

When Security Matters, Riverbed Delivers

Most organizations start by evaluating features and outcomes. They finish by evaluating risk.

Built to meet the security standards of government and defense. Delivered to every customer.

1. What Do Federal Security Certifications Tell Enterprise IT Leaders?

That's a fair question.

Most commercial organizations aren't evaluating Digital Employee Experience (DEX) platforms based on government compliance requirements. They're evaluating them based on business outcomes, employee productivity, operational efficiency, ease of deployment, and cost.

So what do certifications like FedRAMP High really tell an enterprise IT leader?

They tell you how much a vendor has invested in building security into the platform itself.

Anybody can claim a platform is secure. FedRAMP High provides independent validation that a platform has been engineered and operated to meet some of the world's most demanding security standards.

Why?

Because when a DEX platform has visibility into employee devices, applications, networks, collaboration tools, AI activity, and operational workflows, security becomes far more than a compliance exercise. It becomes a fundamental part of the platform you're trusting to support your business.

That's why security-conscious organizations increasingly view **FedRAMP High** not simply as a government requirement, but as evidence of engineering discipline, operational maturity, and a long-term commitment to security.

2. Why Security Matters More Than Ever

Ten years ago, most Digital Employee Experience (DEX) platforms were primarily troubleshooting tools.

Today, they play a much broader role. They sit at the intersection of employee productivity, application performance, network visibility, automation, and increasingly AI governance.

As organizations rely on these platforms to support operational decisions and AI-driven workflows, security becomes more than an IT requirement. It becomes a business requirement.

That's why organizations should evaluate DEX platforms with the same security expectations they apply to other mission-critical enterprise systems.

That raises an important question:

Does it matter how that security is delivered?

3. What Does a FedRAMP High Authorization Really Tell You?

Not all FedRAMP certifications are the same.

FedRAMP defines multiple certification levels based on the sensitivity of the information and workloads a cloud service is designed to protect.

For example, **FedRAMP Moderate** (Class C) is intended for the majority of government business systems, while **FedRAMP High** (Class D) is designed for systems supporting highly sensitive government missions where the potential impact of a security breach could be severe.

As a result, achieving **FedRAMP High** requires significantly more rigorous security controls, stronger operational processes, more extensive continuous monitoring, and greater ongoing compliance than **FedRAMP Moderate**.

For enterprise IT leaders, that distinction matters because a higher authorization level reflects more than compliance—it reflects the level of engineering discipline, operational maturity, and long-term investment required to achieve and maintain it.

But security level is only part of the story.

An equally important question is whether the certification is native to the security of the platform itself – or simply the security inherited from the hosting environment.

A highly secure hosting environment helps protect the infrastructure in which an application runs. But enterprise customers ultimately depend on the platform itself.

The software architecture, secure development practices, encryption, access controls, monitoring, operational governance, and lifecycle management built into the platform determine the level of protection customers experience every day.

That's why the distinction matters.

One tells you **where** the software runs.

The other tells you **how** it was engineered.

Riverbed achieved **FedRAMP High** using the same software that's delivered to commercial customers. That means the engineering, security controls, and operational disciplines required to achieve **FedRAMP High** aren't limited to a separate government product—they're built into the software every customer uses.

For enterprise IT leaders, the takeaway is simple: **FedRAMP High isn't just a government certification. It's independent validation of how a platform has been engineered, secured, and operated—and that's something every organization should consider when evaluating a Digital Employee Experience platform.**

4. A Better Way to Evaluate DEX Security

For years, organizations have evaluated Digital Employee Experience platforms primarily on capabilities—visibility, analytics, automation, AI, and user experience.

Those capabilities remain important.

But as DEX platforms become more deeply integrated into enterprise operations, they should also be evaluated through a security lens.

That means looking beyond feature lists and marketing claims to understand how the platform was engineered, how its security has been independently validated, and whether the software deployed in your environment reflects the same engineering standards as the software that achieved the certification.

Security shouldn't be viewed as another feature.

It should be viewed as a foundational characteristic of the platform itself.

5. Digital Employee Experience Is Becoming Critical Enterprise Infrastructure

Digital Employee Experience platforms have evolved far beyond endpoint monitoring and troubleshooting.

Today they provide visibility across employee devices, applications, networks, collaboration platforms, and increasingly AI-driven operations. They help organizations automate workflows, guide operational decisions, and improve employee productivity.

As their role continues to expand, so does the level of trust organizations place in them.

That changes how they should be evaluated.

The question is no longer simply:

Can this platform improve digital employee experience?

The better question is:

Can this platform be trusted to support increasingly critical business operations?

6. Questions Every Enterprise IT Leader Should Ask

As Digital Employee Experience platforms become more strategic to enterprise operations, security deserves the same level of scrutiny as capabilities, AI, automation, and user experience.

The quality of the answers to these questions may tell you as much about a platform as its feature list.

When evaluating a DEX platform, ask:

- Does the authorization apply to the platform itself, or only to the hosting environment in which it's deployed?
- What level of FedRAMP authorization has the platform achieved, and what does that authorization tell me about its engineering maturity?
- Is the software delivered to commercial customers the same software that achieved the FedRAMP High authorization?
- What engineering, security, and operational disciplines were required to achieve and maintain that authorization?
- As this platform becomes more strategic to my business, does its security posture meet the same standards I expect from other mission-critical enterprise systems?



About Riverbed

Riverbed, the leader in AIOps for observability, helps organizations optimize their user's experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improves IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences.

Learn more at riverbed.com.