zenoss
Own IT.

The Definitive Guide to Monitoring Virtual Environments

TABLE OF CONTENTS

zenoss Own IT.

OVERVIEW

The virtualization of physical computers has become the backbone of public and private cloud computing from desktops to data centers, enabling organizations to optimize hardware utilization, enhance security, support multi-tenancy and more. These environments are complex and ephemeral, creating requirements and challenges beyond the capability of traditional monitoring tools that were originally designed for static physical environments. But modern solutions exist, and can bring your virtual environment to new levels of efficiency, performance and scale.

This guide explains the pervasiveness of virtualized environments in modern data centers, the demand these environments create for more robust monitoring and analytics solutions, and the keys to getting the most out of virtualization deployments.

History and Expansion of Virtualized Environments

HISTORY AND EXPANSION OF VIRTUALIZED ENVIRONMENTS

Virtualization was created so that teams managing IT infrastructure could increase computer resource utilization while simultaneously decreasing the time needed for provisioning and reducing direct capital expenditures. The expansion of these principal benefits is why the virtualization of physical systems has become the backbone of public and private cloud computing from desktops to data centers, enabling organizations to optimize utilization of all kinds, enhance security, support multitenancy and more.

Initially, virtualization generally amounted to emulating CPUs, with the x86 processor being the primary focus. But eventually virtualization expanded to include the rest of the hardware environment – graphics adapters, hard disks, network adapters, memory and interfaces.

In the late 1990s, VMware introduced a technology that enabled most of the code to execute directly on the CPU without the requirement for translation or emulation. Prior to VMware, two or more operating systems running on the same hardware would simply corrupt each other as they vied for physical resources and attempted to execute privileged instructions. VMware intelligently intercepted these types of instructions, dynamically rewriting the code and storing the new translation for reuse and fast execution.

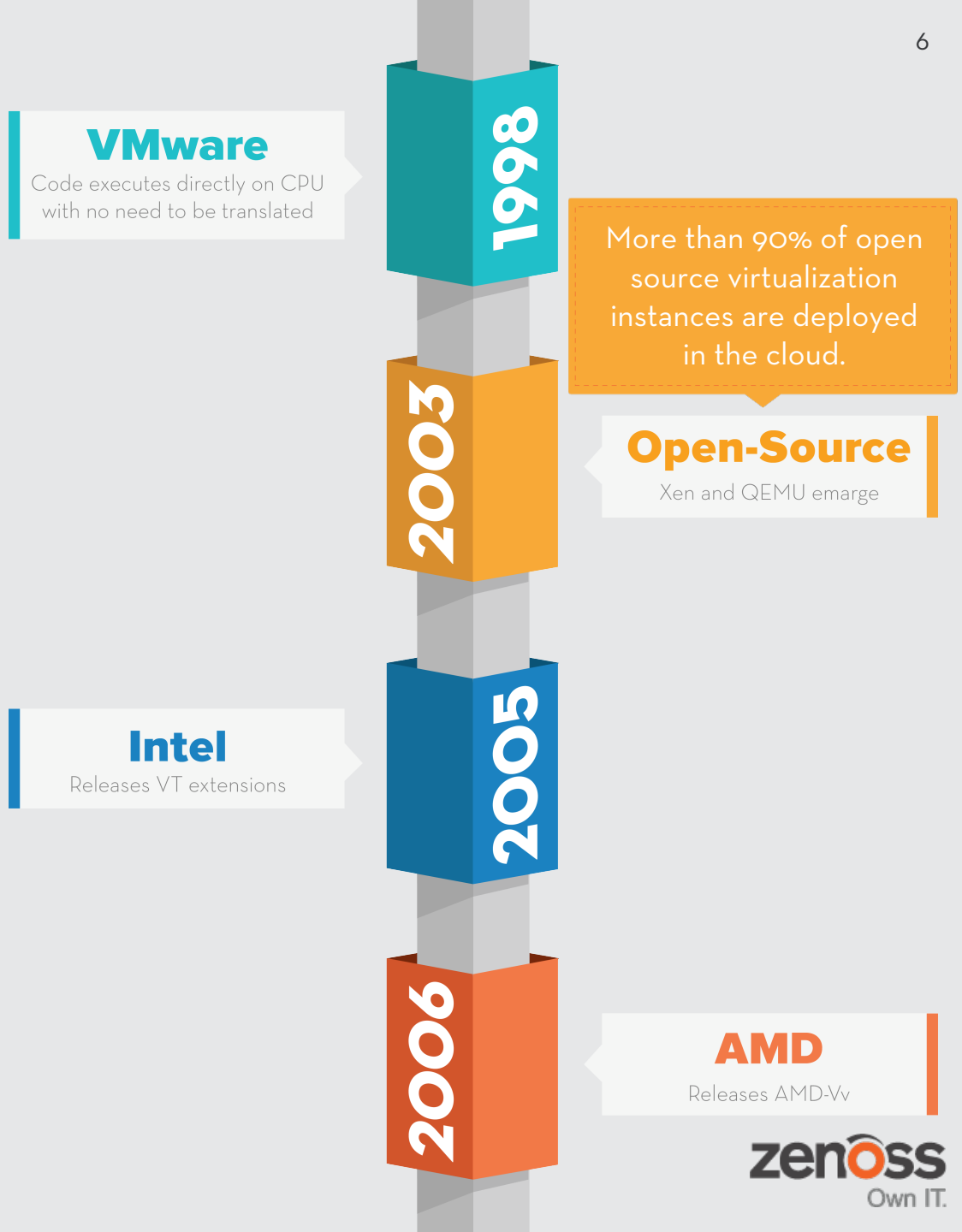
About 80% of x86 server workloads are virtualized.

In combination, these techniques ran much faster than previous emulators and helped define x86 virtualization as we know it today, including the old mainframe concept of the "hypervisor" – a platform upon which IT could create and run virtual machines.

For years, VMware and its patents ruled the realm of virtualization. On the server side, running on bare metal, VMware's ESX became the leading Type 1 (or native) hypervisor. On the client side, running within an existing desktop operating system, VMware Workstation was among the top Type 2 (or hosted) hypervisors.

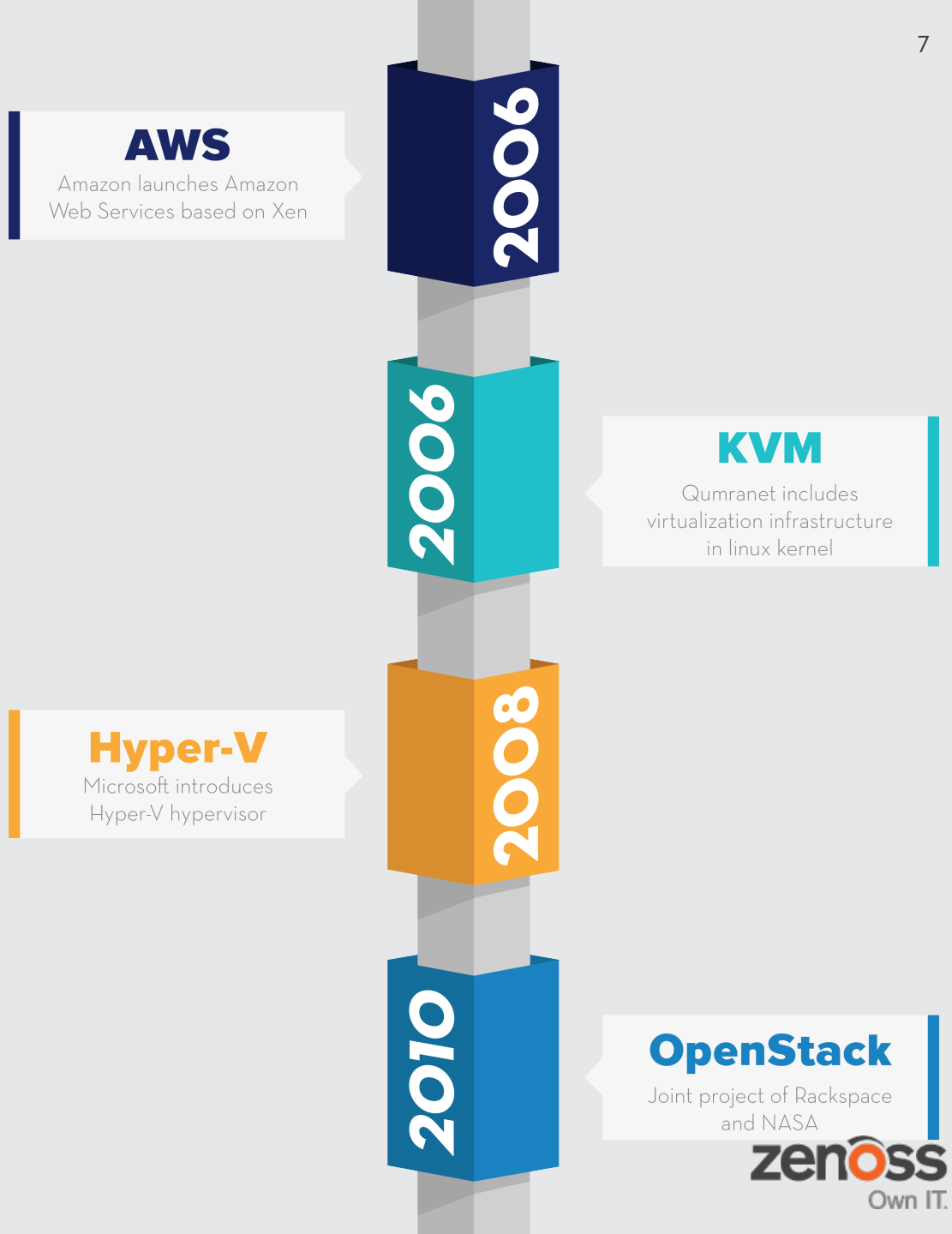
No longer a technology just for developers or cross-platform software usage, virtualization proved itself as a powerful tool to improve efficiency and manageability in data centers by putting servers in interchangeable virtualized containers.

