riverbed

White Paper

Mitigating the Risks of IT Change

Application Discovery and Dependency Mapping with Riverbed SteelCentral.

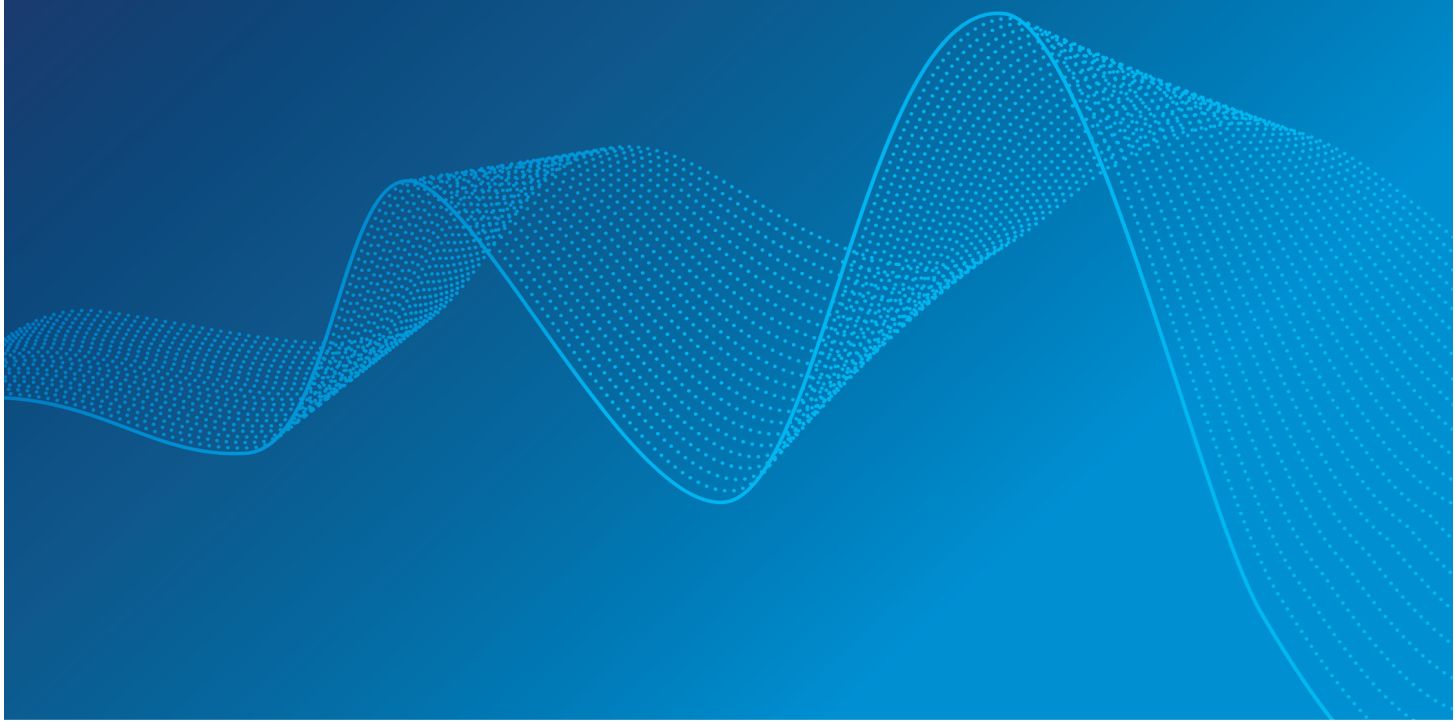


Table of Contents

Executive Summary

Effective IT planning and decision making are dependent upon having a complete asset inventory and an accurate understanding about dependencies available before, during and after IT change activities.

Application discovery and dependency mapping (ADDM) solutions automate the process of discovering and mapping transactions and applications to the underlying infrastructure and application interdependencies. The service models created by ADDM solutions then become invaluable tools for supporting many aspects of digital transforamion, including:

- Managing network change efficiently, such as cloud migrations, data center consolidations, disaster recovery, or virtualization initiatives
- Troubleshooting complex, multi-tiered application ecosystems before, during and after an IT change project
- Supporting regulatory and security compliance

Riverbed® SteelCentral™ NetProfiler is an application-aware network performance management solution with built-in application discovery and dependeny mapping. NetProfiler passively analyzes historical and real-time network traffic behavior to quickly provide information about the interactions, usage and dependencies between users, applications, and servers without agents or scans. It quickly provides a complete and accurate inventory of the IT environment, including an understanding of how services and their underlying IT infrastructure impact the business. The result is:

