


Extending Microsoft SCOM's Reach

How Modern Management Packs Unlock Hybrid and Mission-Critical Monitoring

A Whitepaper by NiCE IT Management Solutions

A photograph of a surfer riding a wave, overlaid with a purple-to-blue gradient. The surfer is in a dynamic, low-to-the-water position, with one arm raised. The wave is breaking, creating white foam. The background is a clear sky.

This whitepaper outlines how to extend Microsoft SCOM's capabilities to monitor hybrid and mission-critical environments effectively.

As IT landscapes evolve toward Azure, SaaS, and multi-cloud platforms, traditional monitoring approaches often leave gaps that hinder performance and reliability.

Modern Management Packs provide a practical solution, enabling Microsoft SCOM to seamlessly monitor new technologies, specialized applications, and non-Microsoft systems, without the need for separate tools.

Through careful assessment, strategic deployment, and targeted customization, IT teams can eliminate blind spots, streamline operations, and ensure SCOM continues to deliver deep, actionable insights across the modern enterprise.

Contents

Introduction 4

The Modern Monitoring Challenge 5

Why Management Packs Still Matter 7

Traditional vs. Modern Management Packs 10

Extending Visibility with NiCE Standard Management Packs 12

Custom Management Packs: When Out-of-the-Box Isn't Enough 15

Operational and Business Impact 18

Getting Started 20

Conclusion 21

About NiCE 22

Executive Summary

In an era of hybrid IT, monitoring environments have become more complex than ever. Many organizations rely on Microsoft System Center Operations Manager (SCOM) as a trusted backbone for infrastructure visibility and health monitoring. Yet as workloads move to Azure, SaaS, and other cloud platforms, IT teams often struggle to maintain consistent oversight without adopting entirely new toolsets.

This paper explores a smarter path forward — one that leverages existing SCOM investments while extending visibility into new technologies and mission-critical systems. Modern **Management Packs (MPs)**, particularly from NiCE, enable SCOM to seamlessly monitor hybrid workloads, specialized enterprise applications, and non-Microsoft platforms.

By understanding how to deploy and customize MPs strategically, SCOM administrators and architects can:

- Eliminate blind spots across hybrid environments
- Avoid costly monitoring migrations
- Standardize data collection and alerting
- Drive proactive operations through deep platform insight

This whitepaper provides a practical roadmap for extending SCOM's reach using **NiCE's portfolio of standard and custom Management Packs**, backed by real-world examples and implementation guidance.

Introduction

Monitoring has always been at the heart of reliable IT operations. For nearly two decades, **System Center Operations Manager (SCOM)** has provided enterprises with a powerful, centralized platform to ensure infrastructure health, service uptime, and proactive incident response.

But in 2025, most organizations are operating in **hybrid** or **multi-cloud** environments. Applications span data centers, Azure, AWS, and SaaS layers. Business-critical workloads — from SAP and Oracle to VMware and custom line-of-business systems — often live outside SCOM's native reach.

In this landscape, traditional SCOM monitoring can start to feel fragmented or incomplete. IT teams often wonder:

Is it time to move on from SCOM? Or can we extend it to handle the hybrid world?

The answer is clear: **SCOM can evolve.**

With the right **Management Packs (MPs)**, SCOM remains a first-class monitoring platform that integrates seamlessly with cloud-native tools and delivers full-stack observability without requiring a rip-and-replace migration.

This paper explains how **NiCE's standard and custom MPs** empower organizations to bridge monitoring gaps, unify visibility, and derive deeper insights from their existing investments — all while maintaining operational stability and cost efficiency.

You'll learn:

- How SCOM's extensibility model works
- Where modern NiCE MPs extend SCOM's coverage
- When to consider custom MP development
- How to align SCOM monitoring with today's hybrid IT realities

Whether you're an experienced SCOM administrator or an enterprise architect shaping the next generation of monitoring strategy, this whitepaper offers a clear, actionable path to extending your visibility — and your value.

