IT Monitoring Buyer's Guide: How to Make the Right Choice

opsview

TABLE OF CONTENTS

STUMPED BY IT MONITORING SHOPPING?

System administrators make choices everyday, especially when shopping for the software, hardware and gadgets that make work easier.

Choosing IT monitoring software can be hard. The market can be sliced up many ways: open source or closed, on-premises or hosted, the big names or the smaller dedicated providers, free or paid, and more.

But the solution you choose ultimately needs to address your unique needs across not only your IT department, but every department that has a stake in critical business systems. You have a lot to consider:

- The scope and nature of your IT environment
- The experience level of those who will manage the tool
- Your required level of security, visibility, automation and more.

Beyond functionality, you also need to consider the larger IT or business goals that your monitoring platform will help you achieve. Are you moving toward a **strategic IT approach**, and therefore need a solution that allows you to be proactive, avoid day-to-day firefighting and support broader business objectives? Or are you comfortable with your existing workflow and just need a solution that can **address an immediate need**?

Luckily for you, you have no shortage of options, whether you're looking to upgrade from an existing platform or monitor a new network from scratch.

In this Buyer's Guide, we dive into the top considerations in the IT monitoring buying process, including the most important factors to look for, how to evaluate solutions and most importantly, exactly where to start. **With insight from our own expert sysadmins**, we're covering everything you need to know to make a better purchase.

PROPRIETARY VS. OPEN SOURCE

The differences between **proprietary and open source software** aren't as big as some might think, despite the rift between the two camps supporting each side. Today, there are a number of paid IT monitoring solutions that had their roots in free open source technology, and many companies use both proprietary and open source applications in their offices without a second thought.

All the same, you'll likely encounter both distribution models as you search for a new platform, so it's worth understanding what you'll get from each.

OPEN SOURCE

Source code freely available for modification, often worked on by community of developers

Advantages

o **Mostly free**, with paid add-ons
o Highly configurable
o Community of **developers** to improve code

Disadvantages

o Varied community engagement can create **gaps in updates or support**
o Over-customization can lead to **narrow usability, knowledge silos**
o No dedicated technical support
o Limited headline features

PROPRIETARY

Source code exclusively licensed and modified by developer

Advantages

o **Domain expertise** from established, well-funded companies
o Consistent updates
o Dedicated tech support
o **Out-of-the-box features**
o Less of a learning curve

Disadvantages

o Prices vary, but **generally more costly**
o Limited customization

WHAT'S IN THE CODE?

Interestingly, the differences in quality between open source and proprietary can be minimal. Software testing firm Coverity compared code quality between a sample of open source and enterprise solutions to measure defect density, which describes the number of code defects per 1,000 lines of code. According to the results, **open source averages 0.59 defects per code, better than proprietary's 0.72 average**. [2]

However, Zach Samocha, Coverity's senior director of product management, clarified to CMSWire in 2013 that **open source typically only has the advantage for projects with fewer than 1 million lines of code**. Anything over that threshold means proprietary typically has the advantage, he said. [3]

The bottom line? Unless you're a hardline subscriber to one particular ethos, **the choice between open source and proprietary has less to do with what's "better" and more to do with your company's specific needs**.

You'll need to evaluate exactly what you need from your IT monitoring solution to determine which product is best for you.