Over the years, some interesting open-source projects emerged, including Xen and Quick EMUlator (QEMU). Neither was as fast or as flexible as VMware, but they set a foundation that would prove worthy down the road. Around 2005, Advanced Micro Devices (AMD) and Intel created new processor extensions to the x86 architecture. These extensions provided hardware assistance for dealing with privileged instructions.



Called AMD-V and VT-x by AMD and Intel respectively, these extensions changed the landscape, eventually opening server virtualization to new players. Soon after, Xen leveraged these new extensions to create hardware virtual machines (HVMs) that used the device emulation of QEMU with hardware assistance from the Intel VT-x and AMD-V extensions to support proprietary operating systems like Microsoft Windows.

A company called Qumranet also began to include virtualization infrastructure in the Linux kernel, called Kernel-based Virtual Machine (KVM), and started using the QEMU facility to host virtual machines. Even Microsoft eventually got into the game with the release of Hyper-V in 2008.

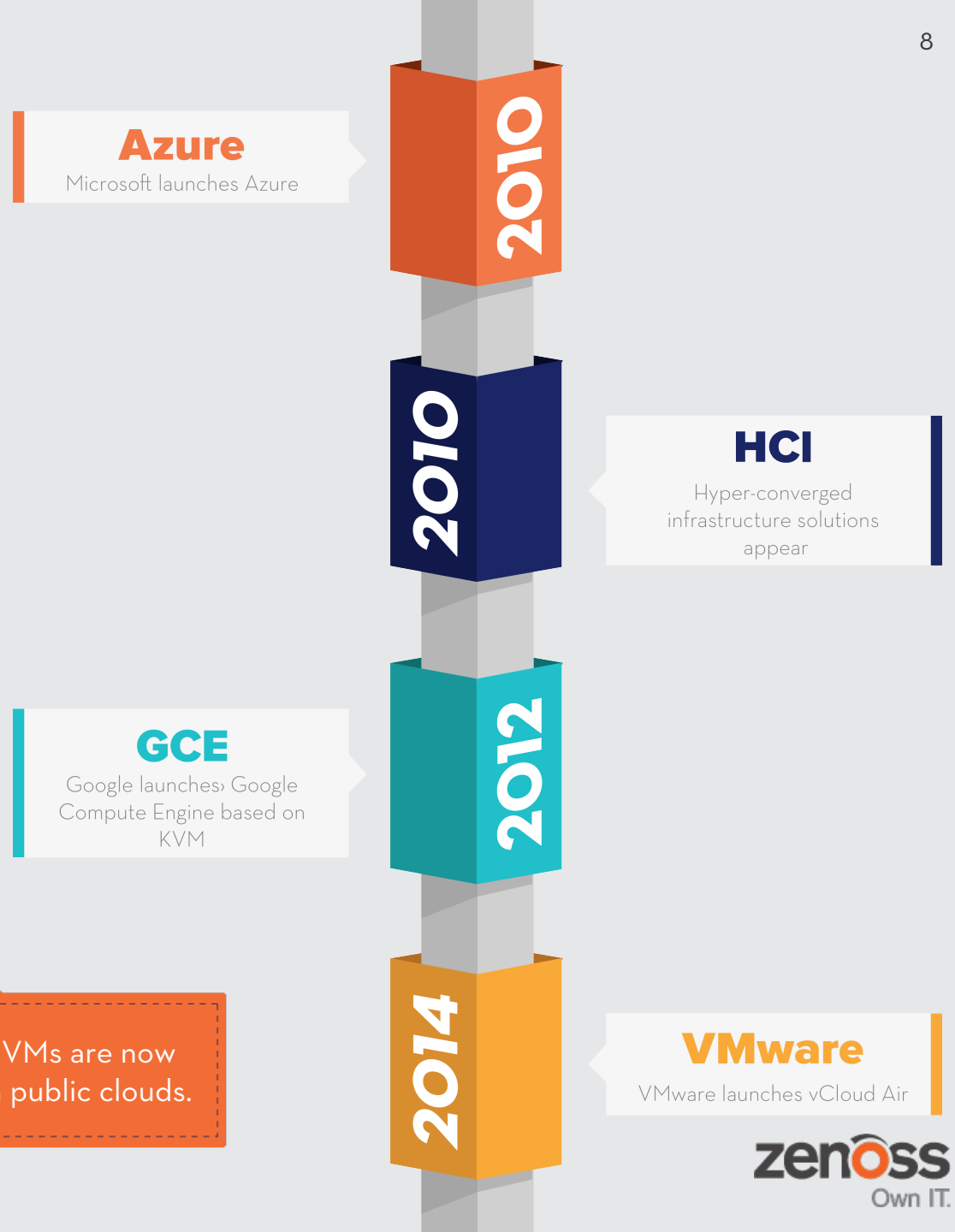


When virtualization essentially became free, or at least accessible without expensive licensing fees, new use cases came to light.

Most notably, Amazon began to use the Xen platform to rent some of its excess computing capacity to third-party customers.

Through their application programming interfaces (APIs), Amazon kicked off the revolution of elastic cloud computing, where the applications could self-provision resources to fit their workloads.

Today, open-source hypervisors have matured and become pervasive in cloud computing. Companies like Google, IBM, HP and Rackspace created their own public cloud offerings, all using the open-source hypervisors Xen or KVM, or both. As such, there is increasing parity in the virtualization market, and technology vendors developing solutions for virtual environments are increasingly required to support all major hypervisors.

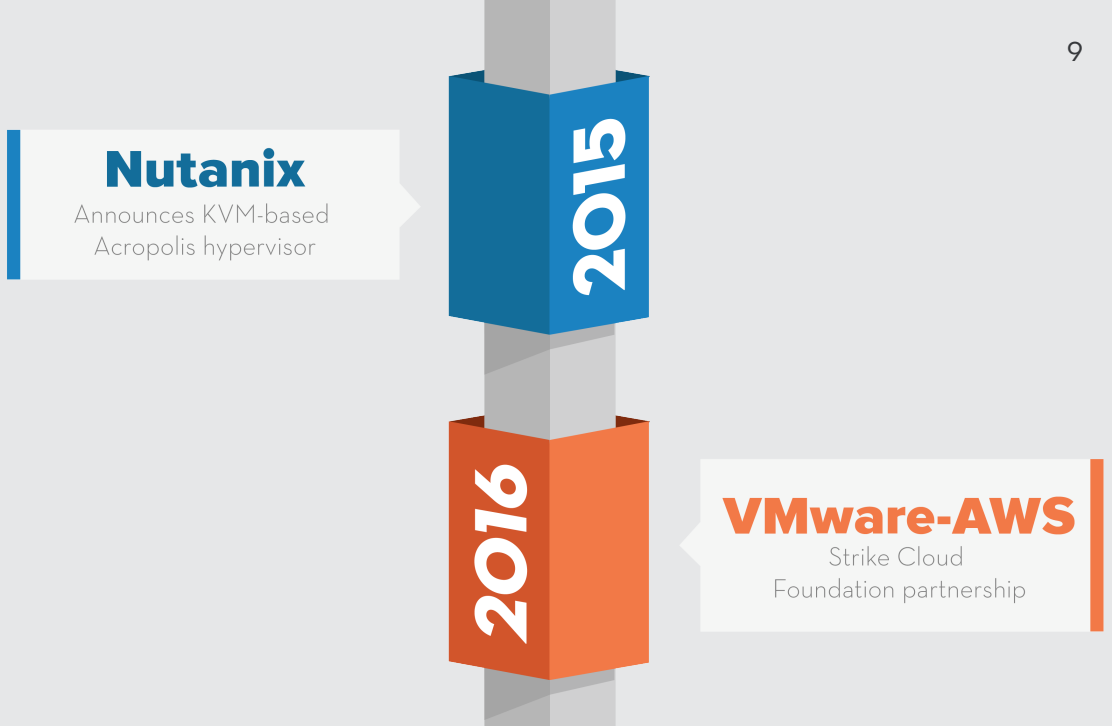


About 15% of all VMs are now delivered through public clouds.

zenoss Own IT.

With this hypervisor parity, innovation became focused on the private/public cloud hardware architectures and the software ecosystems that surround them: storage architectures, software-defined networking, intelligent and autonomous orchestration, and application APIs. Meanwhile, legacy server applications are slowly retiring to give way to elastic, self-defining cloud applications (although they will coexist side by side for some time).

The cloud hardware architectures, evolving software ecosystem, and new breed of ephemeral applications presents new challenges for those tasked with managing these dynamic virtual environments.



Monitoring Virtual Environments

MONITORING VIRTUAL ENVIRONMENTS

New Challenges Emerge

Traditional monitoring solutions are no longer appropriate for the modern virtual environment, according to Forrester Research. Three factors have changed the rules:

1. the number of metrics to monitor
2. uncertainty about the priority of different metrics
3. and lack of expertise in setting reasonable thresholds for alerts and alarms

And the complexity will only increase.