The Modern Monitoring Challenge

The landscape of IT operations has changed dramatically in recent years. What was once a neatly defined data center — where workloads lived on a predictable set of servers and networks — has evolved into a complex hybrid ecosystem spanning on-premises infrastructure, private clouds, and multiple public cloud providers.

This transformation has created a new set of challenges for monitoring and observability. Traditional boundaries no longer apply. Virtual machines coexist with containers, business applications depend on third-party APIs, and critical data flows through systems hosted both in the cloud and on the ground. For IT teams, maintaining consistent visibility across this dynamic environment has become both a technical and organizational challenge.

SCOM: A Trusted Foundation Under Pressure

For many enterprises, System Center Operations Manager (SCOM) remains a cornerstone of monitoring strategy. Its strengths are well established — deep integration with Windows Server, Active Directory, and Microsoft workloads; mature alerting and escalation workflows; and a stable, extensible architecture that has proven itself in even the most demanding environments.

Yet as IT landscapes evolve, many organizations face a critical question:

Can SCOM keep up with the hybrid enterprise?

Some perceive SCOM as a legacy platform, limited to monitoring Microsoft systems or on-premises workloads. In reality, the SCOM framework remains highly capable — but its true power depends on how well it is extended. The core SCOM engine provides the monitoring foundation, while Management Packs (MPs) supply the intelligence to discover, monitor, and visualize specific applications and services.

Without the right MPs, SCOM's visibility can stop at the edge of the data center. With them, it becomes a unified monitoring fabric spanning physical, virtual, and cloud-based resources.

The Risk of Fragmented Monitoring

As hybrid complexity grows, many organizations have adopted multiple monitoring tools in parallel — one for cloud services, one for databases, one for infrastructure, and perhaps a bunch of others for applications. While each tool may excel in its niche, the overall result is fragmentation:

- **Duplicate alerts and data silos** that make root cause analysis slower
- **Inconsistent metrics** across teams and platforms

- **Increased cost and complexity** from tool proliferation
- **Gaps in coverage** where certain systems or dependencies fall outside any monitoring scope

This “monitoring sprawl” leads to inefficiency and confusion. In many cases, it also reduces confidence — IT teams can’t be sure whether issues are truly being detected early or if critical dependencies remain invisible.

A Smarter Path: Modernization Through Extension

Rather than replacing proven platforms like SCOM, forward-thinking organizations are taking a more sustainable approach: **modernizing through intelligent extension**.

By leveraging advanced, third-party Management Packs — such as those developed by **NiCE** — enterprises can extend SCOM’s reach into non-Microsoft ecosystems, hybrid cloud environments, and specialized enterprise applications. These MPs enrich SCOM with the necessary logic, metrics, and automation to monitor systems such as **DB2, Oracle, VMware, Linux, and M365 workloads**, all within the familiar SCOM console and alerting model.

This strategy offers several key advantages:

- **Preserves existing investment:** Build upon established infrastructure and processes rather than migrating to a new platform.
- **Ensures consistency:** Use a single framework for alerting, escalation, and reporting.
- **Reduces training and transition cost:** Operators continue to use tools they already know.
- **Enables scalability:** Extend coverage incrementally as hybrid adoption grows.

In this way, SCOM continues to serve as a **centralized operations hub** — not as a relic of legacy infrastructure, but as a modern, extensible foundation capable of adapting to new technologies.

Looking Ahead

The next sections of this paper explore how Management Packs, particularly from NiCE, provide the technical bridge between traditional infrastructure monitoring and the hybrid, multi-platform reality of modern IT. By understanding the evolving role of MPs and applying best practices in their deployment, SCOM administrators and architects can ensure that their monitoring strategies remain comprehensive, cost-efficient, and future-ready.

Why Management Packs Still Matter

At the heart of every SCOM deployment lies a simple yet powerful concept: **the Management Pack (MP)**. It is the MP — not the SCOM platform itself — that defines what to monitor, how to detect issues, and how to visualize system health.