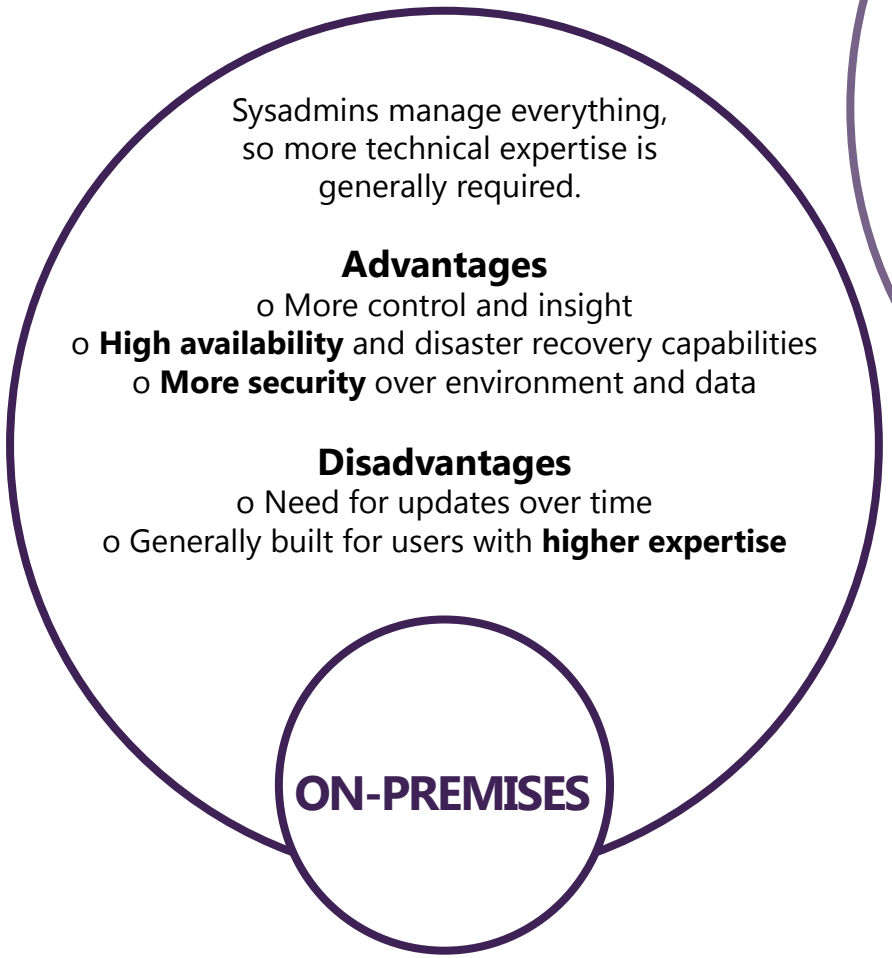
CASE STUDY

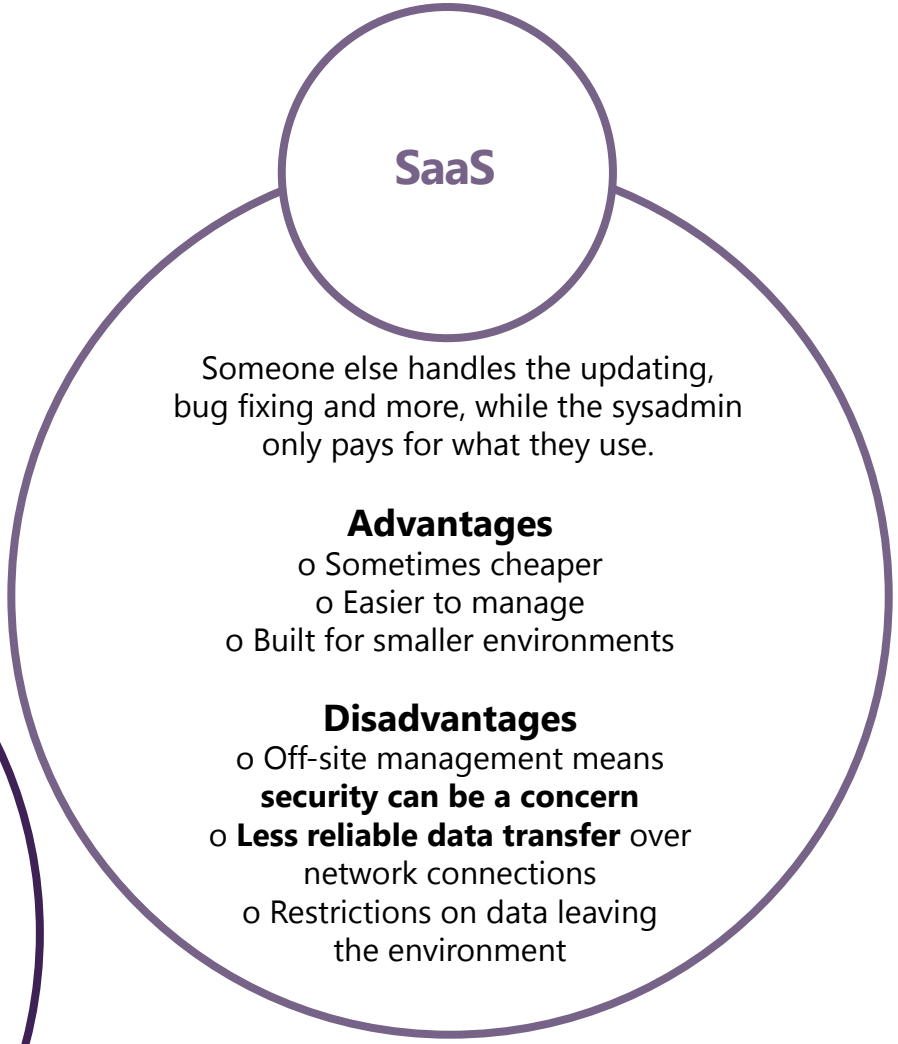
Cornell Keeps Classrooms Connected

Cornell University's students, faculty and staff rely on the school's network for uninterrupted service, so its monitoring solution **must be able to monitor a wide range of devices 24/7**. Desiring the flexibility to support new devices as the school grows and the visibility to track IT across a large campus, Cornell chose Opsview Enterprise for its **extendibility, reliability and deep reporting**.

ON-PREMISES VS. SAAS

The decision between **on-premises and SaaS-based monitoring** comes down to whatever a sysadmin is looking to get out of an IT monitoring tool. Generally, SaaS is best suited for smaller environments and for sysadmins who do not want to be worried about day-to-day management. On-premises is generally for larger environments where security and control are much more of a priority.





A FEW WORDS ON TRANSACTIONAL SYSTEM ADMINISTRATION

Tom Limoncelli, a notable voice in system administration and network engineering, has described the concept of "transactional system administration" as **a model in which sysadmins work in a fairly reactionary, functional manner**. The office sysadmin receives an IT request and then fulfills his end of the "transaction" by completing the request, whether that's adding a new server to the network, setting up a new workstation or resolving a technical problem.

This way of working extends to how networks are managed, sysadmins are hired, and products are purchased and selected. For example, when applying this concept to the IT monitoring buying process, you might simply purchase your solution to fulfill a very rote and basic set of requirements. If you have 20 devices to monitor, you purchase a solution that can handle at least that many. If you have a lot of Windows servers, you purchase something that can monitor those devices.

And so on. Simple, right?

As Limoncelli explains, **this line of thinking is restrictive**. It limits how strategically sysadmins can run their departments, puts more stress on IT to be reactive and immediate, and even limits your earning potential because you're only seen as a functional cog in the wheel – "Mr. Fix It."

Instead, sysadmins should think bigger about how the IT department fits in overarching business strategy. Maybe you only have 20 devices to monitor now, but does the business have growth plans? Will you be adding Linux servers to your Windows environment in the future? Would a solution with automated capabilities free you up to support the business more strategically? Maybe investing in a solution that's "more than you need right now" would be the more economical option long-term.