As part of a webinar, a Forrester consultant asked IT professionals to rank their biggest challenges in managing virtualized environments.

The top response was proactive incident monitoring – knowing early when a problem occurs. This was followed by correlating virtual environment data with storage, network or application monitors, monitoring changes to the environment that might cause a security problem, and optimizing the allocation of virtual resources to different users or applications.

These responses reflect the challenges facing IT professionals. Virtual environments are dynamic and complex, and in many cases they form part of a hybrid solution including on-premises and cloud components.

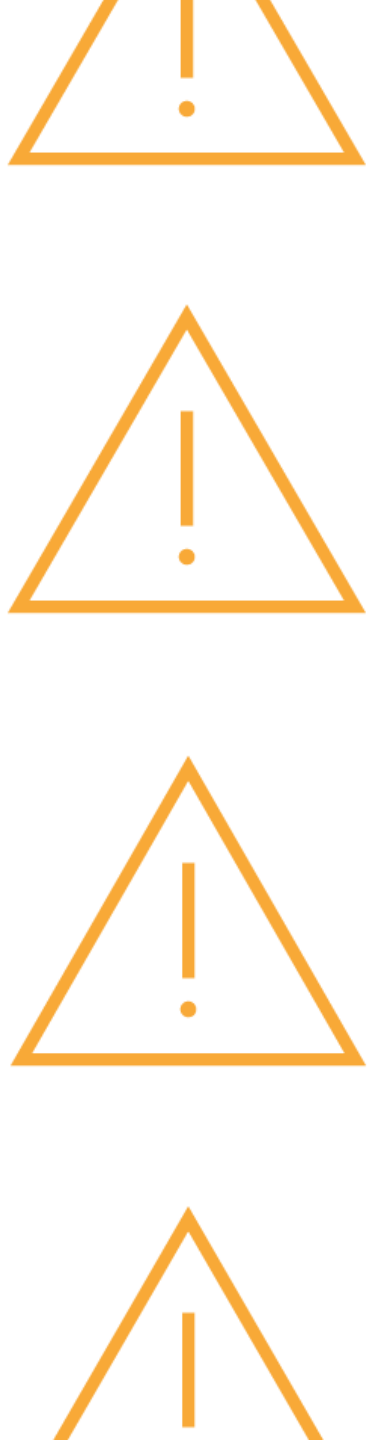
The vast majority of virtualization is in the context of virtual machines, but containers are growing as a virtualization option, driven by easy-to-use developer frameworks, container standards, microservice application demands and cloud computing in general. Consider containers when evaluating virtualization options.

A typical virtualized environment will include virtual machine guests, hosts and hypervisors together with management layers that control performance and availability. These environments are characterized by constantly changing interdependencies, meaning workloads can be difficult to locate as they shift to different virtual and physical machines.

Virtualization makes root-cause analysis more difficult as VMs and applications move between hosts, because the relationships between physical and virtual machines are continuously changing.

To exacerbate the challenge, IT teams are typically forced to use multiple, disparate tools to track performance and issues for the various components in the stack. When problems do occur, pinpointing the source of the issue before disruptions occur is an extremely complex endeavor.

The lack of visibility and inability to detect the root cause of a problem quickly can lead to disruption of service, increased downtime and a poor end-user experience (an outcome which has increasingly become a top priority for IT teams to avoid).



The underlying reason for capacity planning problems is poor systems management techniques and loose IT or business policies.

Stephen J. Bigelow
Senior Technology Editor
Search Server Virtualization

Capacity planning is also more challenging with virtualization.

Because of the dynamic nature of the new environment, there is a risk of under- or over-provisioning services and applications. A resource shortage can degrade the performance of mission-critical applications, while over-provisioning can impact overall operational efficiency and cost control.

Given these problems, it's clear that traditional silo-based monitoring, designed for static environments, cannot diagnose, isolate and resolve performance issues in a modern hybrid environment.

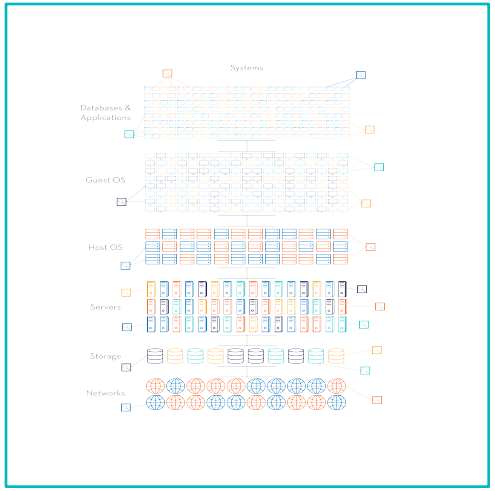
A virtualization monitoring solution that gives deep insight and 360-degree visibility into these complex environments is essential, so new tools and processes must be adopted.

Approaches to Monitoring

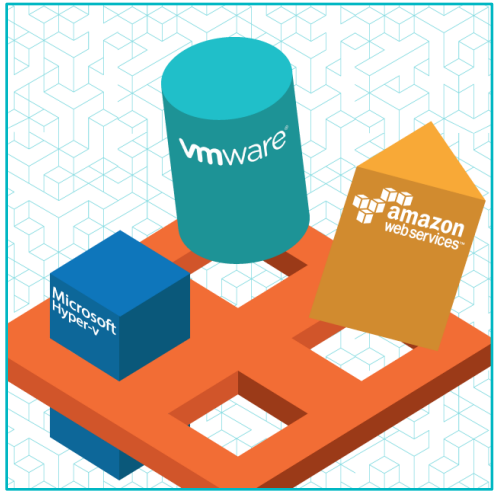
APPROACHES TO MONITORING

There are a number of existing approaches to infrastructure monitoring that each provide benefits and challenges for effective management of highly virtualized environments. These approaches can be effectively summarized in four main categories:

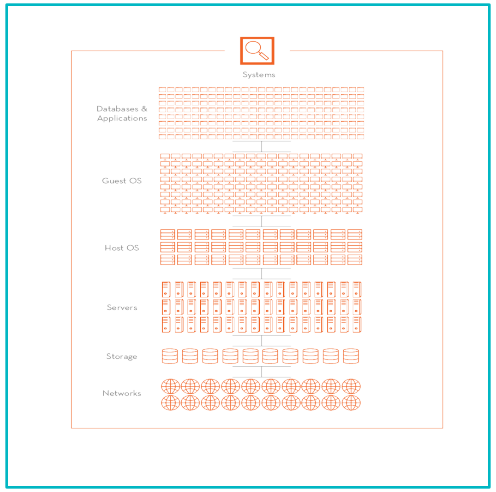
LEGACY FRAMEWORKS



POINT SOLUTIONS



VENDOR STACKS



UNIFIED MONITORING

zenoss Own IT.

LEGACY FRAMEWORKS

The original monitoring frameworks, developed by vendors such as IBM, HP and CA Technologies, were designed to provide insight into the static building blocks of traditional data centers like servers, storage and network switches. Unfortunately, the legacy architectures that these tools were built on predate heavy virtualization adoption, and in most cases they have required additional tools in order to gain visibility into modern virtual environments.

In some cases, legacy vendors have added tools via acquisition to allow for virtualization monitoring. However, these tools often require manual integration or are simply separate tools, and bring with them separate licensing contracts and costs. Tool sprawl and platform lock-in can become increasingly problematic as additional technologies such as containers and micro-services are incorporated into virtualization platforms.

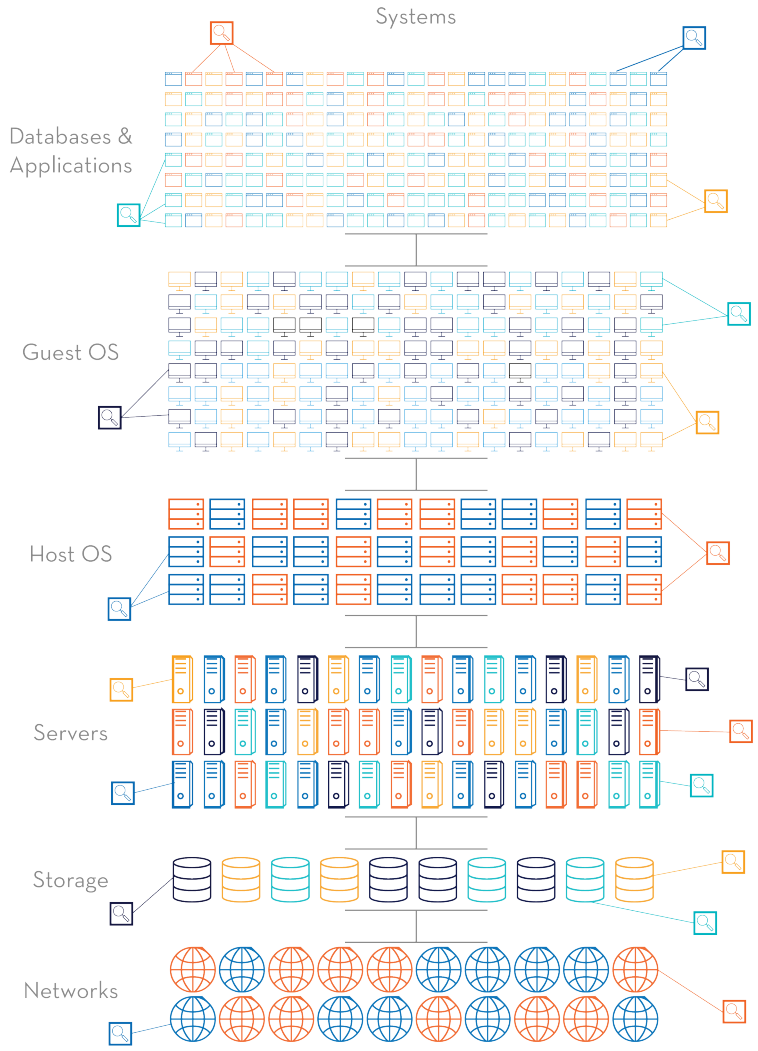
POINT SOLUTIONS

Point solutions are monitoring tools designed for specific technology areas like networking or database management that provide deep insight into specific technology silos.