While the SCOM engine provides the infrastructure for data collection, alerting, and automation, Management Packs supply the *intelligence* that transforms raw telemetry into actionable insight. MPs define the discoveries, performance counters, event rules, and health models that allow SCOM to truly “understand” the systems it monitors.

Without MPs, SCOM is a framework. With them, it becomes a living, adaptable ecosystem.

The DNA of SCOM Monitoring

Each Management Pack encapsulates the domain knowledge required to monitor a specific technology — whether that’s a Windows service, a database, or a virtual infrastructure layer.

A well-designed MP enables SCOM to:

- Automatically **discover components** such as servers, clusters, or application roles
- **Collect metrics** and performance counters relevant to that workload
- **Define health models** that reflect how the system behaves under normal and abnormal conditions
- **Trigger alerts or recovery actions** when thresholds are exceeded or dependencies fail

In short, MPs are the codified expertise that make SCOM intelligent.

The Problem with ‘Set and Forget’ MPs

In many organizations, Management Packs are treated as static assets — installed once and rarely updated. This approach can cause monitoring blind spots to grow quietly over time.

Common issues include:

- **Outdated management packs** that fail to recognize new platform versions or metric models
- **Overly sensitive thresholds** that flood operators with noise
- **Undocumented customization** that breaks during upgrades
- **Redundant or conflicting rules** introduced by overlapping MPs

The result is a monitoring environment that becomes noisy, unreliable, or incomplete — eroding confidence in SCOM's alerts and reducing its operational value.

Standard vs. Custom MPs: Two Paths to Extensibility

Modern monitoring environments demand agility. No two IT landscapes are identical, and organizations often combine a mix of commercial, open-source, and proprietary systems. To maintain complete visibility, SCOM needs to be extended in two complementary ways:

Standard Management Packs

- Developed for widely used platforms and applications.
- Provide prebuilt logic, tested thresholds, and official support.
- Ideal for foundational technologies such as **Oracle, DB2, VMware, M365, or Linux**.
- Rapid deployment with minimal customization.

Custom Management Packs

- Designed for in-house applications, legacy systems, or specialized services.
- Tailored to organizational workflows, KPIs, and dependencies.
- Developed through structured workshops or collaborative design with a partner such as NiCE.
- Ensure no component of your critical stack remains unmonitored.

This two-tiered approach — combining proven, ready-to-use standard MPs with bespoke custom ones — delivers the flexibility and completeness required for modern hybrid monitoring.

The NiCE Advantage: Quality and Continuity

The value of a Management Pack lies in its reliability and accuracy. NiCE has built its reputation on delivering **high-quality, deeply engineered MPs** that integrate seamlessly into SCOM's native model. Each NiCE MP is:

- Developed using best practices aligned with Microsoft guidelines.
- Continuously updated to reflect evolving platform versions and security requirements.
- Tested for performance and scalability in enterprise environments.
- Supported by documentation and services that ensure smooth lifecycle management.

Beyond standard offerings, NiCE provides **custom MP development services** to help organizations capture telemetry from unique or business-critical systems. Whether monitoring a bespoke financial application, a manufacturing control process, or a specific API integration, NiCE ensures that SCOM remains a single pane of glass for operational health.

Why It Matters Now

As observability trends push toward unified visibility, many organizations face pressure to adopt new toolchains. However, building an entirely new monitoring ecosystem is costly and disruptive. By revitalizing SCOM through high-quality Management Packs, enterprises can achieve the same breadth of insight — faster, with less risk, and at lower cost.

MPs are not just legacy components; they are the mechanism that keeps SCOM modern. In 2025, they remain the **critical link between proven monitoring infrastructure and new digital realities**.

Traditional vs. Modern Management Packs

Management Packs (MPs) have been the cornerstone of SCOM monitoring since its inception. However, the nature of IT environments has changed dramatically, and so has the design philosophy behind modern MPs. Understanding the differences helps organizations see why leveraging modern MPs is essential for hybrid, multi-platform operations.