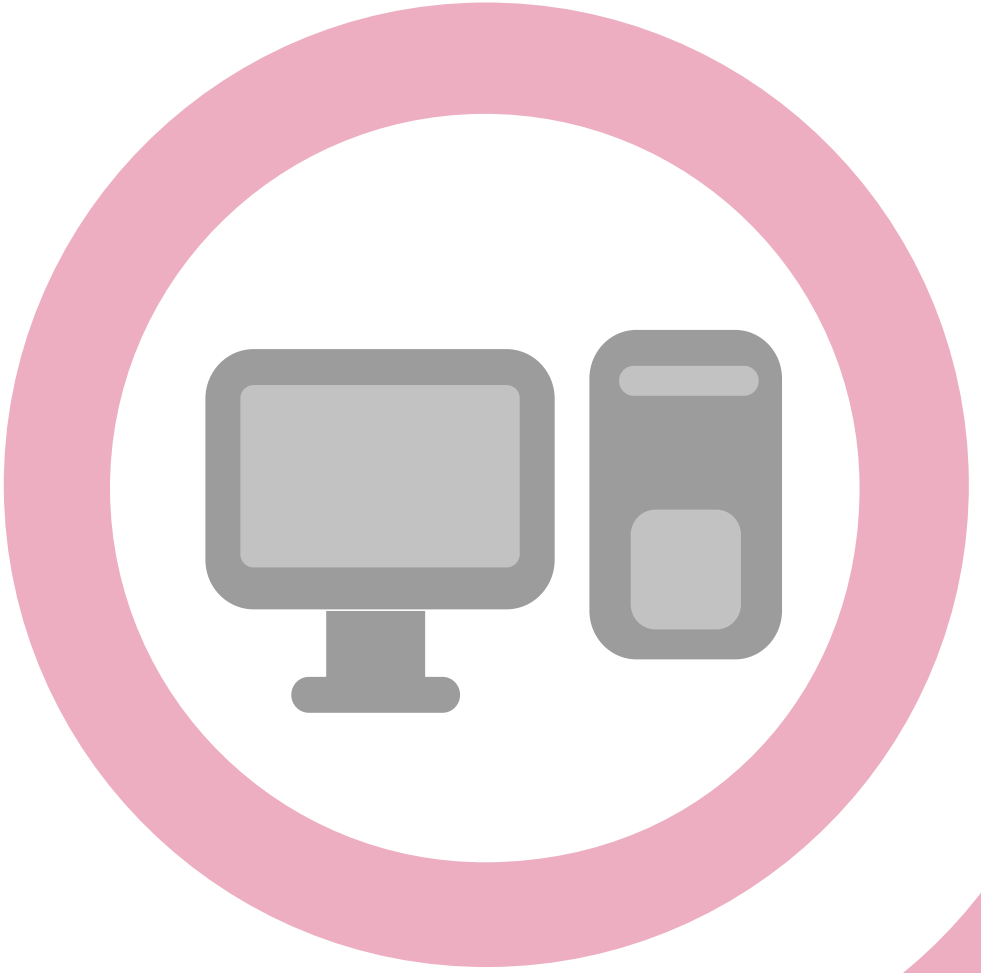
As Limoncelli writes, moving away from transactional system administration is "**better for your company, for you and for your stress level**," because it allows you to focus on what's efficient, automated and sustainable. Incidentally, these are also good qualities to look for in an IT and business service monitoring tool. [4]

HOW MANY DEVICES ARE YOU MONITORING?

How many devices do you need to monitor? It's most likely the number one question you will hear when talking to a sales rep at any monitoring solution company.

However, device count isn't just about knowing where you stand in the pricing tiers. Device count gives you an idea of where you are now, where you might be in the future, as well as showing just how many resources are needed to dedicate to monitoring.

Knowing your device count can offer a cost baseline to guide your purchase, because many smaller and mid-range solutions cap the number of endpoints you can monitor, so it's still the best starting point.



