LEARNING MADE EASY

Riverbed Special Edition

Digital Experience Management

for dummies®
A Wiley Brand

Apply AI to IT operational big data

Gain a complete view of digital experience

Delight your customers and employees

Brought to you by riverbed®

Lawrence C. Miller

About Riverbed

Riverbed®, The Digital Performance Company™, is united in its 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 (DEM) and digital networking solutions that ensure superior digital and user experiences, provide new levels of operational agility, and accelerate business outcomes. Riverbed's 30,000+ customers include 100 percent of the Forbes Global 100. Learn more at **riverbed.com**.

Digital Experience Management

Riverbed Special Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

Digital Experience Management For Dummies®, Riverbed Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-61934-5 (pbk); ISBN: 978-1-119-61935-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie Burchfield-Leighton

Editorial Manager: Rev Mengle

Acquisitions Editor: Ashley Coffee

Business Development Representative: Karen Hattan

Table of Contents

Introduction

We live in a digital world where technology is redefining what's possible. From engineering and IT to individual lines of business, modern enterprises need to measure, manage, and maximize digital performance to deliver highly engaging, secure, and satisfying user experiences. Unfortunately, traditional monitoring solutions are typically focused on a single technology area and often can't scale to support the needs of today's dynamic, distributed environments. They miss the big picture and what matters most: the human experience.

Digital Experience Management (DEM) provides a clear understanding of how digital services are performing and impacting the business. It enables you to deliver high-performing, secure digital services even in highly dynamic and distributed cloud-native environments and identify opportunities for developing new or improved features that are critical for customer satisfaction and retention. DEM improves collaboration among development, operations, network, infrastructure, and security teams and minimizes finger pointing by delivering a shared platform and single version of the truth. Most importantly, by leveraging artificial intelligence (AI), machine learning, powerful visualizations, and big data, DEM enables proactive identification and resolution before issues negatively impact your customers, employees, or bottom line.

About This Book

Digital Experience Management For Dummies, Riverbed Special Edition, consists of five chapters that explore the following:

- The implications of poor performance and the need for DEM (Chapter 1)
- Performance management in complex cloud and mobile computing environments (Chapter 2)
- The role of big data and Artificial Intelligence for Operations (AIOps) in DEM (Chapter 3)

- How to leverage network and infrastructure monitoring for better performance and security (Chapter 4)
- Practical strategies to get the most out of DEM (Chapter 5)

Each chapter is written to stand on its own, so if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backwards).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless. Mainly, I assume that you work in an IT role for your organization. Perhaps you work in application development or you're an application owner, such as a director or vice president of application development, application support, or DevOps. Or, you may be responsible for end-user services such as a service desk, help desk, or desktop support. You might also be responsible for IT operations and/or network operations. As such, this book is written primarily for technical readers.

If any of these assumptions describe you, this is the book for you! If none of these assumptions describe you, keep reading anyway. It's a great book, and when you finish reading it, you'll know why managing the digital experience is the way forward for enterprises today.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much I can cover in 48 short pages, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book, where can I learn more?" try the following resources:

- **`www.riverbed.com/solutions/digital-experience-management.html`:** You can view webcasts, read whitepapers, and learn how your peers are using DEM.
- **`www.riverbed.com/blogs.html`:** Keep up with the latest events and read current articles on the Riverbed blog.

IN THIS CHAPTER

- Addressing internal and external business challenges
- Optimizing the user experience with Digital Experience Management
- Understanding how performance impacts the bottom line
- Measuring the value of digital transformation initiatives

Chapter 1
Advancing the Human Experience through Digital Performance

This chapter explores the performance challenges facing today's digital businesses and how Digital Experience Management (DEM) provides much-needed visibility into both the employee and customer user experience and the underlying applications, network, and infrastructure layers. By using DEM, you can quantify and optimize the effectiveness of your digital transformation initiatives.

Understanding Modern Business Challenges

To build customer loyalty, streamline operations, and increase workforce productivity, today's enterprises must develop and deliver exceptional digital services faster and better than their competitors. For IT and business leaders, a sharp focus on the digital experience of end-users — from application design through application delivery and consumption — is vital to success.

In fact, according to IDC, 85 percent of enterprise decision makers say they have a timeframe of two years to make significant inroads into digital transformation, or they'll fall behind their competitors and suffer financially.

By focusing on DEM, IT teams can optimize the human experience to produce better business outcomes as users interact with digital apps and services. But delivering an exceptional digital experience is easier said than done. The bar is constantly being raised as customers and employees increasingly expect ever more engaging, secure, and reliable digital services.

WARNING

Such expectations are a challenge in and of themselves, but IT environments and processes have become exponentially more complex and difficult to manage. These issues are shown in Figure 1-1. Poor digital performance may be due to any number of issues and is especially difficult to diagnose in highly dynamic and distributed containerized application environments.

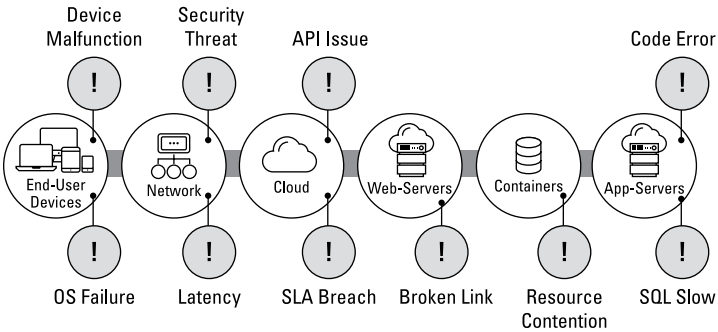

FIGURE 1-1: Potential sources of poor digital performance.

To truly succeed, IT and business leaders must address the following internal challenges:

- **Lack of insight into how digital services are adopted and used:** Measuring the success of digital services is critical for making informed planning decisions and justifying future investments. IT has typically focused on service quality metrics such as resource consumption and availability of infrastructure components. However, these metrics don't provide performance insights as experienced from the end-user's perspective. As a result, they can neither quantify how a digital service is contributing to the company's bottom

line nor identify where opportunities exist to drive future growth. Without these insights, it's difficult for application owners to know if or how users are adopting new digital services and what the overall impact is on the business. This, in turn, hinders future development and initiatives.