These tools can allow individual departments to gain very granular insight into the hardware or systems that they control and manage.

However, this approach can often lead to tool sprawl and the walling off of information between groups, causing distrust and even finger-pointing when problems occur.

Having point solutions that do not span departments can also greatly increase Mean Time to Resolution (MTTR) during service degradations or outages.



zenoss Own IT.

VENDOR STACKS

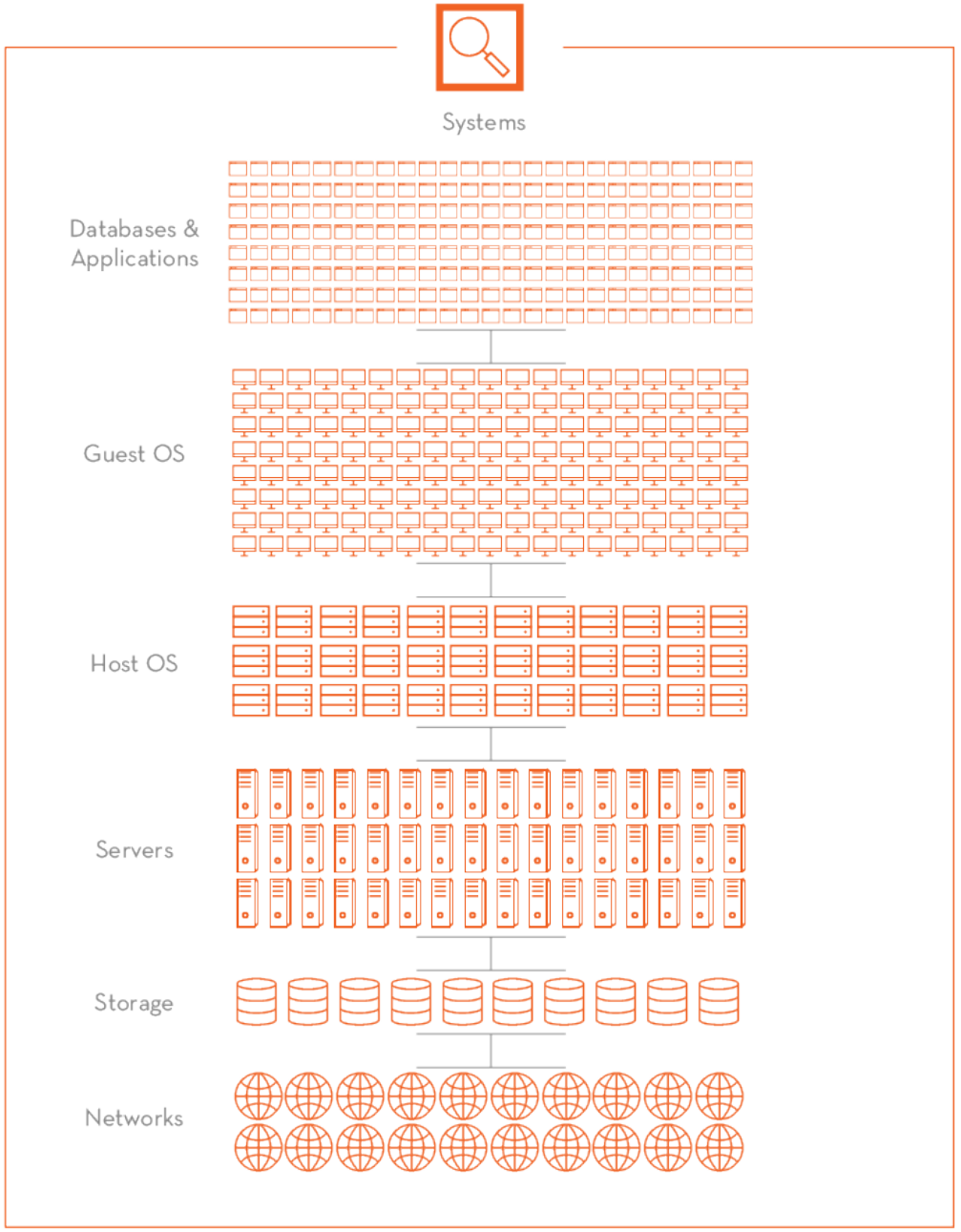
These solutions, provided directly from virtualization vendors like Microsoft and VMware, are designed specifically for the hypervisors they support. They deliver thorough coverage for all facets of the software stack provided by that vendor, and have made attempts to extend monitoring beyond their own platforms.

These tools are exceptional at integrating with other tools sets provided by their vendor and its vendor partners, but can become problematic for heterogeneous environments or companies looking for best-of-breed solutions, as the providers are fundamentally opposed to supporting competing products (e.g. Hyper-V and Azure are both Microsoft products, but VMware or AWS would be competing technologies to those offerings). Thus, vendor lock-in is a risk.

UNIFIED MONITORING

Solutions that are positioned as "unified" are those that offer open and extensible platforms, designed specifically to allow custom integration or the addition of new functionality for holistic coverage across frameworks, software platforms, device types and even physical locations. These tools are designed for heterogeneous environments, and in many cases are primarily targeted at large enterprise-class ecosystems.

In addition, because of the dynamic nature of modern technologies, these tools must also connect with adjacent IT systems like incident management and orchestration platforms to provide automation across the IT toolchain. The greatest value of a unified platform is customization; however, this can be challenging or unnecessary for small IT environments with a very limited number of vendor technologies.



Why Effective Virtualization Monitoring Matters

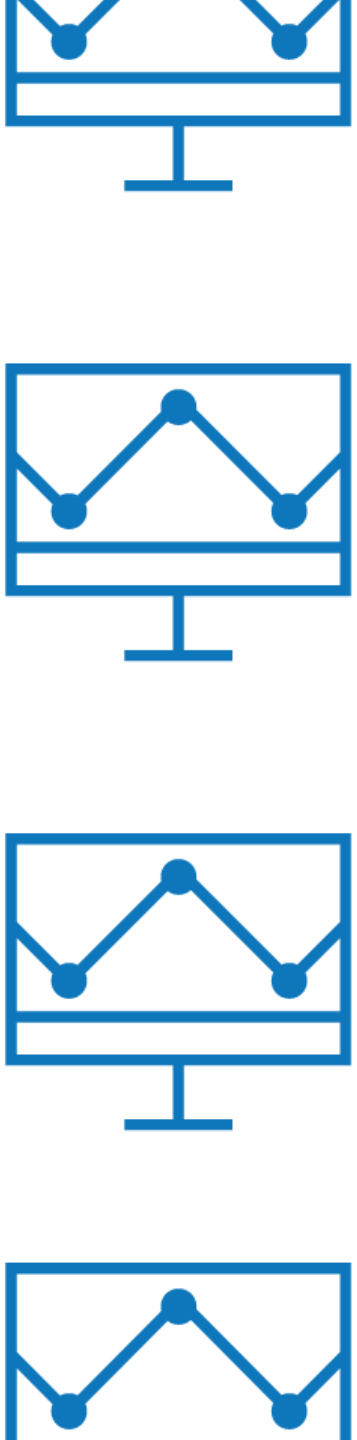
zenoss
Own IT.

WHY EFFECTIVE VIRTUALIZATION MONITORING MATTERS

The growing acceptance and maturity of virtualized environments demonstrate that organizations not only use them for smaller, non-critical applications such as file and print servers or development, they now deploy business-critical resource-intensive services and applications, such as enterprise resource planning (ERP), production and email on virtualized infrastructures.

That accelerated acceptance has, in turn, spurred organizations to adopt other business-impacting technologies like converged infrastructures and "software-defined everything," all of which are leading the industry through a complete digital transformation. Virtualization functions as the cornerstone by demonstrating important financial and operational benefits through reduced hardware and related support costs, increased flexibility, lower energy costs and greater space utilization, delivering lower total cost of ownership (TCO) for businesses of all types.

To realize the full benefits of virtualization, three factors are essential: maximum availability, optimum resource utilization and low TCO.



zenoss Own IT.

