IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Tanium and Deep Instinct Form a Strategic Partnership in Prevention-First Endpoint Security

November 02, 2021

By: Michael Suby

IDC's Quick Take

Considering security vendors' on-going investments and marketing on post-compromise detection and response in the guise of endpoint detection and response (EDR), network detection and response (NDR), and extended detection and response (XDR), the essentialness of prevention can be drowned out. Tanium's announced product partnership with Deep Instinct is a reminder that prevention should never take a backseat for IT and security teams as they hone their endpoint security strategies and technologies investments.

Product Announcement Highlights

On November 9, 2021, Tanium announced a product partnership with Deep Instinct, a provider of deep learning threat prevention technology. Integrated into Tanium's Threat Response, Deep Instinct's Prevention Platform adds pre-execution threat prevention to Tanium's lifecycle approach to endpoint security.

Leveraging Deep Instinct's high detection rate of known, unknown, and zero-day threats; low false positive rate; and low-touch agent, Tanium purports multiple operations-slimming benefits for security teams. Those benefits include reduction in security incidents through early-stage attack detection and disruption, reduction in alert processing, and rapidly extending prevention to newly discovered, unmanaged endpoints.

IDC's Point of View

At a high level, the integration of Deep Instinct's Prevention Platform into Tanium Response fills a product gap in Tanium's endpoint security portfolio. That gap was in endpoint protection platform (EPP)/next-generation antivirus. This gap filler by Deep Instinct, while important, is only part of Tanium's maturing approach to endpoint security.

Another part of Tanium's maturing approach is as a unified solution crossing and combining the functional disciplines of client endpoint management and endpoint security. With Tanium, the building blocks to this integrated solution are the Tanium Platform and Tanium Client. Tanium Platform is the unified administration and policy console and data analysis engine powering Tanium's suite of IT management and security modules. Tanium Client, installed on endpoints, is used for endpoint data collection, inter-endpoint and endpoint-to-platform communication, and, in orchestration with Tanium Platform, policy enforcement and security incident response. From these building blocks, Tanium provides its customers with a single source of real-time truth on inventory, hygiene, security posture, and activity across the entire Tanium-managed endpoint estate.

Deep Instinct also fits into this endpoint management and endpoint security integration. Not as a gap filler, as with EPP, but as an always-on threat prevention backup for delayed endpoint hygiene (i.e.,

delayed software updates and patches). In this use case, Deep Instinct prevents attacks attempting to exploit the security vulnerabilities that the software updates and patches were designed to remediate.

The final part of Tanium's maturing approach in endpoint security is in the marginalization of post-compromise detection and response (i.e., EDR). Tanium's underlying philosophy in endpoint security is prevention first and post-compromise detection and response second. Its facilities to identify and resolve substandard endpoint hygiene and security posture resonates directly with a prevention-first philosophy. Deep Instinct's Prevention Platform further extenuates this prevention-first philosophy.

This is not to say that Tanium is fully divorced from post-compromise detection and response. It is not. Tanium Threat Response serves this purpose. But Threat Response also has a built-in preventive element. Coordinating through the Tanium Platform and leveraging real-time endpoint telemetry and state, Tanium facilitates remediating endpoint vulnerabilities (e.g., unpatched software and lenient configurations) that permitted security incidents to occur. In essence, Threat Response is not only used to stop the immediate bleeding from a security incident but to learn from the incident and quickly pivot to systematically strengthening security posture across vulnerable Tanium-managed endpoints. Threat hunting, also part of Threat Response, applies a similar learn-and-strengthen pivot.

On the other side of the partnership, there is material upside for Deep Instinct. As the endpoint security market is both crowded and highly competitive, Deep Instinct has the potential to accelerate its market penetration with introductions to Tanium's customer base and with Tanium's stamp of approval. In addition, Tanium's customer base consists of large organizations with thousands of endpoints. Not only will this provide Deep Instinct opportunities to prove its product's fit among some of the most demanding customers but will also assist in confirming its product's scalability.

Absent in this product launch is a core attribute of Tanium's overall product strategy: unification through integration. Deep Instinct in not integrated into the Tanium Platform or into the Tanium Client. Concurring with Tanium's assertion that a single, comprehensive, and current source of truth is essential in enterprise-grade endpoint management and endpoint security, IDC maintains that this should be the first emphasis of integration in taking this partnership to the next level.

Integrating their agents into a single agent is also a worthy pursuit but a lower priority. IDC's low-priority justification is based on the view that organizations' motivation for reducing the number of endpoint agents is to reduce the overhead that each additional agent brings. That overhead includes another vendor relationship, administrative console, and agent installation; recurring agent management tasks; and potential endpoint performance deterioration resulting in end-user displeasure and help desk tickets.

Tanium and Deep Instinct could argue that much of this overhead is not present or will be lightened shortly. Based on Deep Instinct's experience-based claims and product design, its agent is lightweight, updates are infrequent (2-3x per year), and CPU consumption is less than 5% at peak. Tanium's core capabilities include software installs, so installing the Deep Instinct agent through the Tanium console should be a routine task. Complete integration of Deep Instinct administration functions and endpoint telemetry into Tanium Platform, however, should remain a top priority to eliminate console sprawl. In addition, Tanium customer support personnel should be fully versed on the Deep Instinct product so to minimize customer hand-offs between Tanium and Deep Instinct customer support staffs.

An argument for agent integration is in facilitating platform parity between Tanium products and Deep Instinct. At the time of initial launch, Tanium will offer the MS-Windows version of the Deep Instinct agent. While currently insufficient for organizations that have mixed platform estates, as most do, support for other platforms is expected in the near future. Whether accomplished through agent integration or independently is a decision that should ultimately be made in the context of customer experience.

Subscriptions Covered:
Endpoint Security