- **Aggressive development pipelines:** Organizations are increasingly embracing DevOps and cloud-native technologies to quickly and continuously develop and deliver new or enhanced digital services. However, accelerating development and release cycles means little if new applications and features are buggy or underperform for users. Yet, all too often, bugs and performance issues find their way into code as feature sets grow. Testing in lab environments is insufficient because it rarely represents real-world conditions in which thousands of people may simultaneously access an app that's delivered on distributed infrastructure across multiple cloud platforms. As a result, increased rates of change can cause service degradations or outages, frustrating IT teams and end-users alike. Application performance must be continuously fine-tuned with high definition monitoring in both development and production so DevOps teams can proactively find and fix issues early — before users complain.
- **Limited cross-domain understanding:** Today's digital services are highly complex. They can span on-premises and cloud-based resources, are delivered across a mix of private and public networks, and must be optimized for multiple device types. In addition, increased reliance on microservices, containers, and third-party services means today's application topologies are more distributed and dynamic than ever before. Any flaw — whether it's a system dependency, coding issue, network congestion, or a problematic user device — can slow an application and disrupt the resulting digital experience, negatively impacting customers and employees.
- **Fragmented tools and IT silos:** A cross-domain understanding of applications and the networks, infrastructure, and devices they run on is essential to managing the digital experience. Most enterprises today use multiple disparate tools to monitor network, IT infrastructure, and application performance, as well as security and other critical functions that comprise the digital experience. Unfortunately, more isn't better. This approach creates IT silos and fosters an

unproductive environment in which IT teams shift blame and the digital experience suffers. As a result, teams spend too much time reactively tackling performance issues, which diverts valuable time and resources away from more strategic business initiatives.

Three Critical Components of DEM

DEM enables business leaders, IT executives, application and infrastructure owners, and end-user services teams to validate that their digital transformation investments are paying off. To succeed, IT and business leaders need a comprehensive, integrated solution that allows them to securely manage the digital experience of every user to build customer loyalty, streamline operations, and increase workforce productivity.

But DEM is much more than simply collecting metrics — CPU and memory consumption, battery strength, boot time, and so on — about device health and performance. These metrics certainly impact the digital experience and measuring them is necessary, but they aren't enough to capture the actual digital experience. To take that next step, you need to do three things well:

- Monitor the actual user experience — what users see as applications render on the screens of their devices. And because today's mobile workforce relies on all types of devices to do their jobs, you must monitor the experience on laptops, PCs, virtual desktops, and mobile devices. You need to cover every type of application in the enterprise portfolio — thick client, web, SaaS, and mobile because this is the modern digital experience.
- Provide end-to-end monitoring and performance insights for key stakeholders, allowing companies to proactively measure, assess, secure, and improve today's digital experiences. It requires a unified approach across end-user devices, applications, networks, and infrastructure both on-premises and in the cloud (see Figure 1-2).
- Deliver cross-platform analytics to surface IT and business insights from big data. This means using artificial intelligence (AI) and machine learning to identify patterns, detect anomalies, visualize interdependencies, and automate remediation.

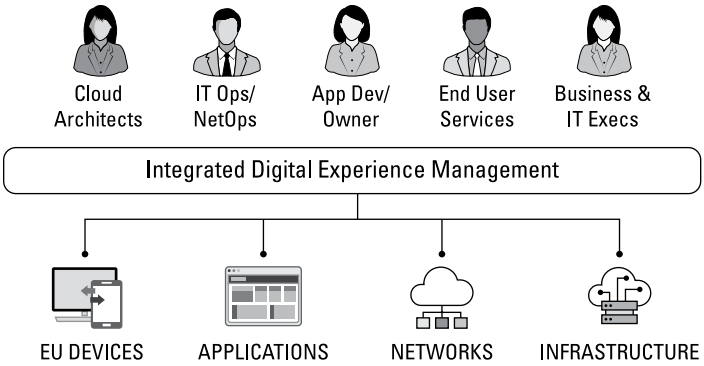

FIGURE 1-2: Business-centric, cross-domain intelligence across end-user devices, application, networks, and infrastructure.

Calculating the Financial Impact of Performance

Today, business is digital. When applications are slow or unresponsive, they cost the business in terms of lost employee productivity, lower customer satisfaction, and lost revenue and company value. Consider the following data:

- According to IDG, 32 percent of IT decision makers say that digital business has already helped their organizations achieve revenue growth, with an average of a 23 percent increase.
- According to research by Information Technology Intelligence Consulting (ITIC), one hour of downtime costs over $100,000 for 98 percent of organizations, and $1-5 million for one-third of organizations, on average.
- According to Forrester, 12 percent of global information workers say that their devices and apps break often and cause too many disruptions to their work. Just 30 percent say they know how to get the technology support they need to be productive.

It stands to reason that a negative digital experience for your customers and employees will result in a negative financial impact to your business.

Recognizing that a poor digital experience can have a significant negative financial impact, organizations are increasingly turning to DEM to proactively ensure a positive digital experience for their customers and employees. DEM not only helps ensure high-performing, secure digital services, but also it can quantify the impact of slow performance and downtime on the bottom line. IT organizations can determine which issues to work on first based on the criticality to the business. Some issues can even be addressed using automated remediation.

Managing the Impact of Change

Digital transformation is all about IT change:

- Migrating apps and services to the cloud to improve agility
- Executing a mobile-first strategy to connect to customers wherever they are on the device of their choice
- Delivering an omnichannel user experience to keep customers engaged

Enterprises are spending millions on digital transformation initiatives such as these to create an exceptional customer experience, improve workforce productivity, and increase competitiveness and market share.

But how do you know these IT changes are really producing a better digital experience for your customers and employees? Unless you measure it, you don't. Measuring — and proactively managing — the digital experience of your end-users is the only way to ensure your digital transformation initiatives are truly making things better.

DEM solutions automatically baseline the performance before the change and compare the performance after so you can quantify and visualize the impact of application, infrastructure, or device changes on your users. Did the device upgrade pay off in better performance for your employees? Is the digital initiative driving the intended results for your customers?

REMEMBER

Make sure that you measure the impact of strategic and tactical IT changes in terms that are meaningful to the business. After all, the traditional metrics by which IT is measured, such as uptime, latency, errors, and so on, don't really tell your business executives whether a change enables their employees to be

more productive or customers to enjoy a better digital experience and be served more efficiently. Monitoring the performance of business activities performed by the end-user closes the gap between traditional IT metrics and meaningful business metrics. Business activities are company-defined user interactions with applications in the context of a business process, such as "look up a patient record" for a medical organization, "process a claim" for an insurance company, or "check inventory" for a retailer. Business activities not only represent a company's fundamental business processes, but also they are common language, equally understood by IT and the business. So, they are the best basis on which to evaluate and communicate the impact of IT change.