- Project times are shortened by two-thirds
- The expense of discovery is reduced by up to 50 percent
- Project benefits, such as cost reductions, efficiencies, etc., are realized sooner

Challenges

Every organization is driving digital transformation with cloud-smart strategies. These initiatives require big changes to the network and application infrastructure that provide services to the end user. Migrating applications to the cloud, consolidating data centers and updating legacy systems set expectations of additional cost savings, faster service delivery, and a more productive workforce that can leverage more innovative technologies. Unfortunately, as many have already discovered, digital transformation is not a simple, linear path.

Consolidation projects can include:

- Migrating branch services into the data center
- Consolidating one or more data centers
- Moving a data center or server to a new location
- Virtualizing and consolidating underutilized computing resources such as servers or storage
- Migrating applications or even whole data centers to the Cloud migrations

The first step in any consolidation project is to assess the current environment. IT change projects such as data center consolidations are typically major undertakings that consume significant time and resources and are fraught with risk. Unfortunately, it is all too common that services are restored with performance and availability problems that cause business disruptions, eroding much of the anticipated savings. Planning for an IT change can be a long and error-prone process. An accurate and comprehensive understanding of your infrastructure is necessary to ensure that your implementation plan is appropriate and will result in a smooth transition. Documentation and historical asset inventories are rarely up to date and the people who built them have invariably moved on, providing an unreliable basis for planning.

Successful consolidation projects mitigate risk and execute efficiently through diligent up-front planning and decision making. High-quality project plans and effective decisions are dependent upon having accurate and detailed information available before, during, and after migration activities. For example, imagine you are moving an application to the cloud; it is critical to understand all the application dependencies so you can make sure all components are properly migrated.

Without precise knowledge of the end-to-end service delivery path, it would be easy to misconfigure the cloud environment and cause an outage or significant end-user experience issues.

Manual Approach Impractical

The "clipboard method" of manually inventorying IT assets and mapping physical components (such as servers and network devices) and logical components (such as users, applications and databases) to specific business applications is outdated and foolhardy. These manual service models, which rely on interviewing application managers about application dependencies, are:

- Expensive and time consuming to build, with days of professional services being cited per business application mapped
- Typically, incomplete due to a limited awareness of the application architecture
- Out of date almost as soon as they are defined
- Nearly impossible to maintain with the rate of change in the IT environment
- Ineffective due to their incomplete and out-of-date nature

Scan and Agent-based Discovery have Drawbacks

There are tools available that can help automate parts of the process, but they can leave gaps and can introduce other problems such as network performance degradation and high deployment costs. Scanning tools can build detailed inventories, but they do not show dependencies and they can slow down network performance. Agents can also help automate the process, but only for the areas of the network where the agents are installed. The high cost of deploying agents effectively limits their scope.

Agents

There are several drawbacks to using, or at least starting a discovery project, with agents. These drawbacks include:

- **Incomplete coverage** due to a limited awareness of the application architecture
- **Time consuming** to install, update and manage. Getting permission from the server/application managers to install agents can be difficult and time consuming. Updating them can be another headache. Also, how do you know if the agents have been removed from the server?
- **Incomplete.** The high cost of deploying agents effectively limits their scope. In addition, not all equipment can support agents; printers do not, for example.
- **Expensive to deploy**. The biggest problem with discovery agents is the expense to deploy. IT must continually balance the cost of deploying an agent with the depth of data needed.
- **Limited functionality**. Agents cannot baseline performance. They do not provide a historical record of performance for the pre-consolidation environment for comparison to post-project performance, so you do not know if performance improved or deteriorated as a result of the move. And an agent almost certainly does not record the usage patterns, such as who used the application and when peak usage occurs.

Scans

Scan-based discovery solutions crawl or scan a network and then automatically log onto a server to see what processes are running and access the routing table to determine who was conversing with whom. While they provide detailed information into the application processes running, the problem with scans is that they are typically:

- **Time consuming**. Scans provide a point-in-time snapshot of what is currently occurring on the network. They must be run over and over again to gain a complete inventory and dependencies map.

