WHITE PAPER

The Intelligent Edge: A Faster, More Efficient Way to Manage Your IT Risk

With an intelligent edge, you can protect your endpoint devices, ensure regulatory compliance, boost employee productivity, and lower software licensing costs.

By Jack Coates, Senior Director of Product Management, Tanium

Introduction

The edge is where business happens. Whether you're selling pizzas, executing complex stock market trades, or managing a global logistics firm, the edge is where your data, human intelligence and technology intersect. The edge is where all the work gets done.

Yet the endpoint devices at the edge of your network are also a source of risk. Those risks include security, operational and compliance risks. Laptops, servers and cloud connections are all prime targets for data thieves and network hacks.

If these endpoints aren't running at their best, then neither is your business. What's more, the challenge of managing the edge efficiently has become even more acute, thanks to mass remote working and resource pressures due to the pandemic.

The bottom line: Your IT security and operations teams must ensure that the edge is always secure, in compliance, properly managed, and correctly licensed. While there are many ways to do this, the best approach involves doing as much of the work as possible locally — that is, at the endpoint device. Compared with other approaches, the endpoint is quicker, cheaper and more accurate.

Fortunately, securing and managing the edge is no longer a complicated process of collecting terabytes and petabytes of data, moving that data to separate silos for processing into information, analyzing that information, orchestrating a response, and then arriving at a course of action days later. Instead, you can now ask simple questions of your endpoints and get direct, actionable answers immediately.

We call this the **Intelligent Edge**. It's your powerful shortcut to getting the answers you need to make informed, risk-based decisions about your business. The Intelligent Edge is also about maximizing the IT resources you already have to gain context-rich visibility and precise control to run a more agile organization. In this and other ways, the Intelligent Edge provides what CIOs and CISOs have been requesting for years. And it's here now.

The problem with data lakes

The Intelligent Edge can mean different things to different people. This white paper uses the term in the context of managing your endpoint devices in a smarter way.

Endpoints connect your organization's two most important assets: people and data. It makes sense to perform as much assessment and remediation as possible where these two resources meet.

Successful businesses must manage legal, operational and security risks across all endpoints. To do so, you need to be continuously aware of all your IT assets, wherever they are.

Unfortunately, many organizations are struggling to gain this essential visibility and control. Our recent survey found that 94 percent of global CIOs have discovered previously unknown endpoints within their IT environments.

This challenge is further compounded by current approaches to monitoring endpoints.

Data lake–based technologies are a popular way for unearthing insight into endpoints. But although data lakes excel at finding "unknown unknowns," they may not be the best value for the money in this case.

Data lakes move and process huge pools of data. Converting this raw data into answers takes significant time and money. And the bill grows each time you need to update those answers.

If you wait until a data lake has collected all the data it needs before asking a question, the answers will likely be out-of-date. Crucially, it may also lose local context.

Ask the right questions, in the right way

Organizations clearly need a more efficient way to collect data, model data and answer users' questions. This approach is the only way to guarantee that you always understand the status of key IT assets and can rapidly take any required action.

The best way to do this: Push intelligence to the network edge. Working at the edge allows you to answer questions as close to the data as possible. It also saves time and maintains context. Compared with data lakes, working at the edge is also much cheaper, because you're no longer shuttling data into separate silos for processing.

The goal is the ability to answer short, simple and, ideally, yes-or-no questions. It's a far more efficient way of working. Compare these two sets of queries:

- "Are systems missing critical patches issued over 30 days ago?" vs. "List all missing patches from all systems."
- "Are these specific systems under memory stress?" vs. "Report memory usage of all systems."

What's the difference? The first question in each set can be answered with a "yes" or "no," and that can generate actionable insights. Instead of asking your team to determine what the data means, you can report on the existence of problems that also have clear solutions.

Ask a clarifying question. Orient yourself. And then take action. When done at speed and scale, this approach keeps the lights on, the doors open, and everything in your business safe and secure. That's the benefit of the Intelligent Edge.

How the intelligent edge adds value

Organizations can deploy the Intelligent Edge for several important use cases. Here are four examples.

Operational hygiene

Cyber-hygiene is a foundational best practice for mitigating risk. Its absence can allow threat actors to breach networks, compromise, steal and extort on a truly global scale. If more organizations took care of patching and configuration management, they could block a large percentage of today's attacks.