FINANCIAL SERVICES CASE STUDY: REFRESH CYCLES

Many organizations deal with the significant costs and benefits of device upgrades by staggering their refresh cycles over a period of several years. A global financial services company planned to refresh its entire device estate over a six-year period and budgeted a $30 million annual investment accordingly. But by using DEM to analyze device and application performance, the end-user services team identified that less than half of the devices targeted for refresh in the current year actually needed it. In other words, device and application performance were acceptable for the users with their current device configurations. In addition, the team determined that a modest memory upgrade would improve the performance to an acceptable level on another 5 percent of devices. The net result was a cost avoidance of about $10 million out of the $30 million budgeted for device upgrades annually.

IN THIS CHAPTER

- Extending Digital Experience Management to the cloud
- Recognizing performance challenges in SaaS environments
- Getting visibility into microservices and containers
- Managing the digital experience on any device

Chapter 2
Managing Performance Across Complex Environments

This chapter explores the growing complexity in modern business environments — including cloud, Software-as-a-Service (SaaS), cloud-native apps, and mobile computing — and how Digital Experience Management (DEM) can improve digital performance in highly distributed, dynamic environments. In these complex environments, visibility is key and DEM helps fill in the gaps in siloed tools and applies advanced analytics and machine learning to surface key insights, ensuring you provide excellent digital experiences to your customers and employees.

Hybrid and Multi-Clouds

The cloud is here to stay. According to the *RightScale State of the Cloud Report*, 96 percent of companies are now using the cloud, 71 percent have adopted a hybrid cloud strategy, and 81 percent have adopted a multi-cloud strategy leveraging nearly five clouds on average.

Although the cloud is a key enabler of enterprise digital transformation initiatives and the modern digital experience, it also introduces some complexity. As a result, IT organizations themselves must transform — specifically, the tools they use to manage the digital experience must extend to the cloud.

Industry analyst Enterprise Management Associates (EMA) reports that companies can trace 45 percent of enterprise network traffic to public cloud applications and services, including SaaS and Infrastructure-as-a-Service (IaaS). This percentage is also expected to grow.

WARNING

Some monitoring solutions support only on-premises deployment and/or provide limited visibility into multi-cloud and hybrid environments. Cloud and SaaS vendors tools, while useful, typically end where their environment ends. This means that you may lack visibility into the end-to-end transaction, which is critical for troubleshooting. Understanding how the application renders on the user's device and analyzing a unified, cross-domain data set help ensure customer and employee satisfaction.

SaaS Applications

Nearly every modern enterprise today relies on SaaS applications for at least some of their business-critical functions. A few popular examples include

- ADP (payroll)
- Box and Dropbox (file storage)
- Concur (expense management)
- Confluence and Slack (team collaboration)
- Jira Atlassian and ServiceNow (service desk)
- Salesforce (customer relationship management)
- Office 365 and Google Apps (workforce productivity)

  Businesses have clearly embraced the SaaS model. For example, Office 365 adoption is growing with one in five users relying on Microsoft Office 365.

WARNING

While the SaaS model removes the need to manage onsite deployments and allows for frequent upgrades, some challenges must be addressed:

- In a SaaS environment, IT organizations typically have little or no visibility into performance issues negatively impacting the end-user's digital experience. This lack of visibility means IT teams are relegated to a reactive "firefighting" role when problems arise. For example, rather than being able to proactively monitor and diagnose potential issues before they're noticed by end-users, on average, more than three out of five Office 365 issues are first reported by end-users, according to a survey by Wakefield Research.
- After an issue is identified and reported, IT teams are further hamstrung by a lack of integration between the SaaS environment and their application and network monitoring tools. Getting a SaaS application performance issue resolved often involves the customer's help desk, desktop support, and internal network teams, IT management, Internet service providers, and the SaaS vendor, which increases delays, frustration, finger-pointing, and costs.

TIP

To proactively detect performance issues in SaaS applications, IT teams should augment their SaaS vendor's monitoring tools and existing service-level agreements (SLAs) with a DEM solution that provides performance insight from the end-user's perspective and provides context in terms that the business can understand. DEM solutions provide the basis for a data-driven discussion with SaaS vendors because they're able to break down the source of delay and identify issues quickly.

Containers and Microservices

Software development has been transformed by the cloud as enterprises replace their monolithic applications with modular, cloud-native applications. The cloud-native approach to development breaks applications into small chunks of functionality, called *microservices*, to drive agility. These microservices are then frequently deployed within resource-efficient containers that can be individually scaled.

REMEMBER

Microservices are self-contained units that enable continuous integration (CI) and continuous delivery (CD), improve application quality, and reduce time to market.

Developers working on a microservice can focus on optimizing a single function, without worrying about the other functions that will eventually comprise the application. They can implement bug fixes and enhancements at any time without waiting for major application upgrades. And while there's no law that says microservices must run inside containers, they usually do so they can be scaled up or down to efficiently meet business demands.

As container adoption has grown, a multitude of orchestration tools and platforms from Kubernetes to Amazon's Elastic Container Services (ECS) and Pivotal Cloud Foundry have come on the scene. Some of these provide an enterprise framework for integrating and managing containers at scale. Orchestration tools enable you to quickly scale and provision dozens or even hundreds of containers at a time. You can also manage the data storage and network communication between containers.

WARNING

Microservices-based applications are ideal for taking advantage of container auto-scaling and auto-provisioning capabilities. However, the IT operations job just got a whole lot trickier because containers and microservices environments are hyper-distributed, transient, and multi-stack, which makes monitoring and troubleshooting them infinitely more complex.

The modern run-time environment includes thousands of components interacting in complex, rapidly changing patterns over multiple tiers. Traditional monolithic application architectures also place relatively light burdens on the network. After the application is loaded and running, most of the activity takes place within the application server and involves only a small amount of external communication. It's different in a microservices architecture in which the application environment can have thousands of distributed components. These components, often deployed in containers, constantly interact with each other over the network. As a result, there's an increased burden and dependence on the network.

Traditional monitoring tools strain to keep up in modern, cloud-native environments — they're not built for big data scale, so they resort to sampling transactions and discard a large proportion of the data that's collected. Sampling metrics once every

few minutes is good enough to discover the up/down status or the overall utilization of a server or VM. However, a minute is an eternity in a cloud-native environment. The only way to get an accurate, actionable understanding of application performance is to monitor in container time — that is, capture every transaction and collect second-by-second metrics.

REMEMBER

Managing today's dynamic cloud-native environments requires the highest levels of data quality and completeness. That's where big data technology (I discuss this in Chapter 3) comes in. It allows you to scale with the volume and velocity of data generated by today's application infrastructure without sacrificing granularity and depth, preserving the full information content of all the system, application, and network data.

TECHNICAL STUFF

According to *Digital Enterprise Journal*, 18 times more data is collected, on average, from monitoring components and dependencies in container-based versus more traditional monolithic environments.