Feature / Capability	Traditional MP	Modern MP
Target Environment	On-premises only	Hybrid & multi-platform
Alerting	Static thresholds	Intelligent health models
Integration	Limited	Cloud, dashboards, automation
Maintenance	Slow, manual	Regular, tested, scalable
Customization	Complex, manual	Modular, supported, automated

Traditional Management Packs

Characteristics

- Designed primarily for **on-premises, single-platform workloads** (e.g., Windows Server, SQL Server).
- Typically reactive, generating alerts based on **fixed thresholds** or static event rules.
- Limited integration with hybrid or cloud-native systems.
- Updates and enhancements are often slow or tied to major SCOM releases.
- Customization is possible but usually **manual and complex**.

Limitations

- Blind spots in hybrid or multi-platform environments
- Higher false-positive rate due to static thresholds
- Increased administrative overhead for tuning, documentation, and upgrades

Modern Management Packs

Characteristics

- Designed for **hybrid, multi-platform, and mission-critical systems**.
- Incorporate **intelligent health models** that consider dependencies and real operational impact.
- Support **automation and integration** with cloud services, dashboards, and external observability tools.
- Actively maintained and updated for new platform versions and releases.
- Often available as **prebuilt, tested, and scalable modules** with optional customization.

Advantages

- Reduced alert noise and improved MTTR (Mean Time to Resolution)
- Unified visibility across cloud, on-prem, and third-party systems
- Faster deployment and easier lifecycle management
- Enhanced operational insight that aligns IT monitoring with business impact

Modern MPs transform SCOM from a platform focused on basic infrastructure monitoring into a **comprehensive observability framework**. Standard and custom modern MPs, such as those provided by NiCE, allow IT teams to extend coverage, reduce operational risk, and derive actionable insights from hybrid environments — all while preserving existing SCOM investments.

Extending Visibility with NiCE Standard Management Packs

While SCOM provides a robust foundation for monitoring, the reality of modern IT infrastructure requires more than out-of-the-box capabilities. Standard Management Packs from **NiCE** extend SCOM's reach into key enterprise systems, hybrid cloud environments, and critical applications, bridging the gap between native SCOM coverage and comprehensive operational insight.

Comprehensive Platform Coverage

NiCE's portfolio of standard Management Packs addresses a broad range of technologies, including:

- **Databases:** Oracle, DB2, MariaDB, MongoDB
- **Virtualization & Cloud Platforms:** VMware vSphere, HMC VIOS, Citrix, Azure
- **Operating Systems:** Linux, Unix
- **Network and Storage Infrastructure:** Selected monitoring for network devices and storage systems

These MPs bring prebuilt discovery logic, health models, performance counters, and alerting rules — enabling SCOM to automatically detect and monitor both standard and advanced configurations of these platforms.

Technical Benefits of NiCE Standard MPs

Rapid Deployment

- Prebuilt logic allows fast onboarding of critical workloads.
- Reduces the need for manual configuration or complex scripting.

Consistency Across Environments

- Standardized health models and alerts ensure uniform monitoring policies across multiple sites and hybrid environments.
- Reduces false positives and alert fatigue.

Operational Efficiency

- Out-of-the-box dashboards and preconfigured reports streamline operational reporting.
- Supports proactive maintenance and faster root-cause analysis.

Lifecycle Support and Updates

- NiCE MPs are actively maintained and tested against new platform releases, ensuring continuity and avoiding monitoring gaps.

Real-World Example: Hybrid Database Monitoring

Consider a global enterprise running a mix of Oracle and DB2 databases across on-premises data centers and Azure infrastructure. Without extended monitoring, IT teams risk blind spots that can impact SLA compliance and system availability.

By deploying NiCE Oracle and DB2 MPs, the organization gains:

- Automated discovery of all database instances and clusters
- Predefined alerts for critical thresholds (CPU, memory, storage, replication issues)
- Health models that reflect true operational impact rather than simple metric thresholds
- Integration into the existing SCOM dashboards for unified reporting

The result: proactive identification of issues, fewer production outages, and faster incident response — all without adding new monitoring platforms.