STARTER OR FREEMIUM (UP TO 25 DEVICES)

Free or trial solutions offer a scaled-down version of an enterprise product with some limited features

Pros

o Some basic functionality (auto-discovery, SNMP trap processing, dashboards)

o Easy to upgrade to full product if part of a commercial offering

o Fully developed graphical user interface (GUI) for easy administration

Cons

o Limited to device cap

o Limited technology coverage, lack advanced features like slave server clustering

o Lack business services (reporting, technical support, notifications and alerts)

Best Fit

o Small offices
o Home offices
o Test environments

PROFESSIONAL-GRADE (25 TO 200 DEVICES)

Professional or business-grade solutions are ideal for growing businesses. Solutions in this range offer a full selection of features but cap you off at the number of devices, typically around 200.

Pros

o Headline features (wide technical coverage, automation, SNMP trap processing)

o Business services (full reports and dashboards, notifications and alerts)

o Business Service Monitoring to enable group-based management

Cons

o Require multiple monitoring instances to cover devices beyond cap

o Lack advanced High Availability, network analysis capabilities

o Lack multi-tenancy to enable single-source management of entire IT estate

Best Fit

o Businesses that want enterprise-grade features
o Businesses planning for high growth

ENTERPRISE-GRADE (200 OR MORE DEVICES)

Pros

o High Availability capabilities to assure business continuity

o Scale to monitor an unlimited number of devices

o Fully featured, including advanced network analysis and full technical support

Cons

o Cost can be high, depending on your vendor
o Learning curve can vary depending on sysadmin expertise

Best Fit

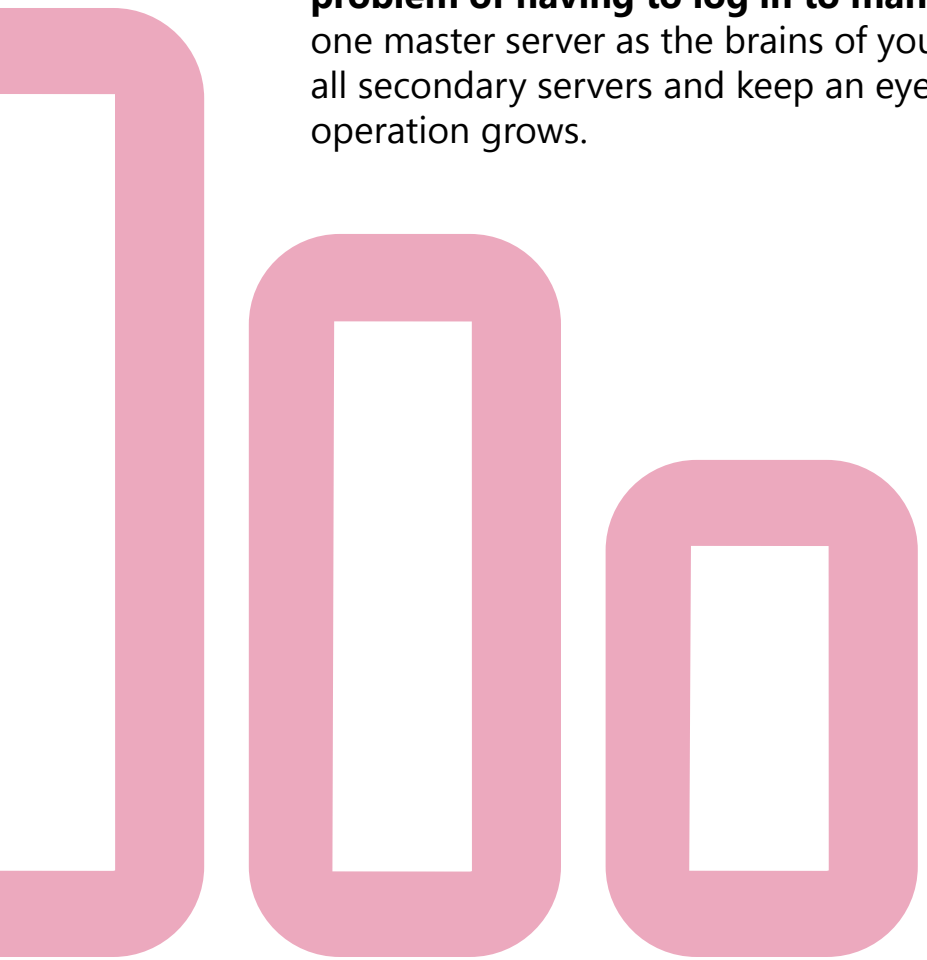
o Large businesses that need to scale

Enterprise IT monitoring solves the scalability problem. These solutions offer unlimited device coverage, central management of an entire network and a full suite of advanced features.