Workforce Mobility

Seventy-nine percent of employees report greater workplace satisfaction when they have the freedom to choose how they accomplish their work, according to Globoforce. From the corner office to the corner coffee shop, your employees need fast, reliable, and secure access to corporate resources from their smartphones, tablets, and laptops to be productive no matter where their work takes them.

Bring your own device (BYOD) policies and the ever-growing number and types of apps and devices complicate the role of end-user support teams. Then, there are the privacy and performance concerns that come up with monitoring the digital experience on personal mobile devices:

- "You're not going to put a piece of monitoring software on my device."
- "I don't want you tracking my location or seeing what I do on my phone."
- "I don't want your monitoring software to slow down my device."

The solution to these mobile device challenges is to instrument the app, not the device. For in-house apps, your developers can build in instrumentation using a mobile software development kit (SDK). For third-party apps as well as in-house apps, non-developers can use a mobile wrapper to instrument an app without tagging the code. Instrumented apps can then be distributed via your enterprise app store.

TIP

Monitor the user's experience to see the actual performance — that is, how the application renders on the user's screen. It's best to correlate three streams of data:

- **Users and their locations:** Automatic discovery of user attributes such as identity, role, department, office and geographic location, subnet, and virtual private network (VPN)
- **Devices and their operating systems (OS):** Automatic discovery of key attributes of every physical, virtual, or mobile device, including make and model, number of cores, disks and shared drives, OS type, version and service pack, boot services, running processes, and the top processes consuming processor, memory, and input/output (I/O) resources
- **Applications, processes, and health indicators:** Automatic discovery of all local, cloud, web, or instrumented enterprise mobile apps running on any physical, virtual, or mobile device

IN THIS CHAPTER

- Bringing big data power to Digital Experience Management
- Uncovering the value of AIOps
- Considering key issues when automating remediation

Chapter 3
Unlocking the Power of Big Data and AIOps

Artificial Intelligence for IT Operations (AIOps) refers to the application of big data analytics, artificial intelligence (AI), machine learning, and automation to IT operations use cases. In this chapter, you discover the power of big data analytics and AIOps in Digital Experience Management (DEM).

Understanding Why Big Data Is Critical for DEM

Traditional solutions typically rely on sampling incomplete datasets for diagnostic information to enable monitoring and alerting. But this approach falls short for DEM, particularly for modern applications, in the following four key areas:

- **Completeness:** Tools that sample transactions or only snapshot performance data based on exceptions provide a fragmented, incomplete view that's insufficient for troubleshooting the long tail of performance issues.

- **Context:** Some tools discard payload and metadata information, which obscures the business relevance that helps prioritize efforts and makes each transaction unique.
- **Correlation:** In today's distributed environments, transactions can traverse thousands of application tiers. Without a *transaction-centric data model,* it is difficult to provide a clear end-to-end picture. Data must be mapped from the end-user transaction across the backend application components and stitched together into a single trace — for every single transaction.
- **Causality:** Without high definition metrics for the application environment, it's easy to miss processor or memory spikes entirely or be misled by "aliasing" effects. Second-by-second metric data is needed to accurately pinpoint root causes such as shared resource issues and other infrastructure dependencies.

Any time data is sampled, filtered, or aggregated, it provides only a snapshot of the real picture, and the results may be inaccurate. Modern applications are highly dynamic and distributed and require a scalable approach to big data that supports

- **Volume:** Petabytes of data generated daily must be transferred, processed and stored. The application environment is transient and must be measured at a high frequency (ideally, one second intervals).
- **Velocity:** Billions of user transactions per day is typical for large and highly digitized enterprises.
- **Variety:** Every transaction is unique; data can be application code traces, unstructured log data, performance metrics, transaction parameters, and so on.

WARNING

Using averages instead of collecting high resolution metrics can flatten out spikes in your data. This means that you may underreport or even miss performance issues impacting your business-critical applications.

Big data technology enables IT to collect, store, analyze, and access petabytes of unfiltered source data across domains — free from inaccuracies and blind spots due to sampling or averages. By capturing, managing, storing, and analyzing all data, big data enables deeper and more accurate insights into the digital experience.

A big data approach to DEM scales to collect all the relevant application workload and application environment metrics and then applies advanced analytics to surface insights. In contrast, some tools collect transaction performance data less frequently and provide less granularity into the application stack and attempt to fill in the blanks with algorithms. It's also important to include metadata because it provides valuable business context. For example, metadata can tell you whether a shopping cart transaction that failed totaled $5 or $500 so that you can prioritize your optimization and troubleshooting efforts accordingly.

Big data insights can be used in DEM in the following key areas:

- **Capturing the "long tail" of performance problems:** IT teams often spend valuable time chasing the symptoms of an application performance problem and looking for a "silver bullet" — one root cause that, when fixed, resolves all the performance problems. However, the reality is that applications are often plagued with multiple performance problems and there is no silver bullet. A big data approach helps IT divide and conquer the long tail of problems more efficiently and identify multiple potential causes contributing to poor performance in a single application.
- **Providing definitive analysis:** Big data mitigates uncertainty and overreliance on tribal knowledge. In the absence of precise data, performance analysis may lean heavily on the troubleshooter's experience, which may or may not be applicable.
- **Diagnosing intermittent problems:** Intermittent performance problems tend to be the most challenging to diagnose for several reasons:
  - The conditions of the failure are often elusive.
  - Recurrence is unpredictable.
  - There are few opportunities to observe the problem.
  - The environment itself is changing during these long-running problems.

  A big data approach addresses all these challenges and enables IT to quickly diagnose challenging, intermittent problems, even if the application environment has changed. With big data, it isn't necessary to reproduce the failure conditions because the diagnostics data is continuously

captured and stored in full detail to aid in root cause analysis regardless of when the problem occurred.

- **Gaining visibility into highly dynamic environments:** A big data approach is effective in diagnosing problems in cloud, virtualized, or containerized environments (see Chapter 2). In these ephemeral application environments, the application infrastructure is constantly changing, and a triggered/sampled approach may miss the state changes, which occur as components are spun up and spun down.
- **Understanding the user journey:** Understanding the user population is invaluable in drawing insight into global performance trends but is sometimes insufficient in understanding the steps that could lead to significant performance problems. A single user action can lead to performance problems for the entire application and a big data approach guarantees that all forensic data is available to reconstruct the breadcrumbs of the incident.
- **Enabling continuous performance improvement:** Big data is more than just monitoring and diagnostics. It can be used to methodically reduce performance bloat and provide the basis for forensic exploration or code audit. The availability of deep performance data becomes the basis for continuous performance improvement. Applications are continually changing with new feature releases and tend to accumulate technical and performance debt. With complete performance data and big data analytics, DevOps teams and developers can better understand where time is being spent.
- **Seeing the bigger picture:** With big data, you can uncover performance problems and patterns that impact the entire application environment not just a single application component. After a problem is discovered in a single application, analytics applied to this big data can help identify other applications that have the same problem or that are potentially at risk.