- **Require credentials** from security/server teams, which are often difficult to obtain en masse as they are viewed as a major security risk.
- **Incomplete**. Often the scans are relegated to running in off hours, when traffic is atypical, for fear of adding to network congestion. Also, does the scan appliance have access to all the data centers and systems it needs for complete coverage? Firewalls can often block scanner access as well.

SteelCentral NetProfiler

The key to minimizing the risks associated with IT change is to automate and improve the planning and discovery process. Quickly identifying all assets, their locations and dependencies without requiring time-consuming or expensive agents, scans, credentials helps ensure that a critical dependency will not be overlooked, e.g. that an essential server is shut down that nobody thought was still being used. The sooner all assets and dependencies are identified, the faster the change can be implemented.

Riverbed® SteelCentral™ NetProfiler is best known as an application-aware network performance management solution that passively analyzes historical and real-time network traffic behavior to provide information about the interactions, usage, performance and dependencies between users, applications, and systems. Because NetProfiler uses flow data collected from existing network devices and augments it with user and application data, it can analyze the entire network without requiring any deployment of agents or probes.

In addition to monitoring and troubleshooting network and application performance, NetProfiler also provides robust discovery and dependency mapping capabilities that are the basis for building complete and accurate service-level dashboards, but that can be used to effectively and efficiently plan and manage consolidation or modernization initiatives.

Deploying NetProfiler at the start of a data center migration project provides significant benefits. NetProfiler can be used to:

- Provide a complete and accurate inventory of the IT environment, including unexpected or unknown dependencies, for more effective planning
- Discover additional optimization and consolidation opportunities, such as identifying under-utilized servers that would be prime virtualization candidates
- Validate and troubleshoot performance before, during and after the cutover to ensure project success
- Assess current utilization and performance of existing applications and networks

Simplify and Accelerate the Discovery Process

SteelCentral NetProfiler simplifies the inventory process by providing flexible, powerful reporting that can be used for discovering IP hosts anywhere on the network. By leveraging a single data repository that de-duplicates and unifies flow records from the existing infrastructure, with the option to add packet-based probes to augment flow data with performance details and application recognition, a complete inventory of IP hosts on the network can be realized.

The reporting capabilities of NetProfiler enable flexible report criteria to discover across the entire network or specific locations. You can zoom in on specific protocols, ports, IPs, etc. For example, it's easy to identify all servers in the datacenter using TCP/7280 (see figure 1).

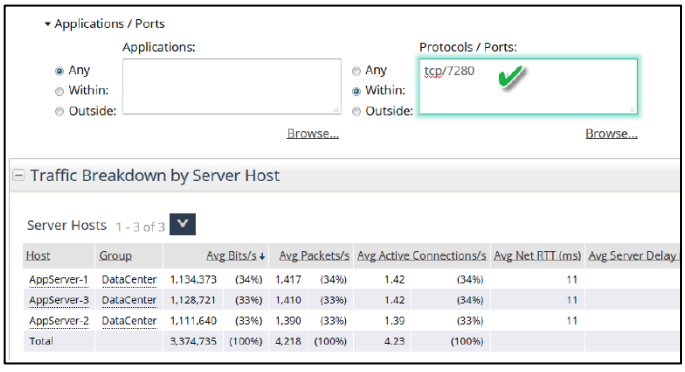
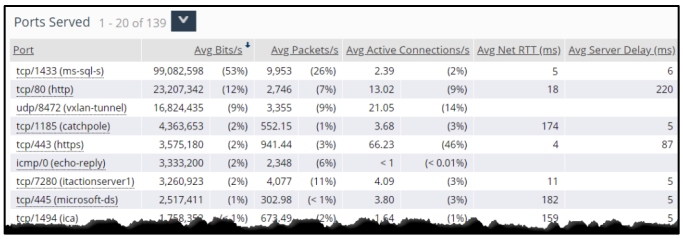


Figure 1 NetProfiler reporting simplifies the discovery of IP hosts using the network.

This information is used to identify top to bottom the IP hosts using the network including throughput, connections, and response times if the network is also instrumented with Riverbed® SteelCentral™ AppResponse. You can filter the results, export to CSV, or even automate the collection with built-in RESTful API support. You could just as easily identify all application ports in the datacenter (figure 2) and use filtering and sorting techniques to view the data you want to see.