AVAILABILITY

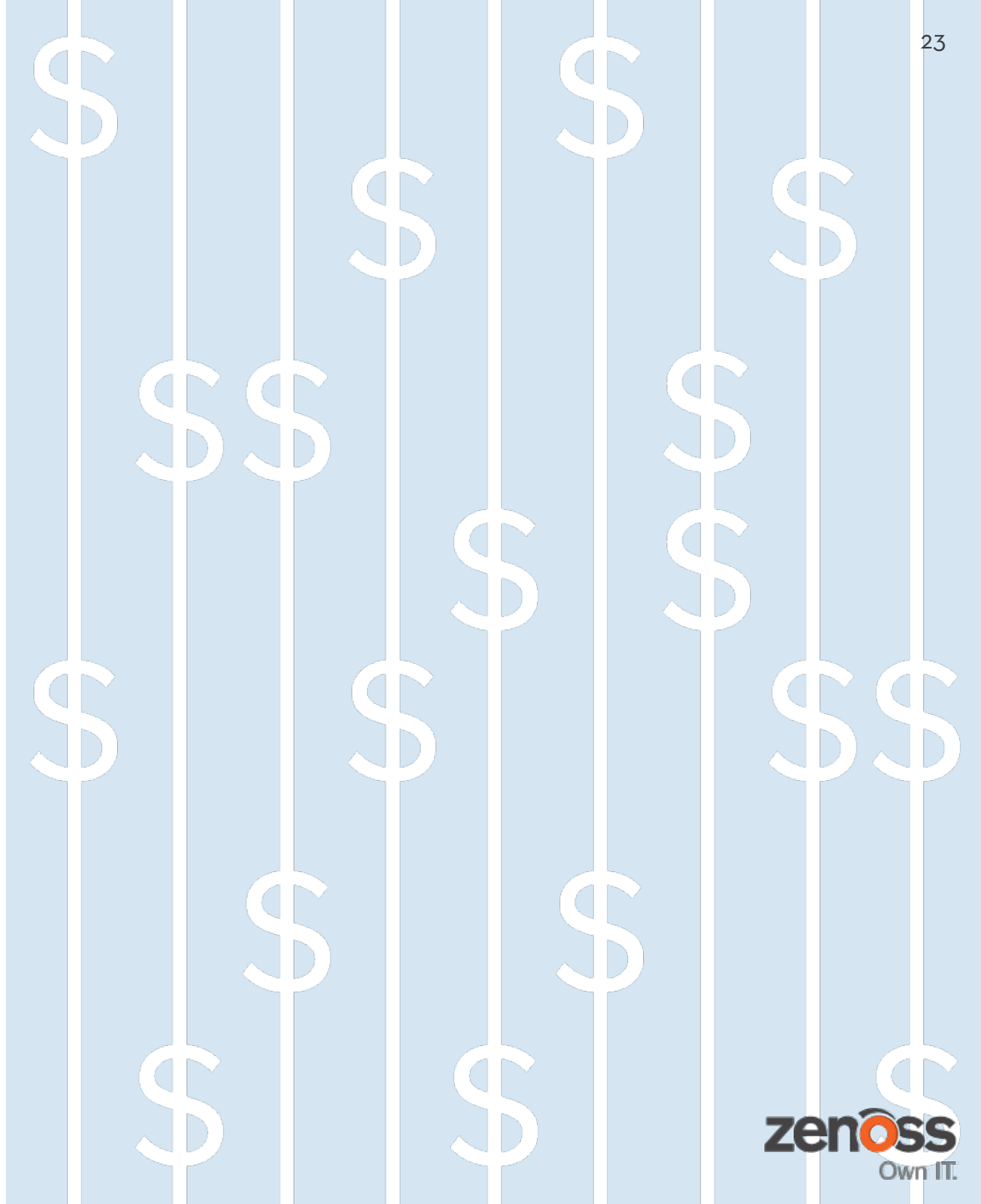
Availability is a key benefit of virtualization, but it is not guaranteed. Precise monitoring tools and techniques are essential to enable proactive problem identification, faster root-cause analysis and intelligent event correlation. When services that depend on virtualized resources experience issues, or dynamically require additional resources, their dependencies can change quickly.

Understanding these dependencies, how they affect other services, and the patterns that underlie the initial cause are the keys to ensuring service availability in a highly virtualized environment. Monitoring systems must be able to quickly adjust and provide full visibility in real time to the underlying devices and systems a service depends on.

TOTAL COST OF OWNERSHIP

If your investment in virtualization doesn't deliver tangible business benefits, like increased agility or heightened service levels, and if it doesn't also reduce your total cost of ownership, then the effort to virtualize is a wasted one, and you may as well maintain a physical environment. Your monitoring solution should also play a part in the overall cost-control agenda by providing straightforward pricing models that allow you to understand the cost effects of quickly spinning up new resources in a monitored environment.

Tools that charge licensing based on the number of virtual devices, or that require separate licensing for added virtualization monitoring functionalities, can quickly offset the cost benefits that virtualization was intended to create. In addition, your monitoring solution should help improve capacity planning and system utilization functions to ensure the highest return on overall system investments.



UTILIZATION

Virtualization has the potential to allow IT departments to fully optimize hardware utilization. However, this requires a high degree of orchestration and automation so that you can push the envelope on capacity usage without over-provisioning resources. Your monitoring tool needs to tightly integrate with the other systems in your IT operations management (ITOM) chain to enable a seamless workflow.

For instance, if a resource is running out of memory, your monitoring tool needs to not only alert on it, but (as part of a modern monitoring tool chain) confirm that resource is supporting a critical service and then kick off a runbook with an automation tool (like Chef, Puppet or SaltStack) that allocates, or spins up, more resources automatically. Your monitoring tool should then also automatically be notified of the new resource allocation, close the initial alert, and then monitor the new resource and its relationships.

A Unified Approach to Monitoring Virtualized Environments

A UNIFIED APPROACH TO MONITORING VIRTUALIZED ENVIRONMENTS

IT teams need a single, comprehensive, easy-to-use solution to meet the challenges and problems of monitoring complex virtualized environments.

By combining host, guest and workload monitoring with a comprehensive visualization of physical servers and network devices, teams can simplify management with a single solution for monitoring the complete virtual infrastructure.

These solutions typically feature a model-driven architecture and are capable of automatically tracking virtual configurations and relationships while providing complete event visibility, performance measurements, testing thresholds and availability reports.

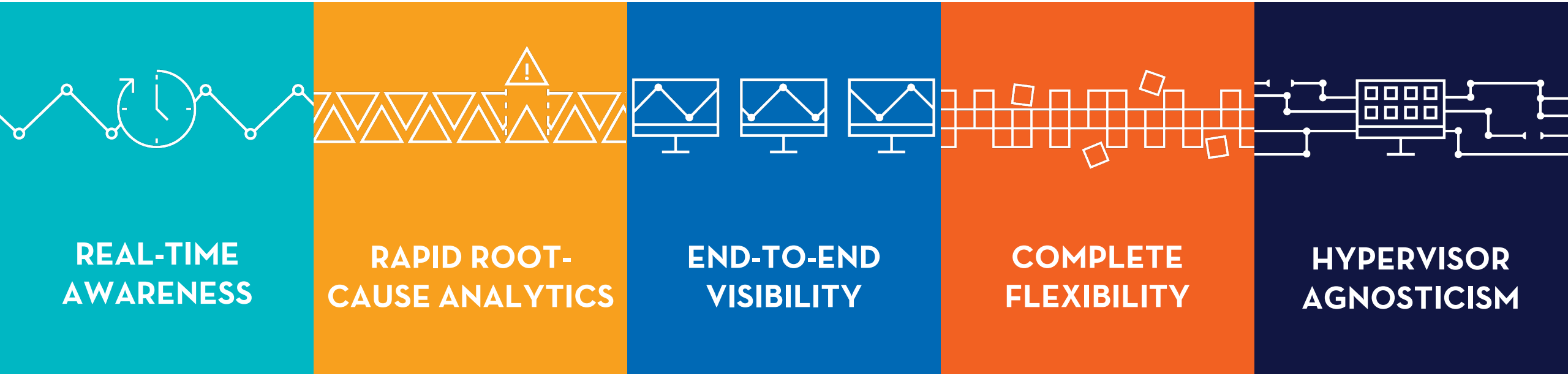
Modern monitoring solutions enable teams to monitor services automatically and consistently, to prevent service disruptions and to report on service levels for physical, virtual and cloud resources.

They eliminate the problems inherent to a "multiple tool" approach by unifying performance and availability monitoring of applications, databases, middleware and web servers, regardless of their physical or virtual locations.

Five key capabilities are required to provide this level of monitoring:

- **REAL-TIME AWARENESS**
- **RAPID ROOT-CAUSE ANALYTICS**
- **END-TO-END VISIBILITY**
- **COMPLETE FLEXIBILITY**
- **HYPERVISOR AGNOSTICISM**

5 KEY CAPABILITIES FOR VIRTUALIZATION MONITORING



zenoss Own IT.

Virtual environments are inherently ephemeral and, unlike static environments, require a real-time management approach. IT teams must be able to capture and track ongoing changes as they occur, monitoring events such as creation or deletion of virtual machines (VMs), pausing or stopping VMs, and provisioning or deprovisioning of resources.

You also need to track compute and storage assignments as they move from host to host in real time. With up to millions of metrics being collected in real time, you need visibility into the health of the entire hybrid IT infrastructure to understand risk situations and accelerate problem resolution before service disruptions occur and business is impacted. This real-time awareness is a required foundational element of any modern monitoring solution.

DISCOVERY

Standard discovery capabilities in a virtual environment include detecting new VMs, host system components (e.g., CPUs), resource pools, clusters, virtual disk images and network adaptors. But the more critical aspect of discovery in an environment where VMs are continuously spinning up and down is the interdependency modeling.

