Challenges

Tanium's biggest challenge in Europe is lack of awareness. The endpoint security space is particularly crowded, and, in addition to the established endpoint protection platform (EPP) players, the new tranche of endpoint detection and response (EDR) vendors has further complicated this busy space. Consequently, Tanium is challenged with being heard above the cacophony of noise from competing vendors. There is also a broad perception in the market that vendors are segmented into two camps: EPP and EDR, with a trend of convergence between the two. Tanium sits in neither camp, though it is closest in terms of outcomes to the EDR space. This complicates the go-to-market message, where CISOs like to think they know what they need to buy, and from whom.

Europe is primarily a channel-led market, with high variability of languages, business cultures, and security maturity across the region. Although Tanium has some strong relationships with systems integrators (SIs) and is building its wider channel portfolio, it needs to expand this considerably. The challenge is exacerbated by targeting a relatively high customer organization size, which precludes many mid-tier partner options, although Tanium is effective in smaller organizations with as few as 300 employees. The focus on relatively large organizations means that it will be most suitable for the large SIs, but these are notoriously difficult to penetrate and execute with. Tanium acknowledges this difficulty, which is driving its focus on MSPs, but there is much work to be done in 2021 and beyond to achieve a broader and deeper channel across the region.

Opportunities

Tanium's technology could be a genuine game-changer for many organizations with some degree of infrastructure scale and complexity. Security is often constrained by having poor visibility in real time and an inability to act quickly when vulnerabilities are exposed. Tanium addresses these core challenges and offers CISOs an opportunity to share a high-level view of security visibility with executives, in order to aid transparency and risk assessment. In some ways, Tanium's ability to determine the state of security in near-real time is so far beyond typical capability as to be unbelievable (which is a challenge in itself), but it is relatively straightforward to prove the case and, in doing so, demonstrate substantial value to customers.

The core linear chain architecture applies not only to security, but also to endpoint management. While this confuses the decision point – endpoint security and endpoint management are typically purchased by different roles in an organization – the opportunity for cross selling from one to the other is strong. Rather than pitching both solutions at the same time, Tanium may find more traction by landing with a single solution and expanding quickly thereafter.

Tanium is just scratching the surface of the market opportunity in Europe. The primary markets in the region are the UK, France, and Germany, and there is plenty of opportunity for deeper penetration in each of these three countries. Beyond this, there is plenty of headroom in other countries – they may not be as large as the top three, but they have a good coverage of large enterprises that will benefit from Tanium's solutions.

ESSENTIAL GUIDANCE

Advice for Tanium

Channel Expansion

Tanium's route to growth in Europe is via the channel. Some companies, such as Trend Micro and Sophos, have established exemplary channel execution in the region, and Tanium should follow their lead.

Geographic Expansion

It is good to see Tanium investing in Europe, and while it is early days, there is a lot of room for expansion geographically. This is partly predicated on channel execution, but as the channel expands, geographic reach should also grow. Knowing which countries to focus on (and which to avoid) will be a key part of Tanium's growth strategy in the next five years.

Go-to-Market Messaging

Tanium's twin approaches of endpoint security and endpoint management may make sense from an architectural viewpoint, but it can confuse buyers that are accustomed to these functions being separate. In fact, we think that these solutions are use cases for the generic linear chain architecture, and Tanium ought to talk more about this core technology as a lead into the capabilities it enables. Once users understand the technology, we are sure that they will understand more readily how it could apply to their own individual use cases. There are very few cases of genuine differentiation in any technology market, but Tanium has one, and thus should broadcast it much more strongly. Customer success stories and online demonstrations (or even a "try before you buy" approach) would, IDC believes, overcome any scepticism as to the value of the portfolio.

LEARN MORE

Related Research

- *European Endpoint Security Forecast, 2020-2024* (IDC #EUR145782220)
- *European Endpoint Security Market Update: Vendors Striving to Differentiate While COVID-19 Drives Transformation* (IDC #EUR145782120)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC CEMA

Male namesti 13
110 00 Prague 1, Czech Republic
+420 2 2142 3140
Twitter: @IDC
idc-community.com
www.idc.com