Confidence Scores: Transparency, Intelligence, and Business Resilience at Scale

Grace Trinidad

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Confidence Scores — Transparency, Intelligence, and Business Resilience at Scale

This IDC Perspective examines Tanium's AEM Confidence Score and what these and other confidence scores provide to enterprise resilience, operational efficiency, and transparent and confident decision-making. Confidence scores in general quantify the reliability of necessary decisions based on data — a powerful tool in our current cybersecurity environment and digital landscape that demands both comfort with uncertainty and rapid decision-making.

Key Takeaways

- Confidence scores that are based on real-time data can reduce decision-making fatigue by offering data-backed insight to overwhelmed cybersecurity admins and analysts.
- When formulated well and transparently, confidence scores can help to maintain compliance with regulatory standards and protect enterprise assets.
- Confidence scores can help small cybersecurity teams make efficient risk determinations and resource allocation — packages that are accompanied by a low confidence score can spur closer monitoring or more rigorous, staged deployment to prevent operational outages and the like. Conversely, packages with a high confidence score can be more confidently deployed.

Recommended Actions

IT buyers and decision-makers who are evaluating vendors as well as vendors looking to engender greater customer trust should do the following:

- Look for data-driven metrics like confidence scores that can help link operational health to strategic goals.
- Invest in scalable platforms that anticipate even greater complexity in the modern IT environment and can innovate quickly as operational and compliance needs change.
- Get comfortable with resilience over protection. The IT ecosystem is rapidly changing. In this document, we have the first look at a confidence score that will become more refined with time.

Source: IDC, 2025

In today's hyper-connected and complex enterprise environments, the role of endpoint management and data-driven decision-making is more critical than ever. CEOs and decision-makers must grapple with cybersecurity challenges while simultaneously driving innovation. This IDC Perspective explores the transformative potential of confidence scores, focusing on their capacity to enhance organizational resilience and operational efficiency. By drawing from Tanium's recent addition of confidence scores and other industry perspectives, this document provides a high-level introduction to confidence scores for executives striving to future-proof their enterprises.

The Strategic Role of Confidence Scores

Confidence scores are emerging as a critical tool in endpoint management and cybersecurity, quantifying the health, safety, and efficacy of deploying changes into an environment using real-time data. These scores aggregate crowdsourced and contextual data to provide a transparent measure of the package's trustworthiness across IT ecosystems. As in statistics and data science, a high confidence score means that there is very little doubt that a package will operate as intended — with both successful installation and little to no performance degradation. Conversely, a low confidence score is an indicator that installation might not be successful or that the package can degrade performance. The innovation of confidence scores in this context is an important addition to improving the overall operational health and cybersecurity of environments, one that this author looks forward to seeing in other companies.

Operational Transparency and Decision-Making

Confidence scores address the pitfalls of blind trust by leveraging real-time data streams, enabling proactive interventions and more nuanced decision-making. As demonstrated by Tanium, packages with a low confidence score can still be safely deployed through tiered "rings of deployment" that are set up by the enterprise admin, allowing for close monitoring of the deployed package in a controlled environment and mitigating issues before they escalate.

Dynamic Risk Assessment

The score's adaptability allows enterprises to respond dynamically to evolving threats. For example, configurations can be recalibrated in real time based on emerging vulnerabilities. This functionality not only supports cybersecurity but also ensures compliance with regulatory frameworks, safeguarding corporate reputation and assets.

Business Outcomes

Confidence scores extend beyond IT metrics, directly impacting business outcomes. By integrating these scores with broader performance indicators, executives can align operational workflows with strategic goals, ensuring optimal resource allocation and stakeholder trust.