Any monitoring tool should be able to track the creation of a new VM and track basic health and status during its lifetime. But only service-centric monitoring solutions are capable of on-demand discovery that dynamically maps the full stack topology and interdependencies.

PERFORMANCE

Mainstream virtualization adoption was initially driven by the value of higher availability, improved utilization and lower TCO. But as organizations move more mission-critical and resource-intensive applications to virtualized environments, there is an increased focus on performance of these environments. To ensure peak performance, it's critical to continuously monitor utilization across the entire stack and identify any deviations in service levels.

A beautiful thing about virtualization is the ability to quickly respond to these performance issues by dynamically reassigning resources, so IT operations teams need constant awareness of performance and utilization levels for applications, guest operating systems, host operating systems, servers, storage and network components.

PREDICTIVE THRESHOLDS

Each organization's virtual environment is unique. This is even more true in elastic, virtual environments, where workloads can vary dramatically in resource type utilization, in persistence and in volume. While a variety of tools typically offer performance and utilization measurement, this information is only useful when it's actionable. To offer actionable information, a monitoring platform for virtual environments needs to be tuned for the specific environment.

Custom thresholds allow IT teams to tune performance monitoring to match their workloads and resources, which is required to help predict true performance issues that may impact services. When deploying a solution, a key step is baselining the environment, then configuring the appropriate predictive thresholds to recognize relevant deviations in service levels.

EVENT MANAGEMENT

Event management facilities gather data from the different systems and components in a virtualized environment to increase real-time awareness of problems or performance issues. At the heart of everything, this is how a monitoring and analytics platform becomes and remains aware of the status of everything in the environment. The platform intelligently correlates and deduplicates system events, fault notifications and status changes for all systems in on-premises and cloud infrastructures.

Administrators can take manual action in response to events, or can integrate with incident management systems to automate management of response activities. Robust event management capabilities provide a single source of information that can reduce costs and increase IT efficiency through prioritization and automation of event workflows.

RAPID ROOT-CAUSE ANALYTICS

In the end, the primary driver for deploying a monitoring solution is to know how application and service issues in your virtual environment are going to impact end users, and ultimately how they can impact your business. Your virtualization monitoring solution should allow you to assess impact and expedite root-cause analysis before disruptions occur. An effective solution will include service policy configuration so it can be tuned for your specific environment.

It must also have dashboards for real-time status of all virtual and physical resources. Without these key elements, you're monitoring for monitoring's sake. When considering monitoring solutions, a key decision criterion should be the solution's ability to quickly assess potential service impact and accelerate root-cause analysis so your IT teams can resolve issues before disruptions occur.

MEAN TIME TO RESOLUTION (MTTR)

ZENIUS

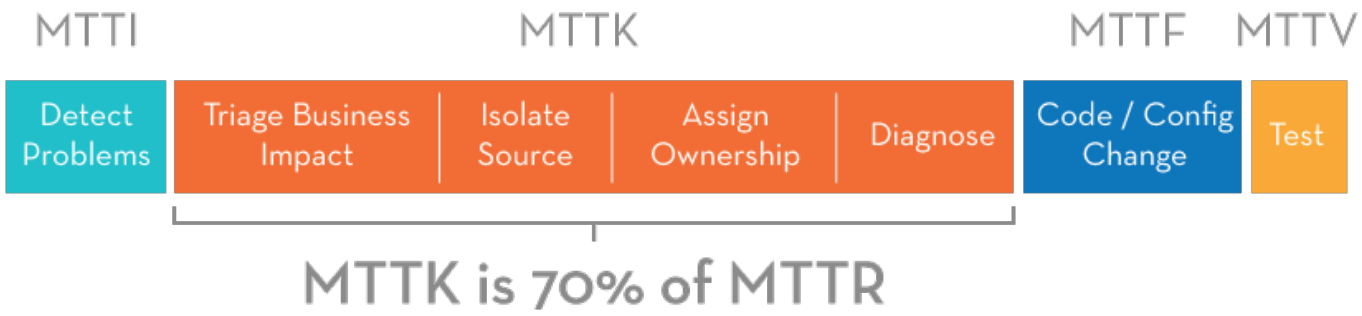
TIP

MTTR is the industry standard measure for issue resolution effectiveness.

zenoss

MTTR can be broken down into four stages:

1. Mean Time to Identify (MTTI) – issue detection
2. Mean Time to Know (MTTK) – triage, isolation, assignment, diagnosis
3. Mean Time to Fix (MTTF) – code, configuration or component change
4. Mean Time to Verify (MTTV) – quality assurance of implemented fix



zenoss Own IT.

RELATIONSHIP TRACKING

Virtualization supports the sharing of a common set of physical resources among many virtual machines. This provides high availability and workload balancing across a virtualization cluster. Solutions such as VMware's vMotion or Microsoft's Live Migration, for example, can move live VMs from host to host with no disruption in service. Real-time VM migration is a wonderful thing, but it invariably translates to management complexity due to the dynamic nature of the relationships between virtual machines, physical hosts and storage systems.

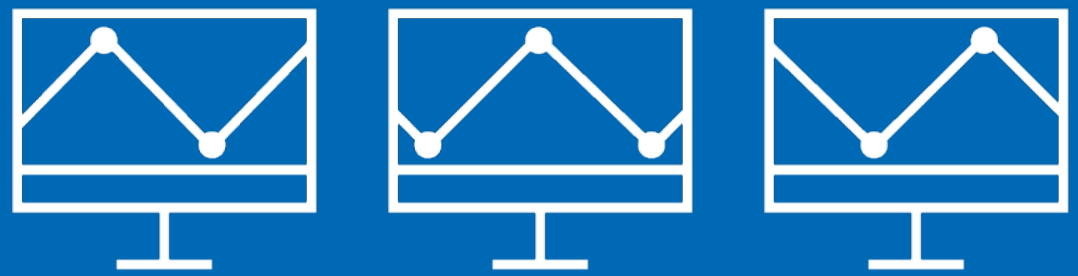
Tracking these relationships is nontrivial, especially in multisite and mixed hypervisor environments. Solutions designed for monitoring virtualized environments include features that support relationship tracking in real time. This is a non-negotiable capability when it comes to troubleshooting and preventing service disruptions.

SERVICE IMPACT

An effective virtualization monitoring solution doesn't just identify problems and root causes, it can analyze service impact by gathering and collating events, alerts and metrics, and by identifying services that are at risk of going down or degrading. That helps IT teams understand potential problems and prioritize responses based on severity and the likelihood of a service disruption.

Solutions that incorporate dynamic service impact modeling automatically generate service and infrastructure topologies, automatically tracking all environment changes to maintain a real-time picture of current relationships and dependencies. In addition to expediting root-cause analysis and resolution, platforms with service impact capabilities can simulate scenarios to identify exposures in infrastructures and services.

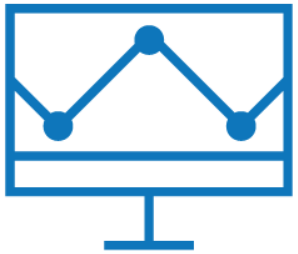
END-TO-END VISIBILITY



Basic virtualization tools typically provide management capabilities for monitoring the environment at the hypervisor and guest OS level. Some offer additional capabilities, either inherently or through integrations, for physical server and/or storage management. But that's typically reaching the limitation of these basic tools. Furthermore, purchasing virtualization management software from a virtualization (i.e., hypervisor) vendor in every case means being limited to single-hypervisor support.

Working with these basic tools means almost every environment will require additional tools to manage the rest of the environment, and potentially multiple tools for multiple hypervisor types. This precludes you from seeing the big picture. A unified monitoring platform for broader environment monitoring provides a complete view of the physical and virtual environment – the only way to tune end-to-end performance and truly ensure issues are resolved before disruptions occur.

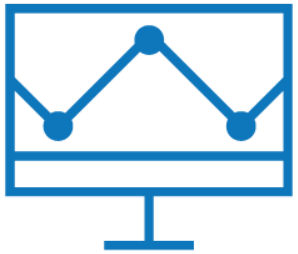
SYSTEMS



A modern monitoring platform that's suitable for virtual environments will monitor the entire stack, including applications, databases, file systems, guest operating systems, host operating systems, servers, storage and network devices. This entails more than up/down monitoring – it should include monitoring all key attributes for each type of system, including memory, CPU, storage, I/O, etc.

Where systems or attributes aren't supported out of the box, the platform should be extensible to allow customization of the data collectors. The platform should also be capable of mapping the dependencies and relationships in real time to provide complete insight into performance and service impact. A unified solution eliminates the complex, costly and ineffective scenario of having one tool per vendor or system type.