Extending to Virtualization and Hybrid Cloud

NiCE MPs also enhance visibility into virtualization and cloud environments:

- **VMware vSphere MP:** Tracks hosts, clusters, virtual machines, and critical resource metrics, integrating seamlessly into SCOM's existing alerting framework.
- **Active 365 MP:** Brings Microsoft 365 workloads — including Teams, Exchange, SharePoint, OneDrive, and Entra Connect / identity sync health — into the same monitoring console, enabling holistic visibility of cloud productivity and identity services.

Why Standard MPs Are a Foundation for Success

Standard MPs serve as the backbone for modern SCOM monitoring, offering a reliable, scalable, and tested method to extend coverage quickly. They provide:

- **Immediate visibility** into widely-used systems
- **Consistency and reliability** that reduce operational risk
- **A platform for further customization** when unique or in-house systems require additional monitoring

Combined with NiCE's expertise in custom MP development, these standard packs create a **comprehensive monitoring strategy**, allowing organizations to maintain full oversight of their entire hybrid IT environment without sacrificing efficiency or accuracy.

While standard MPs cover the majority of enterprise workloads, many organizations operate systems that are unique, proprietary, or highly specialized. The next section explores how **custom Management Packs from NiCE** ensure no critical system is left unmonitored, providing tailored visibility and advanced health modeling for every environment.

Custom Management Packs: When Out-of-the-Box Isn't Enough

While standard Management Packs provide broad coverage for widely used platforms, no two enterprise environments are identical. Organizations often rely on custom or legacy applications, specialized workflows, or niche infrastructure components that fall outside the reach of off-the-shelf monitoring solutions.

For these scenarios, **custom Management Packs (MPs)** become essential — allowing SCOM to monitor every critical system with the same rigor and reliability as its standard counterparts.

When Custom MPs Are Needed

Custom MPs are typically required when:

- **Proprietary or in-house applications** require specific monitoring logic that is not covered by standard MPs.
- **Legacy systems** (e.g., older databases or custom business platforms) lack native SCOM coverage.
- **Unique workflows or integrations** require tailored alerting or performance metrics.
- **Advanced health modeling** is needed to represent the business impact of component failures rather than simple metric thresholds.

Without custom MPs, these systems may remain invisible to SCOM, creating monitoring blind spots that can result in operational risk, delayed incident response, or SLA breaches.

Design Principles for Effective Custom MPs

Developing a high-quality custom MP requires more than simply adding a few alerts. Best practices include:

- **Discovery Logic Aligned to Infrastructure**
Accurately identifies systems, roles, and dependencies to ensure monitoring is complete and dynamic.
- **Health Models Reflecting Real-World Impact**
Alerts indicate the true operational or business impact, reducing noise and improving response accuracy.
- **Performance and Scalability Testing**
Ensures the custom MP does not degrade SCOM performance, even in large or highly dynamic environments.
- **Lifecycle Management and Documentation**
Structured deployment, versioning, and updates guarantee that the MP remains functional during SCOM upgrades or platform changes.
- **Integration with Existing Dashboards and Workflows**
Provides continuity with standard MPs, maintaining a unified monitoring console for operators and architects.

The NiCE Approach to Custom MPs

NiCE brings decades of SCOM expertise to the development of custom MPs. Their approach ensures that every MP is **reliable, maintainable, and actionable**, allowing IT teams to focus on operations rather than monitoring maintenance. Key aspects of NiCE's custom MP services include:

- **Collaborative Design Workshops** - Requirements are gathered from stakeholders to understand systems, dependencies, and KPIs.
- **Rapid Prototyping and Validation** - Early versions of MPs are tested in controlled environments to confirm accuracy and performance.
- **Documentation and Knowledge Transfer** - Every MP includes thorough documentation, deployment guides, and training support for internal teams.
- **Lifecycle Support** - Ongoing updates and version control ensure MPs remain compatible with SCOM and evolving infrastructure.