TECHNICAL STUFF

While capturing detailed transaction records for every user action and backend activity does generate a lot of data, DEM is no different than other use cases for big data in this respect. The same techniques and architecture — for example, leveraging highly optimized, non-relational data stores — apply to DEM. Big data DEM typically uses proven streaming and complex event processing architectures. Just as in Hadoop clustering, a DEM big data

platform can also federate data processing and analytics across the platform components. With a three-tier processing approach, the in-app collectors do minimal work and pass the raw data to a local processor, which then sends the data to the central engine after performing compression and some base analytics. This approach scales far better than a two-tiered approach with in-app collectors that can tax the application and/or the backend system.

Continuously capturing all transactions in detail also results in a system that's far more resilient and easier to manage because there's no reliance on complex rules, inspection, or a trigger engine that needs to be configured and maintained. There is undoubtedly more data persisted with this approach, but managing storage is a technical problem that has been largely solved.


TIP

Overhead is a key concern for any technology that's sitting in line with the application. To minimize overhead, lightweight agents can dynamically discover every component in the application stack, record every critical method and application call in a transaction, and then compress and stream transaction data. Using a three-tier architecture for big data DEM eliminates the need to add compute or processing power to the application stack being monitored.

Leveraging AIOps in Digital Experience Management

Artificial Intelligence for IT Operations (AIOps) addresses the need in modern IT operations to make sense of large quantities of mostly structured, specialized, cross-domain IT data. IT operations teams can leverage AIOps to drive continuous insights and automate remediation faster than humanly possible.

The key to unlocking the power of AIOps is to leverage high-quality, structured data from multiple IT domains. AIOps helps surface issues and causes beyond the usual suspects that you may not have thought to look for, point you in the right direction for faster troubleshooting and remediation, and proactively alert you when normal operating thresholds are breached. It does all of this faster than humanly possible using AI and machine learning to surface patterns and detect anomalies.

Patterns can tell you quite a lot about your environment. They can point forward in time to potential issues that could develop into incidents or can be used to understand usage profiles that inform business or roadmap decisions. Looking backwards, patterns developing over time indicate potential root causes of issues and provide valuable clues for troubleshooting. When patterns show up in data, this usually points to something warranting further investigation.

To surface what's important, AIOps works with data in a number of ways:

- **Visualization:** Intuitive maps, graphs, and charts immediately surface key information and relationships in data. Visualizations can be created at the user transaction level to make large volumes of data meaningful and to better understand business impact. This includes topology maps that capture the dynamic relationships between microservices and their underlying dependences so you can better detect resource contentions.
- **Pattern recognition algorithms:** While some patterns are easily identified visually, others lie hidden inside vast amounts of data. The primary goal of machine learning is to automatically surface these patterns by looking for regularities in datasets. With unsupervised learning, the more granular and complete the training dataset, the better the results you can expect.
- **Automated anomaly detection:** Anomaly detection is the ability to statistically learn what's normal and what's not for different sets of transactions. It proactively watches for transactions and metrics that aren't behaving as they should and, if done right, takes seasonal variance into account.
- **Correlation:** By statistically correlating key performance indicators across all application tiers, the system can find groups of metrics on tiers that are spiking in tandem. This narrows down the set of possible culprits for a troubleshooter to investigate, which is especially helpful in chasing down performance issues in distributed containerized and microservices environments with thousands of nodes.
- **Event management:** This is one of the first areas that machine learning was applied to in IT analytics. What's top of mind for IT today is to build more actionable context into alerts (events) and optimize the incident management

workflow by incorporating automated remediation and cross-domain root cause analysis.

REMEMBER

The insights driven by AIOps are only as good as the data provided. Factors to consider include

- **Data granularity:** By collecting data at higher frequencies (for example, one-second intervals rather than one-minute intervals), IT teams can more reliably identify resource contention patterns and troubleshoot issues, especially in highly dynamic environments where state changes occur on short time scales.
- **Observability:** Observability represents a "shift left" for monitoring as developers take on the task of building applications able to externalize their internal state early in the development lifecycle. As observability becomes the de facto standard, there has been a staggering increase in the amount of data generated by modern apps.
- **Multiple data sources:** AIOps uses traditional monitoring sources across all IT functions, as well as newer observability-based sources. Examples include transaction trace data, user and device data, application log data, observability data, infrastructure metrics, and network packet and flow data.
- **Data completeness:** At the end of the day, analytics are only as good as the datasets to which they're applied. Incomplete or unreliable datasets will inevitably lead to wrong or inconclusive results. You won't find the needles in your haystacks if you're only examining a handful of hay from each stack.
- **Scalability:** The term *scalability* has evolved from the ability to support large enterprises to the ability to support increasingly large volumes of metrics and data. The reality of monitoring modern, hyperscale cloud-based environments is a big data reality where the application environment changes rapidly on very short time scales.

Leveraging Automation and Remediation

While the AIOps system can find meaningful correlations, correlation isn't necessarily causation. Every infrastructure environment is unique, and every problem is different. Training neural

networks to recognize general failure scenarios and root causes is a difficult AI problem. This is where purely algorithmic approaches need to be bolstered with expert knowledge — embedded into the algorithms themselves — to improve outcomes for specific sets of problems.

In the infrastructure context, candidates for automation include re-routing network traffic to reduce congestion and free up bandwidth, spinning up additional cloud instances and concurrently expanding the software-defined wide area network (SD-WAN) fabric, and re-distribution of containerized workloads. For other sets of problems, such as code errors, the system may simply present prescriptive or actionable conclusions to the operator.

Most IT organizations have runbook processes that specify the actions for IT to take in response to commonly expected problems. These processes clarify how to analyze the problem conditions, diagnose the issue, then fix it, based on a set of recovery actions. The recovery action is composed of either manual steps or running scripts to clear the condition and verify proper operation.

These runbooks are ideal candidates for automated remediation, but it's important to consider when a fix should be automatically applied. Some key questions to ask include the following:

- How frequently does this problem occur?
- What is the impact/criticality when the problem occurs?
- Does the problem manifest itself in the same way each time or is there variability?
- How long does it take to fix? (For example, you may want to have a human examine the issue before proceeding if it will cause a two-hour system reset.)

