Q&A

TANIUM

The future of client management

FEATURED SPEAKER
Andrew Hewitt
Senior Analyst at Forrester

In today's environment, it's critical for IT operations leaders to manage and configure their entire IT estate in real time, proactively discover remote endpoints, deploy software, and monitor end-user impact with minimal network strain. We recently caught up with our guest Andrew Hewitt, Senior Analyst at Forrester to talk about the importance of developing a robust client management strategy and bringing IT operations and security teams together. The following Q&A is a deeper dive into the discussion from our interview.

How will the convergence of security and operations tools impact the employee experience?

Andrew: Historically, when organizations think about experience and security, they see them as two diametrically opposed forces: an increase in experience leads to a degradation of security, and vice versa. With the convergence of security and operations tools, enterprises have the opportunity to both simultaneously improve the overall employee experience and security posture at the same time. We will see this play out in four key ways:

- Faster identification of malware on devices, protecting employee computing resources from circumvention and preventing malware from causing disruptions to employee productivity.
- Improved ability to see the impact of policies and security agents on end-user experience overall, as indicated through high CPU utilization, reduced memory, etc.
- Less conflict between endpoint management and security policies, leading to a more consistent experience for employees
- Faster time to market with new innovative technologies due to the ability to simultaneously manage and secure those technologies within a single platform

How can operations leaders determine whether they are investing too much or too little in endpoint management relative to their peers?

Andrew: Organizations that invest in too little endpoint management relative to their peers will likely see signs of poor IT hygiene popping up in their environments. For example, if your patch success rate is less than 95%, you're investing too little in endpoint management. The same will apply to visibility — organizations should have close to 100% visibility over all the endpoints in their environment, with a high percentage of those devices under management. If management processes aren't optimized for employee experience (e.g., enabling employees to install patches at their convenience), you'll likely see high rates of dissatisfaction from employee surveys, indicating a need to invest more. Of course, if your organization is experiencing a high number of endpoint breaches, it's likely you're underinvesting.

It's difficult to determine if you're overinvesting in endpoint management relative to peers but some of the key signs could include: negative employee feedback surveys that indicate policies are too restrictive, performance metrics spiking due to agent overload, administrators spending most of their day on mundane endpoint management task (i.e., your organization is giving them too many unnecessary tools to manage). Another telltale sign that you're overinvesting is the number of endpoint management tools in your environment. If you have more than 3-4 tools for all of your endpoints (including mobile and virtual), you likely have overlapping capabilities that you could consolidate into one or fewer platforms.

How important should endpoint automation be relative to CIO priorities over the next couple of years?

Andrew: Endpoint automation should be a top priority for CIOs over the next couple of years. Although it's not as high of a priority as improving cybersecurity posturing, maintaining costs, and improving user experience, it's impact on each of those priorities is immense. Why is automation so important? While endpoint management itself is foundational to protect the business and support user productivity, it's still core infrastructure — every organization needs endpoint management. Because every company will have some form of endpoint management, it's not an area that organizations should use to truly drive differentiation for their customers. In the future of work, administrators will and should spend way less time on manual endpoint management tasks and should instead use automation and orchestration to complete the same tasks in a fraction of the time, enabling them to free up time for other more difficult tasks. For example, there are other technologies that require huge investments (AI, cloud,

hybrid work technologies) that the business will need to different against competition. Automation is key to getting endpoint management to do its job with little to no human intervention. Without automation, IT pros spend too much time on the nuts and bolts and can't spend time addressing more difficult challenges that could potentially lead to better innovation and differentiation for the firm.

What are the prerequisites to achieving endpoint automation?

Andrew: There are many different levels of maturity when it comes to endpoint automation. On the most basic level, IF:THEN policy functionality can achieve a great deal of low-level automation. For example, quarantining a device if malware is found, pushing a patch automatically, or even emptying a recycling bin when storage starts to run out. These types of automation every customer can start to take advantage of today.

The trickier form of automation relates to what we call "self-healing," in which multiple automations occur simultaneously to fix experience issues, rid endpoints of malware, or bring endpoints back into a known state of compliance. There are a few prerequisites to this kind of model:

1. **Full visibility and control over the endpoint estate.** Without having a full inventory of what's in your environment, it's impossible to execute any form of remediation on the endpoint.
2. **An understanding of what "good" looks like.** Whether it's an ideal policy state, experience level, or corporate image, the organization needs to understand what they're trying to achieve from an endpoint perspective. What level of experience is acceptable? What kinds of policies do you always want turned on? What are you purposely leaving out? These kinds of questions will help define your ideal endpoint state.
3. **Real-time and historical data.** This helps detect anomalies and drifts away from the ideal endpoint state.
4. **An analytical model.** An algorithmic approach can help identify likely root causes and suggested remediations to help drive automation without human intervention.
5. **A culture of automation.** People will be the biggest obstacle to widespread automation; in particular, fear of automating oneself out of a job. You need to cultivate a culture in which automation is praised and employees don't have to fear about future job opportunities due to automation.

Learn how Tanium's Converged Endpoint Management (XEM) platform converges teams and data to provide a real-time view of endpoints across your environment for visibility, control and trust in IT decision-making.

LEARN MORE

How will endpoint tools and processes change how operations teams produce actionable insights in the next couple of years?

Andrew: Over the next couple of years, we'll see numerous changes in how operations team produce insights from endpoint tools and processes:

- We'll increasingly see admins collecting telemetry data to understand operational, security, and experience issues happening in their environment and using that data to drive remediation.
- We'll see admins increasingly building customized dashboards within endpoint management consoles that provide instant alerts, recommendations, and likely root causes to endpoint issues.
- We'll increasingly see administrators compare security and operational data side by side to understand the trade-offs between security policies and user experience.
- The move towards SaaS for endpoint management tools will enable cross-department, -industry, and -geographic benchmarking for customers, enabling tools to suggest appropriate configurations or policies based on unique customer needs.