Real-World Example: End-to-End Microsoft 365 and Identity Monitoring

A professional services firm relies heavily on Microsoft 365 for daily collaboration and productivity. When users experience delayed email delivery or failed Teams calls, identifying the root cause across hybrid identity, Entra Connect synchronization, and cloud service health can be complex.

By implementing the **NiCE Active 365 MP** (including **Entra Connect MP** capabilities), the organization achieves:

- Continuous monitoring of Microsoft 365 workloads such as Exchange Online, Teams, SharePoint, and OneDrive
- Real-time visibility into Entra ID health and synchronization status
- Unified alerting within SCOM, correlating on-premises and cloud service dependencies
- Comprehensive SLA reporting for internal and external compliance

The result: faster identification of user-impacting issues, reduced helpdesk load, and complete hybrid visibility across both identity and collaboration platforms.

Why Custom MPs Drive Business Value

Custom MPs ensure that no critical system is left unmonitored, delivering:

- **Operational Confidence:** Complete visibility into all mission-critical workloads.
- **Reduced Risk:** Early detection of failures in proprietary or unique systems.
- **Efficiency:** Consolidated monitoring reduces the need for multiple tools and platforms.
- **Strategic Insight:** Aligns monitoring data with business KPIs for informed decision-making.

When combined with NiCE's standard MPs, custom MPs create a **comprehensive, hybrid-ready monitoring environment**, capable of supporting both today's workloads and tomorrow's innovations.

With the combined power of standard and custom MPs, organizations can maximize operational visibility, efficiency, and reliability. The next section will explore the **operational and business impact** of a fully extended SCOM environment, including measurable outcomes and success metrics for IT teams and business stakeholders.

Operational and Business Impact

Extending SCOM with NiCE standard and custom Management Packs transforms monitoring from a reactive activity into a **strategic operational asset**. Organizations gain measurable benefits that improve IT efficiency, reduce risk, and support business objectives.

Operational Benefits

Faster Incident Detection and Response

- Standard and custom MPs provide complete coverage for hybrid and mission-critical workloads.
- Operators receive actionable alerts that reflect real operational impact, reducing investigation time and accelerating resolution.

Reduced Noise and Alert Fatigue

- Predefined health models and thresholds prevent unnecessary alerts.
- Teams can focus on genuine incidents instead of filtering false positives.

Unified Monitoring Across Hybrid Environments

- On-premises, cloud, and third-party systems are consolidated into the same SCOM console.
- IT teams benefit from a single pane of glass, simplifying workflows and reducing operational overhead.

Improved Maintenance and Proactive Management

- Consistent monitoring enables trend analysis and capacity planning.
- Predictive insights prevent outages before they impact users or business operations.

Business Benefits

Reduced Operational Risk

- Complete visibility over critical systems ensures SLAs and compliance requirements are met.
- Early detection of potential issues prevents costly downtime.

Lower Total Cost of Monitoring

- Leveraging existing SCOM infrastructure avoids the need for multiple third-party monitoring tools.
- Standardized MPs and scalable custom MPs reduce maintenance and training overhead.

Strategic Decision Support

- Monitoring data becomes actionable intelligence for business leaders.
- Integration with reporting and visualization tools (e.g., Power BI, dashboards) provides clear insights into system health, availability, and performance metrics.

Getting Started

Implementing an extended SCOM monitoring environment is easier with a structured approach. NiCE provides guidance, tools, and services to ensure organizations gain the most from their investments.

Self-Assessment Checklist

Before deploying standard or custom MPs, IT teams can evaluate their readiness:

- Does SCOM currently monitor all mission-critical workloads?
- Are existing MPs up-to-date and properly configured?
- Are hybrid workloads (cloud, virtualization) visible within SCOM?
- Do dashboards and reporting tools provide actionable insights for both IT and business stakeholders?
- Are there systems or applications that remain unmonitored or partially covered?