Port	Avg Bits/s		Avg Packets/s		Avg Active Connections/s		Avg Net RTT (ms)	Avg Server Delay (ms)
tcp/1433 (ms-sql-s)	99,082,598	(53%)	9,953	(26%)	2.39	(2%)	5	6
tcp/80 (http)	23,207,342	(12%)	2,746	(7%)	13.02	(9%)	18	220
udp/8472 (vxlan-tunnel)	16,824,435	(9%)	3,355	(9%)	21.05	(14%)		
tcp/1185 (catchpole)	4,363,653	(2%)	552.15	(1%)	3.68	(3%)	174	5
tcp/443 (https)	3,575,180	(2%)	941.44	(3%)	66.23	(46%)	4	87
icmp/0 (echo-reply)	3,333,200	(2%)	2,348	(6%)	< 1	(< 0.01%)		
tcp/7280 (itactionserver1)	3,260,923	(2%)	4,077	(11%)	4.09	(3%)	11	5
tcp/445 (microsoft-ds)	2,517,411	(1%)	302.98	(< 1%)	3.80	(3%)	182	5
tcp/1494 (ica)	1,758,358	(< 1%)	673.49	(2%)	1.64	(1%)	159	5

Figure 2 Flexible reporting can focus discovery on what you want to know more about.

Identifying Consolidation and Migration Opportunities

NetProfiler collects a wide range of application-centric metrics that can be applied to IT project planning, such as data center consolidations or cloud migrations. These metrics include:

- Logical inventory of IP addresses
- Application inventory by IP and protocol
- Bandwidth traffic pattern analysis by host, network, location and application
- Worst performing hosts and applications classified by network round trip times, server delays, resets/retransmits

In addition to the discovery process, NetProfiler can identify application dependencies visually and dynamically. For example, to drill into a server IP host to understand its connections on the network, a connection graph is part of the report. This dependency diagram is interactive and can be exported to third-party tools (figure 3). This allows IT to accurately move servers and applications to the cloud or second data center without “breaking” them. It also helps develop appropriate firewall policies that will not disrupt service delivery.

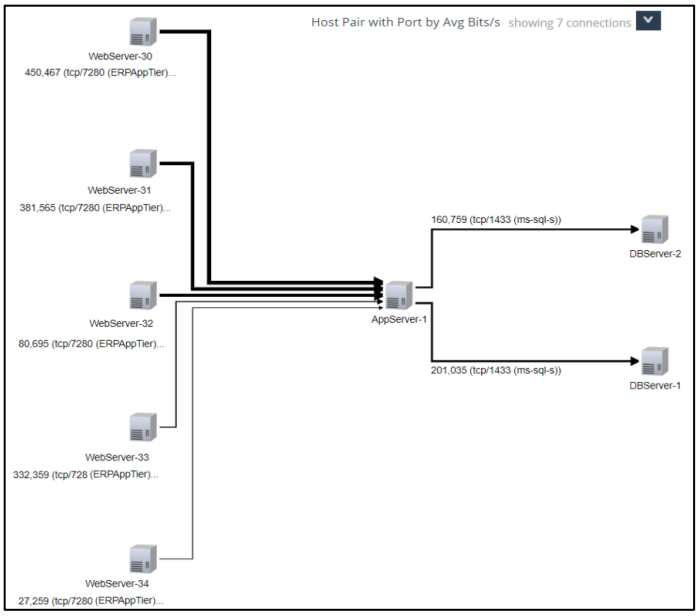


Figure 3 Connection Graphs illustrate the relationships between application components.

Creating Service Maps to Baseline Performance Before and After a Change

Creating application-specific service maps are essential to effectively and efficiently planning and managing consolidation or modernization initiatives, as well as for monitoring end-to-end application performance and identifying problems with greater clarity before, during and after the changeover. The discovery and dependency information enables easy, step-by-step processes to create service maps

Adding a service map begins by identifying an application server—all that is needed to get started is the name, IP address, or CIDR range for the server. The service wizard uses both real-time and historical traffic data to determine the clients or front-end components such as web servers, load balancers or users that have connected to the server within a certain timeframe and the applications, protocols and server with which they connected.

Figure 4 The discovery wizard automates and simplifies the process of identifying all the components and dependencies for a given application.

When the front-end components have been defined, the discovery process is repeated, but this time looking for back-end components—hosts that the application server connects to in the role of client. Back-end components typically include authentication systems, DNS servers, databases, etc. The discovery process can be repeated at each tier to uncover additional dependencies.

