Defense Contractor, Diagnosing Severe Performance Issues with End User Experience Monitoring

How Maintech used empirical End User Experience Monitoring to trace widespread performance complaints back to their real source, redesign device requirements, and reduce friction between security and operations teams.

MAINTECH

About the Client

The client is a defense contractor operating in a highly regulated, security-first environment. The sensitivity of its work demands a substantial layer of mandated security tooling on every end-user device, deployed across a large and complex estate.

That security posture is non-negotiable. The organization needed to understand its effect on the people relying on those devices to do their jobs.

The Challenge

The organization had faced sustained performance complaints across its workforce. The symptoms were consistent, but the cause was unclear, with no shortage of plausible explanations.

By the time Maintech was engaged, the following conditions were in play:

Widespread user complaints.
Staff reported applications that were slow to respond, connectivity that felt unreliable, and noticeable delays when accessing files. The issues were affecting productivity across the organization.

No objective data.
The complaints were based on user perception, with no measurement of what the devices were actually doing when performance degraded. Without that evidence, every diagnosis was a hypothesis.

A complex, heavily secured environment.
Network, servers, devices, and the security stack itself were all potential contributors. In an estate of this size and sensitivity, isolating the real cause required a systematic, granular approach.

Friction between internal teams.
The security function mandated the tooling. The operations function fielded the complaints. With no shared source of truth, the two teams held competing views on the cause, and the conversation went in circles.

The organization needed a partner who could measure what was happening and produce evidence both teams could trust.

The Solution

Maintech deployed its managed End User Experience Monitoring to gather empirical data on how the environment was performing for real users. The work was structured so that each phase built on the last.

End User Experience Monitoring Deployment

Maintech rolled out monitoring across three layers of the user experience: the devices themselves, the key websites users depended on, and the core file services they accessed throughout the day. The goal was to capture how the environment behaved in practice, at the point of use, across a representative sample of the workforce.

This gave full visibility into real device behavior, where before there had only been reported symptoms.

Empirical Analysis and Root Cause Identification

With monitoring in place, Maintech measured device-level CPU, memory, and disk IO alongside connectivity to key websites and file services, correlating each metric against the periods when users reported problems.

The data was consistent and unambiguous. The security tooling was repeatedly driving endpoint CPU and disk IO to saturation under normal working conditions, the primary cause of the slow applications, connectivity issues, and file-access delays. The analysis surfaced several smaller server-side issues worth resolving too, but the main driver was clearly the load the security stack placed on each device.

For the first time, the organization had a documented, measurable root cause rather than a set of competing theories.

Optimization and Cross-Team Alignment

The findings gave the organization a practical path forward. Device requirements were redesigned around the workload the security tooling demanded, so endpoints could carry the mandated protection without degrading the user experience, and the smaller server-side issues were addressed in parallel.

Just as importantly, the empirical data gave the security and operations teams a single, shared reference point. With the cause measured and documented, the two functions were able to collaborate on the solution.

This reduced the friction that had built up between the teams and turned a contested problem into a shared, solvable one.

The Outcome

The engagement gave the defense contractor a resolution grounded in evidence rather than opinion.

The months of performance complaints were traced to a measurable, documented cause.

Device requirements were redesigned around real workload data, allowing the organization to maintain its full security posture while restoring a workable user experience.

The smaller server-side issues identified during the analysis were resolved alongside the main finding.

The organization came away with two lasting assets. It retained an ongoing End User Experience Monitoring capability that surfaces issues with hard data, and it gained a repeatable, evidence-led method for diagnosing future problems before they escalate.

Why This Matters for Highly Secured Organizations

Security tooling is essential in defense and other regulated sectors, and it carries a real resource cost on every device it runs on.

Industry guidance is explicit that endpoint security software can consume significant CPU, memory, and disk resources, and that it requires careful configuration to avoid slowing the systems it's there to protect (Palo Alto Networks).

When that cost goes unmeasured, it shows up as performance complaints that are easy to misattribute to the network, the servers, or the hardware. Organizations end up chasing the wrong fixes while the bottleneck persists and internal teams pull in different directions.

Maintech's work with this client shows that a disciplined, evidence-based approach to End User Experience Monitoring can locate the true cause quickly, even in a complex and heavily secured environment. The methodology is rigorous and the results are durable, because they are grounded in how the devices perform for real users.

For organizations carrying a heavy security stack, the question is whether they have the data to manage that tooling.

Maintech delivers managed monitoring, end-user services, and infrastructure support for complex, security-conscious environments. To discuss what End User Experience Monitoring could reveal in your estate, contact the Maintech team today.

www.maintech.com

Global - contact@maintech.com

MAINTECH