After you've determined that the fix can and should be automated, AIOps systems can be enabled to support automated remediation. For audit purposes, the system can maintain a log of remediation actions taken, their success or failure, and who implemented them. This self-service capability results in a number of advantages:

- Improved user satisfaction
- Reduced trouble ticket volume and duration
- Improved first-level resolution rates

TIP

Although automated remediation is powerful, human judgment still plays a critical role. Not all activities can or should be automated. For example, any automation requiring a lengthy system reboot should be carefully evaluated, allowing the user to determine when the reboot should be executed.

REMEMBER

The power of AIOps is in analyzing IT big data and taking action faster than what's possible by humans, to drive better business outcomes. IT organizations can benefit from AIOps, leveraging machine learning and visualizations across extremely large, cross-domain datasets. Using AIOps, IT can accelerate root cause analysis, automate remediation, and ultimately drive better business outcomes and proactively manage the digital experience.

IN THIS CHAPTER

- Understanding the role of network and infrastructure monitoring in DEM
- Applying network data to strengthen your security posture
- Enabling integration and collaboration across teams

Chapter 4
Improving Performance and Security Using Network and Infrastructure Insights

Across-domain understanding of applications and the networks, infrastructure, and devices they run on is essential to managing and securing the digital experience. Performance issues can occur in a user's application or device or in the underlying network or infrastructure. A lack of visibility into any one of these areas creates a blind spot in your user's digital experience.

In this chapter, you discover how to integrate network and infrastructure monitoring as part of your Digital Experience Management (DEM) strategy in order to improve both performance and security.

The Importance of Integrated Network and Infrastructure Monitoring

Modern digital businesses need secure, reliable networks more than ever before. According to Digital Enterprise Journal, 68 percent of organizations say the role of the network has become more strategic, and 41 percent of companies use IT operations data for business purposes. Maintaining a high-performing and secure network in today's hybrid cloud architectures is particularly critical to businesses and requires a broad view across IT domains.

As enterprises adopt disruptive digital transformation strategies and initiatives, they need tools that let them quickly and easily monitor their users' digital experiences, spanning from the datacenter to individual end-user devices. To support digital transformation, IT organizations need to move beyond traditional network and infrastructure monitoring tools that provide siloed root cause data. DEM provides complete visibility, including network and infrastructure monitoring that's tightly integrated with your application and end-user experience monitoring so you get the whole picture from end to end.

Network visibility ensures that your network team and monitoring solutions can see and interpret everything happening on a network. Visibility encompasses device discovery, network performance and security issues, and topology mapping. No matter how large and complicated your enterprise network gets, full visibility is a necessity for network monitoring solutions and DEM practices.

Why is full network visibility important for network monitoring? According to Enterprise Management Associates (EMA), for a DEM implementation to be successful, it must extend across the full IT infrastructure stack and support and unify stakeholders in the decision-making process and active responses. This means integrating infrastructure monitoring and security monitoring tools and processes as well and applying artificial intelligence (AI) across the full dataset. Other key requirements for an integrated monitoring solution include

- Support for containers and cloud-centric architectures
- Ability to scale across hybrid architectures

- Integration of data with Artificial Intelligence for IT Operations (AIOps) platforms for business and IT insights with analytics and visualizations
- Ability to collect infrastructure metrics from
  - Physical and virtualized servers
  - Networks, including software-defined networks (SDN)
  - Storage infrastructure, including network attached storage (NAS), storage area networks (SAN), and SAN fabrics
  - Databases
  - Hypervisors, such as VMware and Hyper-V


TIP

Start by monitoring the end-to-end transaction, then use integrated network and infrastructure monitoring to drill down into the root cause of network-based issues. Integration will drive faster mean time to repair (MTTR) than "swivel chair" diagnostics — that is, IT operations teams literally swiveling their chairs to pull up multiple tools on multiple screens and attempting to manually correlate all the information.

Network performance management (NPM) solutions monitor enterprise networks that support complex mission-critical applications. Key NPM functions include

- Polling the infrastructure for availability and performance
- Collecting and reporting on flows to understand the who, what, where, and when of network utilization
- Analyzing packets for a deep dive into application performance from a network perspective


WARNING

Many NPM solutions are available to enterprises today. With so many options, it can be difficult to choose just one. And like a kid in a candy store, most enterprise don't choose just one. According to EMA, the majority of enterprises today use five or more IT infrastructure monitoring tools. Unfortunately, more isn't better. The proliferation of tools in the enterprise creates IT silos, further complicates remediation efforts, and fosters an unproductive environment in which IT teams shift blame and spend too much time firefighting issues. As a result, these teams are unable to focus their time and resources on more strategic initiatives and performance and security — and ultimately, the digital experience — suffer.

Flow data can be exported by most network devices, such as routers and switches. It includes the following information: where the data originates, who requests it, where it's going, and what path it takes to get there.

Full packet capture solutions copy a data packet in real-time as it crosses a specific point in the network — such as a Switched Port Analyzer (SPAN) or mirrored port — and stores it for real-time and historical analysis. Packet data provides richer insights into the actual data that's traversing the network, such as response time, network errors, and application details.

Together, flow, packets, and SNMP analytics provide an end-to-end solution to network monitoring to give you a holistic view of your applications are performing on the network.

Applying Insights to Strengthen Your Security Posture

Enterprise security teams are starting to apply tools such as security analytics, security information and event management (SIEM), and threat intelligence feeds to detect breaches that bypass their perimeter detection. By leveraging the wealth of raw data collected by NPM tools, security teams can gain a more complete view of the enterprise network to more quickly surface indicators of compromise.

According to Mandiant, the average targeted malware compromise is present in an enterprise network for 205 days before detection. Similarly, the Ponemon Institute reports that the average time to detect a data breach is 206 days.

With threat actors often able to achieve their attack objectives in a matter of minutes or seconds, there clearly needs to be a better way of finding and mitigating threats. Enterprise security teams that have long focused their efforts on prevention, need to equally prioritize detection and remediation approaches.

Transforming network flow and packet metrics into security analytics provides essential visibility for broad threat detection, investigation, and mitigation. With complete visibility across the enterprise, enterprises can further strengthen their security posture through rich threat detection capabilities, such as

- **Threat intelligence:** Alerts on potential enterprise threats, such as when a system communicates with blacklisted sites, enable quick investigation and remediation.
- **DDoS detection:** By quickly and accurately identifying DDoS attacks, you can make informed mitigation decisions to end service disruptions sooner.
- **Cyber threat hunting:** Proactively search for hidden security threats on your network before they become business-impacting events.
- **Network security analytics:** Baseline traffic and automatically identify threats that generate unusual patterns, such as unexpected new services, hosts, or connections.
- **Incident forensics:** Obtain full historical details of an incident so you understand the complete scope of an attack.