A number of researchers and cybersecurity vendors currently offer some version of confidence scoring, including vendors who are developing tools to protect against artificial intelligence (AI) and machine learning (ML) threats. However, the methodology behind these confidence scores is either opaque or requires unique configurations or calibration for each organization, community, or source. While some confidence scoring approaches can be crowdsourced to provide a starting point that can then be tailored, managing these confidence score permutations can add to the burden faced by cybersecurity professionals in an increasingly complex and fast-moving environment. The following section details one vendor's confidence score not only to highlight the much-needed simplicity they have offered but also to emphasize the importance of transparent confidence scoring techniques that can be easily explained across the organization in order to better align operational resiliency with strategic business goals.

Tanium's Confidence Score

Tanium's Confidence Score is an integral part of its Autonomous Endpoint Management (AEM) solution. AEM leverages AI and patented data techniques to provide intelligent automation and decision-making capabilities for managing IT endpoints. This real-time data collection and analysis built on a scalable, self-organizing platform creates the conditions for a confidence score that is continuously updated in real time. In the example provided when its AEM Confidence Score was announced, Tanium assigns a confidence score to Windows patches that have been released within the last 365 days or are applicable in your environment. The AEM Confidence Score rates the probability that a patch deployment will succeed and will not cause post-installation downtime. As the number of organizations deploying a specific package increases, so too does the robustness of the confidence score. Due to this foundational, real-time architecture, Tanium is positioned to improve its current AEM Confidence Score with contextual data as well as AI, as its scalable architecture allows the company to process enormous amounts of data across endpoints without bottlenecks.

When Tanium's AEM Confidence Score was introduced to users at Tanium Converge 2024, you could almost hear the collective sigh of relief. The enthusiasm in the room underscored how much decision-making fatigue cybersecurity admins wish to be relieved of. As we will see in the following figures, the AEM Confidence Score is somewhat straightforward in nature, but that does not actually diminish its value to users. Decision-making aids — such as Tanium's AEM Confidence Score — that are

transparent in methodology and easy to explain are supremely valuable, especially in our current push toward AI, a technology that lacks transparency as a matter of course.

While Tanium has not disclosed its formulas in detail, the general approach shared with IDC is shown in Figures 2 and 3.

FIGURE 2

For Confidence in Package Deployment

$$Efficacy = \frac{Success}{Success + Failed}$$

$$Safety = \frac{\text{\# of endpoints with a degradation}}{\text{\# of endpoints that used application}}$$

Source: IDC, 2025

FIGURE 3

For Confidence in Patch Performance

$$Efficacy = \frac{Success}{Success + Failed}$$

$$Safety = \text{\# of uninstalls}$$

Source: IDC, 2025

These are then used to provide a confidence score summary that includes the following:

- **Installation success:** The percentage of endpoints with successful installation
- **Performance degradation:** The percentage of endpoints that ran the action and experienced a notable degradation of performance; degradation currently includes app crash (high-impact degradation), CPU spike, abnormally high CPU usage, and abnormally high memory usage (lower-impact degradations)

Tanium currently categorizes confidence into three levels — low, moderate, and high, with additional color-coded indicators for each degradation. Users can leverage these ratings to make informed decisions about how and when to deploy changes. If a change is high confidence, a user may choose to deploy the change quickly and without extensive testing, but if a change is moderate or low confidence, a user would likely benefit from doing some more independent testing and research to understand the impacts to their environment.

Confidence Scores into the Future

While Tanium's AEM Confidence Score is an exciting addition to the company's offerings, this author recommends the following improvements to refine and enrich this and other confidence scores:

- **Environmental context:** At Tanium Converge 2024, attendees were in agreement that enterprise environments can vary widely. Incorporation of environmental data such as geolocation, device type, and environmental sensitivity and complexity can provide a more contextualized assessment that further aids in decision-making.
- **Dynamic weighting:** As of this writing, Tanium's confidence score is a straight-talking indicator of package installation success and performance. Dynamic weighting can take into consideration current or immediate threats and provide additional data on package or patch criticality.
- **Display by distribution rather than category:** Categorization of risk is somewhat arbitrary and can be misleading — if high confidence is a score of 90%, what about packages that eke out 89%? Presenting the AEM Confidence Score as a distribution rather than as a category can prevent anchoring or over-generalization biases from entering into decision-making.