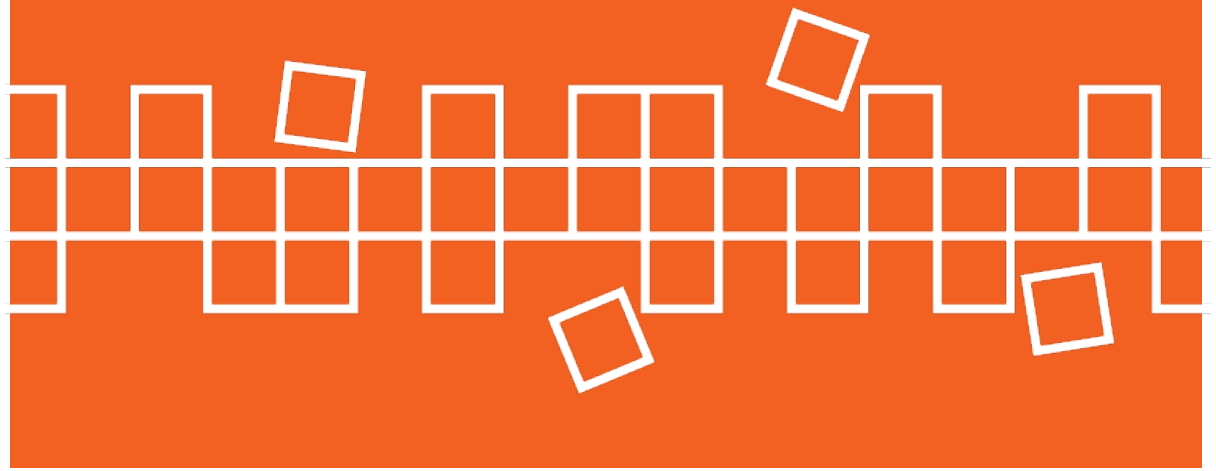
CAPACITY PLANNING



Understanding all key attributes of all interconnected systems, and understanding the relationships between them, is necessary to predict the need for additional resources. Optimizing the utilization of an IT infrastructure can help reduce overall costs and make more efficient use of IT resources, as well as prevent VM sprawl.

Unified monitoring platforms help teams understand resource utilization throughout the entire stack in physical, virtual and cloud environments. This enables IT operations teams to prepare for budget cycles, ensure responsive systems and applications, and eliminate unnecessary costs and complexity.

COMPLETE FLEXIBILITY

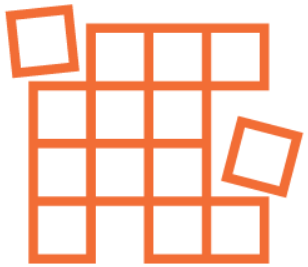


No monitoring solution can provide maximum value as a standalone entity. Vendors who develop modern monitoring and analytics platforms have recognized this and offer greatly increased value through integrations and extensions. With the layered stacks of virtualized environments, the need for this flexibility is reinforced.

Managing these dynamic and ephemeral environments requires a flexible monitoring platform that can be customized with standard APIs or extensions (plug-ins) to provide the broadest coverage of existing infrastructure resources, and to extend monitoring to new technology resources.

The solution should feature a platform that's architected to be extensible so that IT teams can unify, enhance and extend monitoring capabilities without the need to replace existing tools or acquire additional ones.

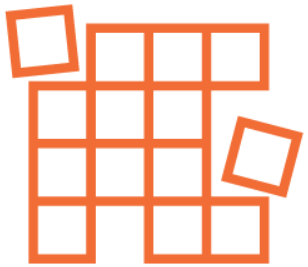
INTEGRATIONS



Today's virtual monitoring platforms rely on integrations to enable automating routine and complex tasks throughout the ITOM model. This includes automating discovery, ticketing creation and performance or system failure response actions, and even integrating with complex configuration management systems.

With the ultimate goal of complete digital transformation in mind, significant weighting should be placed on integration capabilities that automate and streamline cross-team processes, achieve much higher levels of productivity, and eliminate issues caused by human error. When evaluating monitoring platforms, make sure you closely review the ecosystem of solutions whose effectiveness can be improved by that platform.

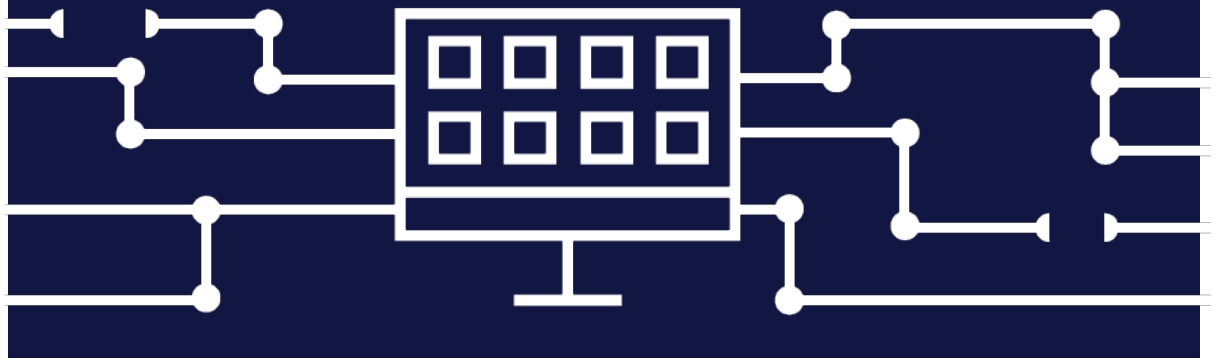
EXTENSIONS



Extensions, or plug-ins, are modules that use standard APIs and protocols including SNMP, WMI and SSH. They're the connectors between monitoring platforms and the systems they monitor. They collect configuration information and monitor specific elements, devices or systems without the need for agents, which consume system resources, are often difficult to deploy, and are limited by compatibility issues. Extensions have the capability to discover hosts, host CPUs, virtual machines, resource pools, clusters, virtual disk images, network adaptors and other key components.

They monitor memory, throughput, CPU utilization, storage and disk read/write metrics, as well as collecting events and forwarding them to a management console. These modules are also critical in mapping service impact relationships between components in the stack. You should choose a monitoring platform that not only has robust coverage with out-of-box extensions, but also offers the ability to easily create new extensions for your organization's custom systems and applications.

HYPERVISOR AGNOSTICISM

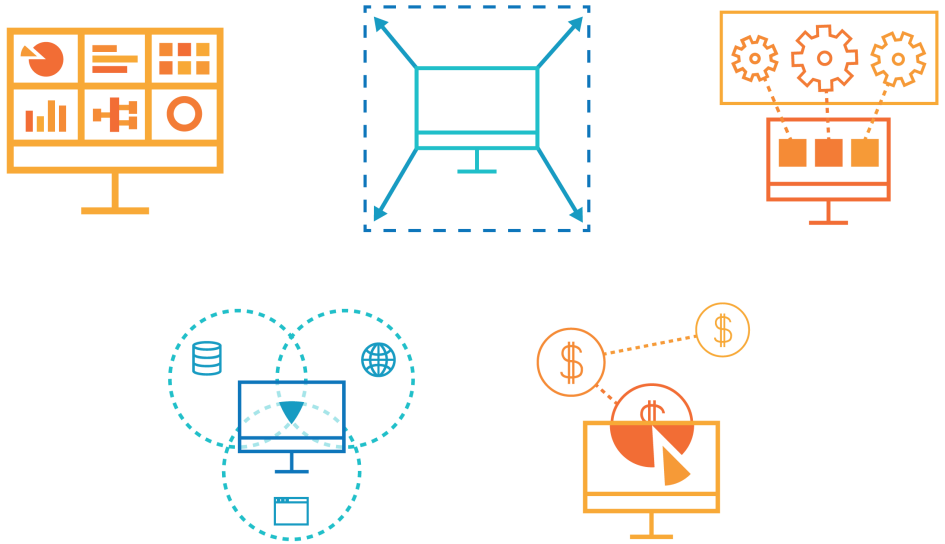


In the hierarchy of needs, this is a simple yet critical requirement. You may currently have a homogeneous virtual environment. But relying on single-hypervisor management solutions inherently means you're locked in. For a range of reasons, including mergers and acquisitions, full or partial cloud migration, new application support, or simply infrastructure diversification, most organizations eventually need to support multiple hypervisors.

At a minimum, your management solution should support VMware vSphere and Microsoft Hyper-V, and ideally also support Citrix XenServer and KVM. And at a minimum, this support should include automatic discovery of and performance metric collection for components such as resource pools, hosts, host CPUs, physical block devices, NICs and storage repositories.

Evaluating a Monitoring Solution

EVALUATING A MONITORING SOLUTION



Additional Considerations

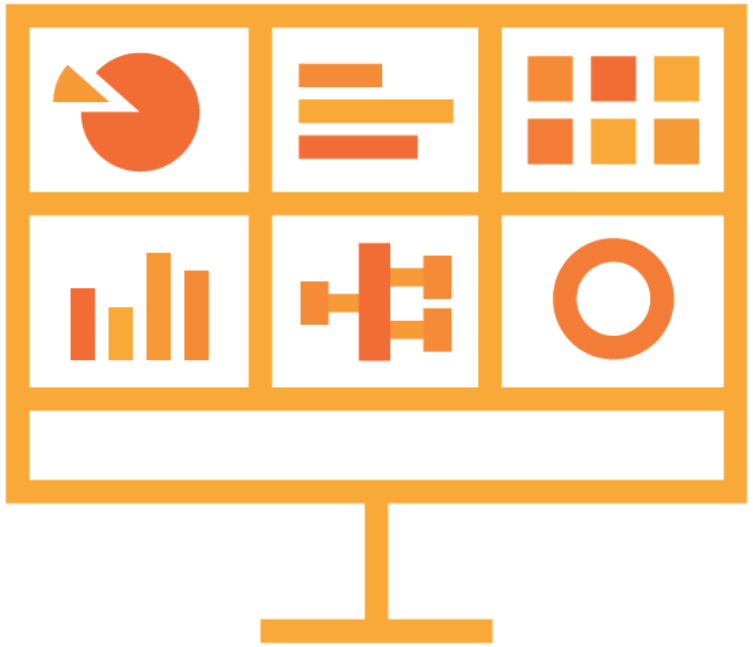
Monitoring solutions for virtualized environments must provide the five essential features of real-time capability – real-time awareness, rapid root-cause analysis, end-to-end visibility, flexible customization and support for multiple hypervisors. However, there are a number of other important capabilities that could be pivotal in the success or failure of your monitoring platform deployment.