One common challenge is server certificate expirations. Today, your customers, employees and partners use services that need certificates for secure communications. What's more, these certificates must undergo regular renewal and updating to the latest standards.

Unfortunately, like many things with long time frames, certificates are easy to forget and challenging to understand. An Intelligent Edge approach can help by empowering your systems to discover other servers on the network, and then "teach" each server to report its own status to IT with a simple message like "X certificate expires within 30 days."

Sensitive data assessment

Another common challenge is inventory management of sensitive data. For example, your corporate policy might state that no endpoint should store personally identifiable or health information. By teaching your endpoints to recognize this sensitive data, you can quickly and easily report on its presence — and without requiring your staff's perfect adherence to data-handling policies.

Security signaling

One irony of cybersecurity is that in most breaches starting from an employee's endpoint device, the security products actually worked as intended. That is, they notified the security operations center (SOC) analysts of an intrusion, just as they should. But if this information (the "signals") is obscured by a cacophony of other information and data (the "noise"), then the security team can miss the message that there is a security threat.

An Intelligent Edge approach can do better. It provides enhanced awareness of events happening at the endpoint and across multiple triggers. An Intelligent Edge can then increase the amount of signal for prioritized events, so that it's not lost in the noise.

The Intelligent Edge also offers another benefit. Because endpoints commonly have plenty of free disk space, you can store data on them more cheaply and efficiently than in a data lake. Doing so also delivers a greater depth of historical data for investigations and response.

The Intelligent Edge is also faster. Data lakes commonly impose a seven-day limit on data, due to cost implications and the need to move data across the network. By contrast, the Intelligent Edge processes everything locally, which supports the goals of the SOC team. It's also more secure, as there's no need to move data, which exposes it to extra risk.

Risk management

Performing risk assessments at the endpoint saves time and money, while also supporting efficient SOC operations. Consider this example: A vulnerability assessment requires you to know how long a particular bug has been present and how old the finding is.

To produce answers, a data lake would send highly granular data on thousands — or even hundreds of thousands — of endpoints. Also, this information would date back to the installation of the compliance product, which could be years in the past. This big-data based process quickly becomes expensive and unwieldy.

What the user really wants to know is dwell time (how long has the vulnerability been present) and scan age (how long ago did we last verify the vulnerability's presence). Using Intelligent Edge techniques, the user can ask these direct questions. Even better, the system will require far simpler computations to deliver rapid, actionable answers. Using these techniques can also reduce your network traffic load by as much as two-thirds, and with all associated cost savings.

Simplicity Is everything

IT and security leaders need fast, actionable and trustworthy data to optimize their security and operations and continually manage their risk. The Intelligent Edge can provide all that, and with powerful simplicity. It's the difference between getting a simple yes or no answer versus being deluged with thousands of metrics.

The powerful simplicity of the Intelligent Edge can help your organization answer the fundamental questions listed on the following page.

What is the current state of my IT assets?

Are we okay operationally? Can we perform our core business functions? Are there pegged CPUs and unpatched vulnerabilities that we must take care of?

Have our IT operations improved over time?

Has performance improved across specific business units and networks? Are mean-time-to-detect and mean-time-to-resolve coming down? The Intelligent Edge can rapidly answer questions like these in a high-information, low-data way.

Do I have an accurate and complete dataset?

The Intelligent Edge is about providing continuous real-time visibility at scale to produce better outcomes. In a world where more and more corporate endpoints are in bandwidth-restricted home offices, this network-efficient approach makes increasing sense.

Can I maximize my IT investments to gain insight and control?

Your organization undoubtedly has a lot of expensive IT equipment to support your staff and power your business. Why not leverage any spare CPU cycles on these assets for comprehensive endpoint management and monitoring? That's far better than using other solutions that require you to invest in hundreds of additional servers.

Conclusion

The Intelligent Edge is the necessary approach for today's dynamic, distributed networks that are under threat from cyberattacks every minute of the day. By moving intelligence and data analysis to the edge, organizations gain the speed, visibility and insights to survive and thrive in this new era of remote work and pervasive cybercrime.

Schedule a free consultation and demo of Tanium.

Schedule Now

Let Tanium perform a thorough gap assessment of your current capabilities.

Get Gap Assessment

Launch Tanium with our cloud-based offering, Tanium as a Service.

Try Now

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.