ADVICE FOR THE TECHNOLOGY BUYER

To capitalize on the benefits of confidence scores, CEOs and decision-makers must adopt a proactive and integrated approach to IT and security management. In detail:

- **Foster a data-driven culture:** Real-time data must be integrated into organizational workflows. Confidence scores should serve as a key performance indicator (KPI), linking operational health to strategic goals.
- **Invest in scalable platforms:** Platforms that unify endpoint management and cybersecurity (like Tanium) offer a scalable solution to the complexities of modern IT environments. Their ability to integrate seamlessly with existing tools, such as Microsoft Intune, ensures compatibility and enhances operational coherence.

- **Prioritize resilience over perfection:** As highlighted during Tanium Converge 2024, the pursuit of perfection can hinder progress. Rapid iteration guided by real-time confidence metrics allows organizations to achieve resilience without sacrificing agility.

The convergence of confidence scores and autonomous endpoint management is revolutionizing enterprise resilience. By quantifying trust and enabling real-time, data-driven interventions, these innovations empower organizations to navigate the complexities of modern IT landscapes. For CEOs and decision-makers, the imperative is clear — invest in the right platforms, embrace transparency, and prioritize resilience to ensure sustained success in a rapidly evolving digital world.

Through the lens of Tanium's pioneering technologies, it becomes evident that the "power of certainty" lies not in reacting to the past but in acting with confidence on the present. The future belongs to those who can adapt, innovate, and scale securely.

LEARN MORE

Related Research

- *IDC ProductScape: Worldwide Small and Medium-Sized Business Endpoint Protection Market, 2024–2025: Technology Supplier Solution Functionality* (IDC #US52830124, January 2025)
- *IDC's 2024 U.S. Enterprise Endpoint Management Survey: Assessment of Endpoint Device Management Technology Adoption and Trends in Endpoint Operations and Security Management* (IDC #US50820824, October 2024)
- *Worldwide Corporate Endpoint Protection Survey, 2024* (IDC #US52593024, September 2024)
- *Endpoint Security Market Not as Mature as Expected: Room for Improvement* (IDC #US52579824, September 2024)
- *Worldwide Market Analysis Perspective 2024: Corporate Endpoint Security* (IDC #US52540624, August 2024)
- *Worldwide Client Endpoint Management Software Forecast, 2024–2028* (IDC #US51633624, July 2024)
- *Worldwide Corporate Endpoint Security Software Forecast, 2024–2028: Consolidation on the Horizon* (IDC #US52439323, July 2024)
- *Who Has Responsibility for Endpoint Security Activities?* (IDC #US52282624, May 2024)

Synopsis

This IDC Perspective explores the transformative potential of confidence scores, focusing on their capacity to enhance organizational resilience and operational efficiency. Confidence scores are a transformative tool designed to enhance enterprise resilience and operational efficiency through data-driven decision-making. In today's complex IT landscapes, where cybersecurity risks must be balanced with innovation, confidence scores are an (ideally) transparent metric to guide these decisions. By aggregating real-time and crowdsourced data, these scores quantify the likelihood of successful software deployments and performance stability. Described in this document is IDC's first look at Tanium's AEM Confidence Score, what this confidence score provides to cybersecurity professionals, and thoughts on how similar confidence scores can be improved in the future. For technology buyers, investing in scalable platforms and prioritizing resilience over perfection are key strategies. Ultimately, confidence scores combined with autonomous endpoint management empower organizations to navigate modern IT challenges with agility and certainty, positioning them for sustained success in an evolving digital landscape.

"Decision-making aids — such as confidence scores — that are transparent in methodology and easy to explain are supremely valuable, especially in our current push toward AI, a technology that lacks transparency as a matter of course," says Dr. Grace Trinidad, research director, Trust Measurement and Metrics at IDC.

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com