Overcoming Collaboration Challenges

Collaboration across teams — from network and security teams to apps, end-user services, DevOps, and others — can be easier said than done. It's the seams between teams where problems often arise, and the handoff between cloud providers, application, network, and infrastructure operations teams in the quest to track down problems is a common one. Network teams may be looking at things like congestion and packet loss — but they traditionally haven't had great visibility into problems on data leaks or configuration changes, which might be the root cause of the trouble.

Common challenges to successful collaboration and best practices to address them include

- **Lack of defined processes and best practices:** To address this challenge, organizations should leverage their IT service management groups for help in defining and applying best practices and processes. Network discovery and mapping tools that power network and service topology visualizations can also help build a foundation for shared processes across network and security teams.
- **Siloed data that can't be easily shared:** Both network and security teams need access to consistent, relevant, and current information to successfully perform their respective

functions. A lack of integration between datasets and the tools that analyze them is a significant barrier to successful collaboration that must be addressed.

- **Different goals and priorities:** When it comes to goals and priorities, network and security teams often find themselves being pulled in opposite directions. The network team is focused on performance and availability, while the security team is focused on locking down the network and preventing unauthorized access to applications and data. However, this is often just a matter of perspective. After all, if a network is compromised by a distributed denial-of-service (DDoS) attack or terabytes of data are being exfiltrated, performance and availability will suffer. Helping network and security teams overcome this challenge requires strong leadership.
- **Insufficient support and buy-in from IT leadership:** Finally, effective leadership support and buy-in is critical to successful collaboration. This means more than a "mandate from above." Effective collaboration between network and security teams requires time, resources, and accountability.

Effectively addressing these challenges provides enormous potential benefits to the enterprise. These benefits include

- **CapEx reduction and OpEx efficiencies:** Network and security collaboration can drive cost efficiencies in overall capital expenditures (CapEx) and operating expenses (OpEx), for example, by identifying redundant functionality in individual tools and technologies used by the respective teams. Removing these redundant solutions can help organizations consolidate future investments in tooling and instrumentation, avoid acquisition of new infrastructure through more effective capacity management, eliminate maintenance costs, reduce administrative overhead, and streamline workflows.
- **Risk reduction:** Successful collaboration reduces the likelihood of poor network design, network equipment misconfigurations, and change errors that potentially expose security vulnerabilities in the network. With a better understanding of the network environment, security teams are also less likely to implement security controls that have an adverse impact on network performance.

- **IT productivity enhancement:** Effective collaboration can help drive productivity gains by accelerating the ability of network and security teams to identify and remediate incidents, whether performance- or security-related. Reduced MTTR not only means greater productivity for end-users but also for network and security teams that can focus more on strategic business initiatives.
- **Improved responsiveness and agility:** With better insight into network and security issues and trends, IT will be better able to support new business initiatives through a shared understanding of the network environment.

IN THIS CHAPTER

- Considering the perspective of your business and IT executives
- Empowering IT and network operations teams
- Taking ownership of digital experience as an app owner or developer
- Realizing the value of Digital Experience Management for your customers and employees

Chapter 5
Ten Ways to Get the Most from DEM

When you implement a Digital Experience Management (DEM) platform, you want it to work the best for you. So in this chapter, I give you ten tips to help your organization get the most out of your investment.

Refocus Your SLAs to Align to Business Processes

To show how well your IT team is supporting your company's digital business strategy, you need more than service-level agreements (SLAs) or operational-level agreements (OLAs) based on application uptime and network latency. Ensuring an excellent digital experience requires tracking the performance of the business activities your customers and employees execute on all your critical apps. A robust DEM platform enables you to establish digital experience SLA targets and measure compliance based on your users' experience with applications in the context of a business process, for any app, all without tagging the application code.

REMEMBER

To set a proper SLA target, you must first understand normal application performance based on your users' actual experience. Then, compare every user's experience to the established SLA. Your DEM platform can allow you to automatically create or manually set your SLA performance baseline and then monitor ongoing SLA compliance for every user, device, department, geography, and other parameters.

Quantify the Financial Impact of IT Performance

IT performance has a financial impact across the enterprise both in terms of the customer experience and workforce productivity. For your customer-facing and employee-facing applications, it's important to get insight into every transaction (rather than relying on sampling incomplete data sets) and associated transaction user data (for example, an online retailer might track key customers and high dollar value transactions). Then, you can identify issues with the most financial impact, prioritize your remediation efforts, and development initiatives accordingly.

You also need to assess the impact of poor performance on workforce productivity, including

- Understanding normal response times for business activities performed by the workforce
- Tracking the volume of key business activities
- Identifying the productivity loss (in hours) due to poor app performance
- Quantifying the productivity loss in financial terms by department, function, role, location, and so on

Hold Cloud Vendors Accountable

Nine out of ten enterprises rely on public cloud providers, but how do you know your cloud vendor truly supports your digital business? Their SLAs stop at their clouds' edge and performance and availability metrics don't reflect the actual digital experience of your users.

Although Software-as-a-Service (SaaS), cloud providers, and IT outsourcers benefit the enterprise, there's a corresponding loss of visibility and control. SLAs offered by IT vendors covering infrastructure uptime, incident response time commitments, and penalties don't consider the end-users' experiences. It's not uncommon for IT vendors to provide reports showing everything is green, yet your users are complaining about poor performance.


TIP

With DEM, you can identify whether the issue is in your environment or in your cloud provider's environment. You can monitor the performance of cloud-delivered apps as they render on the screens of your workforce, even for third-party apps hosted outside of your control. DEM monitors all of a user's applications whether local, web, cloud, or mobile, running on any device. It tracks response time — as experienced by the user — for every monitored business activity performed on that app and automatically calculates a baseline for normal performance. It then compares actual response times to the automatic baseline or to a manually set threshold and aggregates this information across the enterprise, enabling you to have a data-driven discussion and resolve issues quickly with your cloud providers.

Scale Your Monitoring to Support Cloud-Native Environments

In a world of increasing architectural complexity, detecting and diagnosing cloud-native application performance problems has never been more elusive. To effectively troubleshoot microservices-based applications and containerized workloads, you need complete and granular information about both the workloads and their environment.