Deployment Options

NiCE Standard MPs

- Quickly expand coverage for databases, virtualization platforms, OS, and hybrid cloud systems.
- Prebuilt dashboards and alerting rules enable rapid operational adoption.

Custom MP Development

- Design tailored MPs for proprietary applications, legacy systems, or specialized workflows.
- A collaborative approach ensures MPs align with operational and business priorities.

NiCE Services

- We offer workshops, health checks, and optimization services to ensure SCOM is fully leveraged.
- Lifecycle support guarantees continuity through upgrades and environmental changes.

Conclusion

System Center Operations Manager remains a **powerful and flexible monitoring platform**. Its core capabilities, when paired with the right Management Packs, provide unmatched visibility into hybrid and mission-critical IT environments.

By combining NiCE's **standard MPs** for broad coverage with **custom MPs** for unique or proprietary systems, organizations can:

- Extend SCOM's reach across cloud, virtual, and on-premises workloads
- Consolidate monitoring into a single operational view
- Reduce operational risk, improve SLA compliance, and drive business value

Monitoring doesn't have to be fragmented or reactive. With NiCE, SCOM becomes a **centralized, intelligent monitoring ecosystem**, capable of meeting today's hybrid IT demands while remaining flexible for future growth.

Unlock the full potential of your Microsoft SCOM environment. Request a **free SCOM Extension Readiness Assessment** today or engage NiCE for custom MP development to ensure complete visibility and operational confidence across all mission-critical systems.

About NiCE

NiCE Services for Microsoft System Center encompass consulting services tailored to System Center Operations Manager, Configurations Manager, and Service Manager. Our offerings include SCOM Health Assessments, training, advice and provisioning for third-party SCOM tools, as well as SCOM-centric monitoring solutions for business elements such as applications, databases, operating systems, services, and custom applications.

NiCE Management Packs for Microsoft SCOM are available for AIX, Azure AD Connect, Entra ID, Citrix VAD & ADC, Custom Applications, HCL Domino, IBM Db2, IBM HMC & VIOS, IBM Power HA, Linux on Power Systems, Log Files, MariaDB, Microsoft 365, Microsoft Teams, Microsoft SharePoint, Microsoft Exchange, Microsoft OneDrive, Mongo DB, NetApp ONTAP, Oracle, Veritas Clusters, VMware, and zLinux.

Our commitment

1. Ongoing development, incl. latest version support
2. Top required metrics come out-of-the-box
3. Integrated source knowledge to solve issues faster
4. Custom development & coaching
5. Highly responsive support team
6. Easy onboarding & renewals
7. Largest set of Microsoft SCOM Management Packs

About Microsoft System Center Operations Manager (SCOM)

Microsoft SCOM is a powerful IT management solution designed to help organizations monitor, troubleshoot, and ensure the health of their IT infrastructure. SCOM provides comprehensive infrastructure monitoring, offering insights into the performance, availability, and security of applications and workloads across on-premises, cloud, and hybrid environments. With its robust set of features, SCOM enables IT professionals to proactively identify and address potential issues before they impact the business, improving overall operational efficiency and reducing downtime. By leveraging SCOM, businesses can achieve greater control over their IT environment, ensuring a seamless user experience and enhancing the reliability of their services.

Take advantage of all the benefits of advanced monitoring using NiCE Management Packs for Microsoft System Center Operations Manager. Contact us at solutions@nice.de (EMEA, APAC), or solutions@nice.us.com (US, LATAM) for a quick demo, and a free 60 days trial.

NiCE IT Management Solutions GmbH

Liebigstrasse 9
71229 Leonberg
Germany

www.nice.de
solutions@nice.de

NiCE IT Management Solutions Corporation

3478 Buskirk Avenue, Suite 1000
Pleasant Hill, CA 94523
USA

www.nice.us.com
solutions@nice.us.com