The result is a NetProfiler Service Map. Service maps illustrate the relationships between application components that are delivering. Services are viewed in NetProfiler service-level dashboards in terms of service segments, which are defined by a client component, a server component, and the applications and ports in use between them. The line representing the applications and ports in use between two components can be color-coded—red [critical], yellow [poor], green [normal]—to indicate its health status (figure 5).

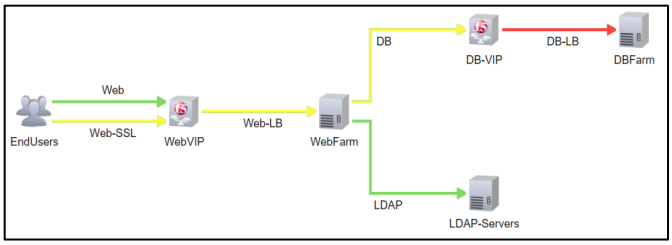


Figure 5 SteelCentral NetProfiler Service Maps leverage behavior-based analytics to profile each tier of an application service.

The service map enables drill-down to provide additional information about the application tiers, such as service performance reports, service incident reports, and traffic analysis for the segment.

NetProfiler continuously monitors application performance for an understanding of anomalous activity, learning performance behavior patterns based on time of day and day of week. This is a powerful combination of being able to report/alert on specific SLA values, in addition to levering machine learning to help identify anomalous behavior that might not be exceeding typical thresholds. Utilization information helps identify servers that are under-utilized and potentially have excess capacity and can be reused in other ways to support consolidation/virtualization initiatives.

Validating Performance

NetProfiler, in combination with AppResponse, can be used to create “before” and “after” snapshots of application dependency maps and performance.

Creating a baseline service map of an application’s dependencies allows administrators to compare the new environment to the old to determine if groups of users, servers, databases, etc. have been inadvertently left out or if certain tiers of the application are missing.

Base-lining performance information provides validation or proof that services are, or are not, performing as accustomed. This information is helpful to understanding if additional steps need to be taken to improve user performance—such as implementing a WAN optimization solution at remote offices—and also in refuting perceptions of service degradation.

Proactive Monitoring and Troubleshooting in All Phases

NetProfiler can be brought into an organization when the change has failed, and IT has little visibility into what has gone wrong. But why wait until the project has failed or been derailed? Using NetProfiler at the start of an IT assessment or change project provide the missing visibility to troubleshoot problems at any stage of the process. Additionally, when the project has been successfully completed, IT still has a network performance management solution to monitor and troubleshoot the new environment.

NetProfiler provides a single, integrated view of all network data for comprehensive analysis and reporting on network and application status, and for troubleshooting network performance and security problems faster than is possible with competitive offerings (figure 6). As a result, the impact and duration of service outages is minimized, and network management costs are reduced. Typical results include over 80% faster problem resolution and more than 30% fewer downtime incidents per month.

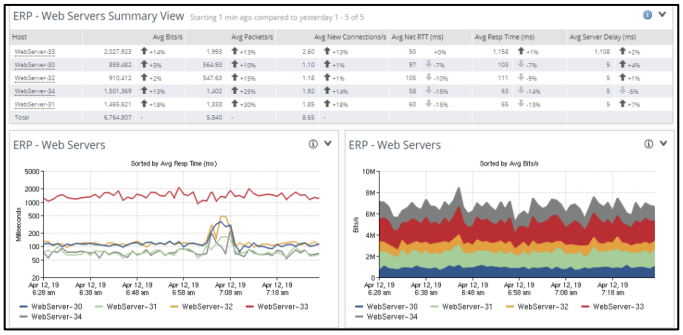


Figure 6 NetProfiler simplifies the task of proactive monitoring and troubleshooting throughout all project phases.

Supporting Security and Compliance

NetProfiler's ADDM capabilities can also assist when establishing and reviewing security and compliance policies. NetProfiler helps uncover all the moving parts of an application, including the hosts, paths, ports, and protocols that need to be secured or monitored for compliance. It helps identify and secure any gaps in coverage that might have been overlooked during the change process, and it also helps find unrelated systems that need to be treated at the same trust level due to proximity.

Understanding where IT assets sit in the network and their dependencies enables the IT organization to focus and rationalize investments. It helps answer questions such as:

- How many firewalls and/or intrusion detection/prevention systems are really necessary?
- What is the best location for them?
- Do I have gaps in my coverage that leave me vulnerable to attack or open to non-compliance penalties and litigation?