DEM takes a scalable big data approach to monitoring cloud-native applications that delivers unified visibility across the application ecosystem, is easy to deploy and manage, and results in faster troubleshooting for even the toughest, intermittent performance problems. A modern DEM platform must be fully adapted to the cloud-native ecosystem and deliver

- Complete end-to-end transaction visibility across distributed infrastructure

- Lightweight, non-intrusive instrumentation that automatically discovers application components, containers, and their relationships
- Unified analytics across application, user experience, network, and systems data
- Transaction tracing that stitches together logs and metrics
- Container-aware mapping and visualization
- Second-by-second infrastructure metrics

REMEMBER

Your DEM platform should provide full operational visibility into transactions, containers, and microservices running on modern cloud-based application infrastructure, including

- Docker
- Kubernetes
- Red Hat OpenShift
- Pivotal Cloud Foundry
- OpenStack
- IBM Cloud
- Amazon Web Services (AWS) Cloud and Elastic Container Service (ECS)
- Google Cloud Platform (GCP) and Container Services
- Microsoft Azure

Integrate Your Network and IT Infrastructure Monitoring

Many traditional monitoring tools provide siloed root-cause data from infrastructure devices and networks. However, the critical view — the top-down correlation of all this data — is available using DEM solutions. This is especially critical in hybrid environments in order to quickly and easily monitor your users' digital experiences and isolate issues to determine whether your cloud provider or your internal team should address them.

When network and infrastructure metrics are integrated into a DEM platform, enterprises can better troubleshoot performance issues and drive business value.

TIP

Make sure to focus on

- Blending views of end-user experience, application, network, and infrastructure performance with executive, business, and domain-specific use cases
- Providing seamless, contextual drilldowns to view network and infrastructure details and to accelerate mean time to resolution (MTTR)
- Automatically mapping application and underlying infrastructure and network dependencies for better capacity planning and performance optimization
- Accelerating the performance of SaaS applications through automated remediation and software-defined wide area network (SD-WAN) technologies
- Combining network flow data for traffic monitoring with deep packet analysis for troubleshooting and Simple Network Management Protocol (SNMP) for infrastructure visibility to get both breadth and depth

Integrate Network Security Analytics with DEM

While the real intelligence starts with human beings who understand where and why someone might attack them and sets up an appropriate defense, DEM tools incorporate network security analytics to help fend off attackers. Your DEM tools can handle significant volumes of network information that would be difficult to digest by even a superhuman. To fend off cyberattacks, your organization needs both network analysis tools and a dedicated individual who can make actionable and intelligent decisions on the fly.

Integrating network security analytics and DEM enables operational efficiencies across IT operations and security teams. Leveraging AI and other advanced analytics helps turn millions of real-time data points from multiple sources across the enterprise compute environment into actionable insights including

- **Data exfiltration:** Detects when large volumes of data are staged or moved out of your network unexpectedly

- **Distributed denial-of-service (DDoS) detection:** Quickly identifies a wide range of DDoS attacks and automatically triggers mitigations or black hole routes
- **Blacklisted communications:** Alerts you when your system communicates with known malware, viruses, spyware, and so on, so you can investigate and take action
- **Security analytics:** Examines network traffic to identify threats that generate unusual traffic flows, such as unexpected new services, hosts, or connections
- **Incident forensics:** Provides full historical details so you get the complete scope of the attack and you can drill into the packets for even more details

Apply AIOps to Find Problems Faster than Humanly Possible

The volume of data collected from today's highly dynamic, interdependent application environment has exceeded the capacity of humans to analyze and consume in a timely fashion. DEM tools apply artificial intelligence (AI) for IT Operations (AIOps) to enable you to quickly surface insights and proactively resolve issues before your business is impacted. Modern AIOps capabilities include

- **Visualization:** Intuitive maps, graphs, and charts immediately surface key information and relationships among data.
- **Pattern recognition algorithms:** Automatically surface patterns by looking for regularities in datasets with machine learning.
- **Automated anomaly detection:** Proactively watch for transactions and metrics that aren't behaving as they should.
- **Correlation:** Find groups of metrics on tiers that are spiking in tandem to chase down performance issues even in distributed containerized and microservices environments with thousands of nodes.
- **Event management:** Build more actionable context into alerts (events) and optimize the incident management workflow by incorporating automated remediation and cross-domain root cause analysis.

Monitor the End-User Experience Everywhere for Every App

End-users expect a seamless omnichannel digital experience on their preferred devices, when and where they choose to use them. To deliver a superior end-user experience, IT teams need a robust DEM platform that can monitor the real-time user experience of business applications, including web, SaaS, cloud, and mobile apps, regardless of device, network, or location.

TIP

Your DEM tool should support

- All types of devices, including physical, virtual, and mobile devices
- All types of enterprise application technologies including thick client, web, SaaS, and mobile
- All geographies and locations from the corner coffee shop to the corner office

Compare End-User Experience Before and After a Change

Digital transformation initiatives create change throughout IT. No matter the type of change and whether changes are strategic or tactical in nature, the key to ensuring a successful project is making sure it actually results in better service for your users. By comparing the end-user experience before and after a change, you can determine whether your efforts paid off.

REMEMBER

Unlike predictive analysis, with DEM you can compare performance before and after a change by using real, objective data. App owners, infrastructure and operations teams, and desktop support can use this information to verify that changes or upgrades or even a migration to SD-WAN actually result in better service for their customers. Assess business activity volumes and response times relative to SLA targets before and after a change and create meaningful reports for business stakeholders. These response times — as experienced by the end-user — help quantify the impact of changes.

Shift from Reactive to Proactive

Performance monitoring nirvana is to resolve issues before your customers and employees are impacted. With DEM, you get proactive notification when performance issues impact digital experience so you can quickly isolate and resolve issues, protecting employee productivity, your brand, and your bottom line. DEM shows you everything about the performance of your business-critical apps from end-user experience to the networks and infrastructure that underpin them.

With DEM, for any app and device, you can immediately, remotely, and non-invasively diagnose user experience issues by doing the following:

- Reviewing all applications running on any device
- Identifying every business activity performed
- Tracking response times versus baseline performance
- Validating complaints of poor application performance
- Profiling user devices and analyzing device resource consumption
- Checking key device parameters, such as network and disk performance or Wi-Fi signal strength

REMEMBER

To get the most from DEM, choose a platform that provides an end-to-end view of the user experience with visibility into the applications, infrastructure, and networks that underpin it. Advanced DEM solutions leverage the power of big data and AIOps to surface relevant IT and business insights so you can deliver the best possible experience to your customers and employees.

Advancing the human digital experience

Performance is everything. If apps and services are slow or unsatisfying, orders aren't fulfilled, work isn't finished, customers leave, and your digital ambitions fall short. You need unified visibility into the digital experience — from the user to the network to the application and down to the line of code — to deliver highly engaging, secure, and satisfying digital experiences. Use DEM to gain cross-domain understanding and build customer loyalty, streamline business operations, and increase employee productivity.

Inside...

- Optimize your users' experience
- Gain cross-domain visibility
- Simplify cloud-native monitoring
- Leverage big data and AI
- Quantify the impact of change
- Analyze the network impact on users
- Strengthen your security posture

riverbed®

Lawrence C. Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-61934-5
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.