These include:

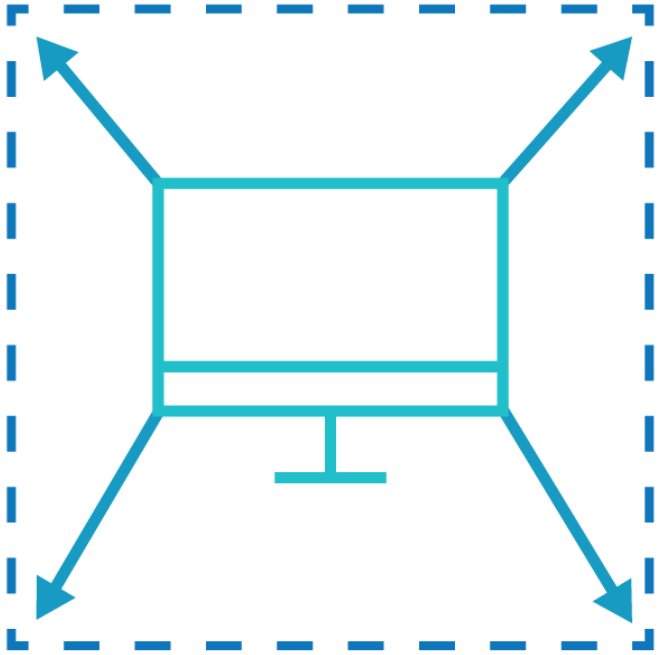
- **Unified view**
- **Scalability**
- **CMDB support**
- **Converged infrastructure support**
- **Licensing**

UNIFIED VIEW

Monitoring solutions offering a unified view enable IT teams to view and monitor the entire stack through a single console. This eliminates duplicate costs, ensures that teams can assess the status and dependencies of all infrastructure components, and makes it easier to expedite root-cause analysis and prevent service disruptions.



SCALABILITY



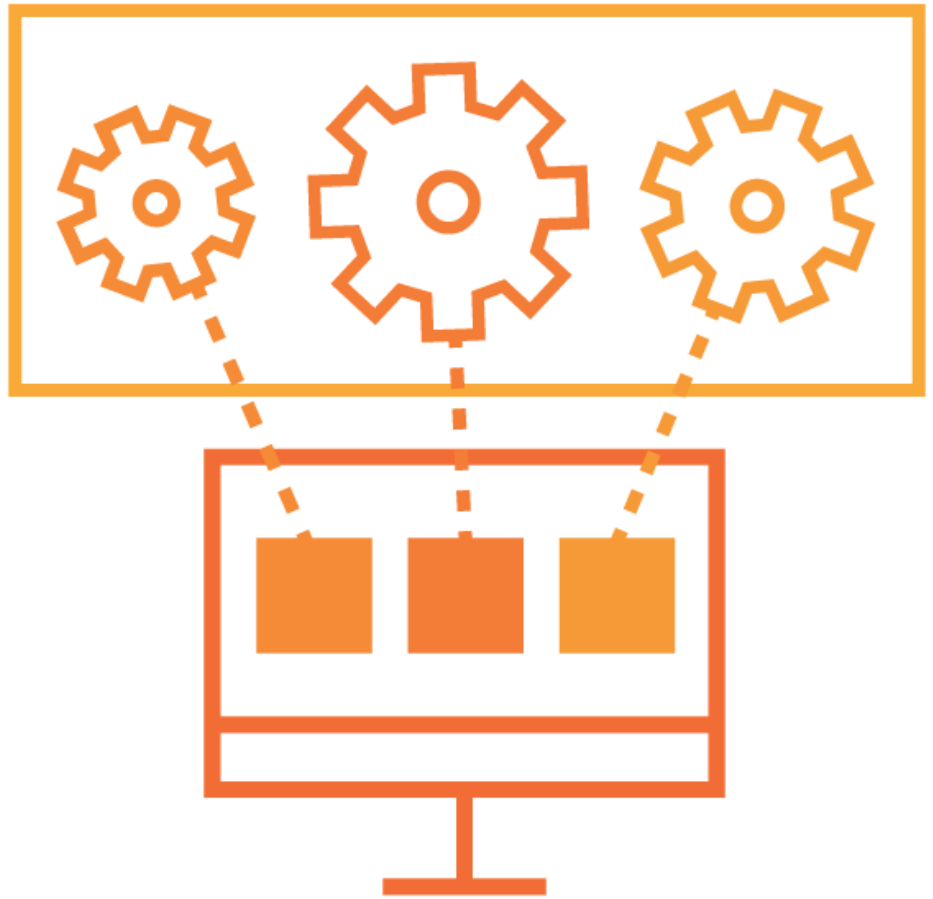
Virtualized environments can be dynamic and complex. For scaling purposes, they demand management solutions have an elastic approach to monitoring and data collection, and they require big data back ends (e.g., OpenTSDB HBase). They should also be capable of load-balancing monitoring services across pools of resources. They should have centralized, out-of-band management for ease of deployment and upgrades. There is also the binary aspect of requiring or not requiring agents.

When it comes to scaling for enterprise and service provider environments, agentless solutions are the only viable option, allowing you to avoid the management and compatibility limitations inherent in agent-based solutions.

While many monitoring solutions work effectively at small scale, few have the flexibility and capability to operate in elastically scaling environments. Monitoring solutions must give the team the ability and the confidence to see, know and act responsively at scale.

CMDB SUPPORT

A configuration management database (CMDB) stores information on all the significant entities (configuration items) and their relationships in the IT infrastructure. A well-architected monitoring solution can leverage the CMDB through integrations, automating the intake of new targets to monitor, device information, controllers and other attributes. The monitoring platform should also be able to populate the CMDB with additional information it gleans through its own connectors or plug-ins.



CONVERGED INFRASTRUCTURE

Converged infrastructures integrate diverse IT components into a single, optimized solution. This type of infrastructure typically includes servers, data storage devices, networking equipment and software for management, automation and orchestration. Although all converged systems come with some management tools, it's far more effective to utilize a central platform to unify monitoring of converged infrastructure, as well as traditional and cloud-based systems.

At a minimum, your monitoring platform must understand relationships between operating system workloads and virtual machines, virtualized hosts and service profiles, and data stores and LUN-based storage. It must visualize workload relationships and track service dependencies between components and underlying dynamic infrastructure. This is no different than monitoring traditional virtual environments, but further includes the management of packaged converged systems.

LICENSING

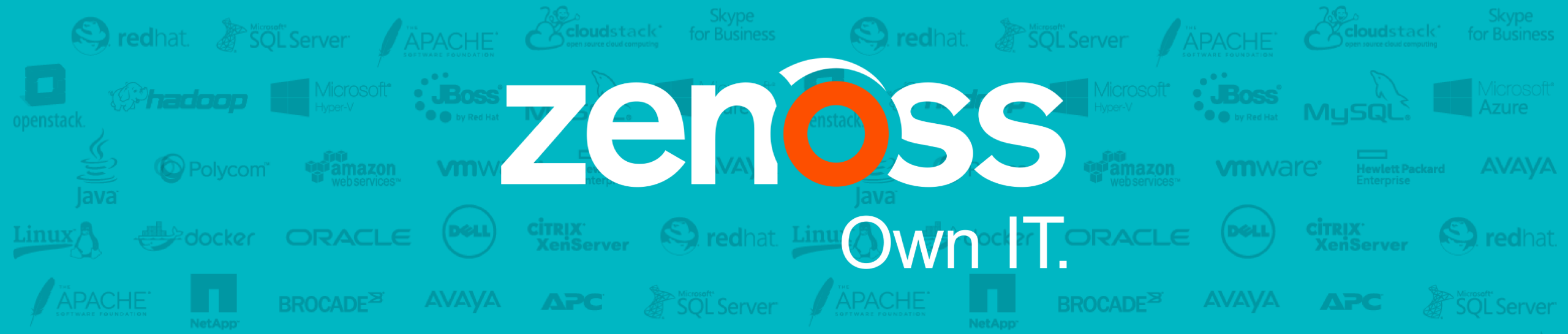
Virtualization licensing can be complex as well as expensive. A monitoring solution should offer simple licensing that can be easily managed. While this is rarely top of mind when evaluating solutions, it can be a source of great pain if not given the proper attention.

Zenoss for Virtualization Monitoring

Zenoss works with the world's largest companies to ensure their IT services and applications are always on. As the global leader in hybrid IT monitoring and analytics software, Zenoss provides complete visibility for cloud, virtual and physical IT environments.

The Zenoss unified monitoring platform provides a single view of all systems and interdependencies in real time, eliminating monitoring complexity and making it easy for IT teams to identify and resolve issues before they cause disruptions with IT services.

The Zenoss model-driven architecture automatically tracks virtual configurations and relationships while providing complete event visibility, performance measurements, testing thresholds and availability reports.



For more information on Zenoss virtualization monitoring solutions:

www.zenoss.com

1-512-687-6854 direct)

1-888-936-6770 (toll free)

linkedin.com/company/zenoss-inc-

twitter.com/zenoss

zenoss Own IT.