In addition, NetProfiler's security analytics automatically monitor for unusual changes in behavior and proactively alerts on changes that could indicate an emerging security issue. Activity that NetProfiler can detect includes unusual surges in bandwidth characteristic of distributed denial of service (DDoS) attacks, host or port scans, the addition of new hosts or server ports, brute force, exfiltration and suspicious connections.

Supporting Disaster Recovery

Once the project is complete, you'll probably need to reassess your disaster recovery plan. With applications and data more distributed than ever—they can reside in the cloud, corporate data centers, remote offices, and/or on user computers—it is sometimes difficult to account properly for every system and application. NetProfiler can provide visibility into many steps of disaster recovery, including:

- Aid in disaster recovery planning by identifying all the components that need to be protected under a DR program
- Validate post-disaster that systems have been recovered and are operating as expected
- Monitor backups to ensure they occur as scheduled
- Identify and troubleshoot "disasters"

NetProfiler Accelerates IT Change

To summarize, having an accurate asset inventory and dependencies map is critical to the planning process for data center consolidation as well as other IT change projects. NetProfiler accelerates IT consolidation by enabling fast, accurate and complete discovery of IT assets and their dependencies. In addition, NetProfiler's application-aware network performance management capabilities can also be leveraged to validate performance and troubleshoot issues before, during and after an IT change event.

NetProfiler provides several benefits over traditional scan or agent-based discovery. These include:

- **Easy to install and use**. Because SteelCentral NetProfiler passively leverages flow data from existing network devices, it provides cost-effective and broad, organization-wide visibility. There is no need to install agents or probes on every server or network segment. The only information needed to start the discovery process is the identity of the application server.
- **Fast time to value**. NetProfiler typically accelerates the process of creating a complete and accurate inventory of the IT environment by more than 60%. Unlike scan solutions that only provide a point-in-time view, NetProfiler uses a historical view of server-to-server communications. This enables NetProfiler quickly identify every connection that occurred—even the backup that runs weekly on Sundays at 2 am—regardless of when you run the discovery. There is no need to scan again and again. Alternatively, uploading agents to every server is time consuming and tedious but is totally unnecessary with NetProfiler. Administrators can get up and running within hours.

- **Cost-effective**. With NetProfiler organizations get two products for the price of one—application-aware network performance management for ongoing monitoring and troubleshooting, and automated discovery and dependency mapping. NetProfiler's application-aware network performance management capabilities are a valuable and necessary tool to monitor and troubleshoot any network, at any stage of the process. These capabilities help you uncover additional consolidation or virtualization opportunities, optimize network architectures, and eliminate waste; avoid problems by receiving early warning of brewing issues; and validate the consolidated environment is working as expected.
- **Mitigate risks**. Organizations can use the increased visibility to moderate the risk of failed cutovers through better planning and by creating before and after snapshots of performance and application dependencies.
- **Seed scan/agent solutions**. If application configuration information is required, the use of scans or agents may be necessary. SteelCentral NetProfiler discovery data can be used to identify where to place agents or which servers require credentials to scan. For example, if a data center has 200 servers, but only the 15 Oracle servers are of interest, NetProfiler can quickly and easily identify them—including the Oracle servers assumed to be used only for development but are in production. NetProfiler shortens time and expense of deploying agents by limiting the scope of the project to a more manageable size.
- **Accelerate end state savings**. Because SteelCentral NetProfiler accelerates the planning process, shortening and improving the quality of the outcome. Projects are completed sooner and the desired benefits—the cost savings, efficiencies, etc., are also achieved faster.

SteelCentral Platform

NetProfiler is also an integrated module of a complete digital experience platform. Riverbed SteelCentral is the only end-to-end solution that blends device-based end user experience, infrastructure, application, and network monitoring to give you a holistic view of your users' digital experience. Drive digital transformation with Riverbed's Digital Experience Management platform.

riverbed

Riverbed®, The Digital Performance Company™, is united in our purpose of *Advancing the Human Experience in the Digital World*. Behind every digital experience is a human one, and Riverbed enables organizations to measure digital experiences and maximize digital performance so they can deliver better and more powerful human experiences—for customers, employees, partners, patients, and citizens. Riverbed's Digital Performance Platform includes a combination of Digital Experience Management and Next-Generation Infrastructure solutions that ensure superior digital and user experiences, provides new levels of operational agility and accelerates business outcomes. Riverbed's 30,000+ customers include 100% of the *Forbes* Global 100. Learn more at riverbed.com.