THE SCALABILITY PROBLEM

If you apply a rough rule of thumb, you can conservatively monitor **250 endpoints** from a single monitoring box (you may be able to monitor more, depending on other factors, but 250 is a solid baseline to use). So, when you hit 1,000 devices, you need to have four boxes looking after your estate. That contributes to increased overhead costs for patching, powering and managing all of that equipment.

If you have a single enterprise monitoring tool that can scale, **you don't have the problem of having to log in to manage four separate servers**. Instead, you have one master server as the brains of your monitoring operation, allowing you to control all secondary servers and keep an eye on everything at once, no matter how large your operation grows.



MIT Scales for Better Visibility

CASE STUDY

MIT has a complex infrastructure environment comprising of approximately **2,500 servers across three data centers** in the Boston metropolitan area. The scale of the environment was starting to reach the limits of their self-developed Nagios-based monitoring tool. Switching to Opsview Enterprise gave MIT **enhanced functionality, configurable dashboards and deep reporting**.

WHAT ABOUT DESIGN & USABILITY?

The look and feel of your software – its GUI – impacts user experience. If the product is hard to use and not simple to learn, it could slow down productivity, complicate new sysadmin training and make it harder to scale monitoring capabilities as your business grows. On the other hand, experienced sysadmins might be comfortable with any interface or even prefer to see all the "gears" of their IT monitoring solution as a matter of trust, to know that application inside and out.

A really expensive and ineffective monitoring tool that just happens to look great won't do you much good, so you shouldn't prioritize cosmetics above all. But at the same time, a feature-rich solution that takes forever to learn and administer could hurt much more than it helps. Your final decision here will require a balance between functionality, cost and team experience.

Here are a few questions to ask yourself as you're evaluating the design and usability of IT monitoring.

HOW EXPERIENCED IS MY TEAM?

If you're an expert sysadmin, you can probably work within any GUI. However, you may add less experienced team members later on, or your most talented administrator may leave the company and take all that knowledge right out the door.

CASE STUDY

Cisco was struggling to deploy its existing monitoring solution across its IT estate, and the solution was **hard to administer without in-depth knowledge of the program**. Cisco switched to Opsview Enterprise to monitor its network, encouraged that the program's simple GUI allowed for faster configuration and a shorter learning curve.

Cisco Opts for Ease of Configuration

Know Command Line?

Plenty of open source tools offer attractive interfaces that anyone can read, but depending on the vendor, you may need to know how to work completely within command line to add a new server or service check. Some open source software is a bit easier to configure, but the learning curve remains steeper compared to commercial tools.

Learning Curve

Most commercial solutions allow you to administer entirely within a robust GUI, so the learning curve is shorter. If your best sysadmin leaves the company, a trainee can easily pick up the slack. Plus, if you ever need help, you can call up technical support or access company documentation from a knowledge center or user community.

Flexibility

Depending on your level of experience, you may want to customize your monitoring solution. Open source monitoring is great for sysadmins who want a highly flexible environment to play in, while some commercial vendors include strict proprietary licensing that sometimes makes customization difficult or even impossible.

HOW MUCH TIME DO YOU HAVE FOR ADMINISTRATION?

Most sysadmins would prefer to treat monitoring as a "set it and forget it" IT function, but there will be times when you need to sit down and add a new device or create some service checks. How long do you want these processes to take?

Integrations

Commercial solutions offer out-of-the-box integrations that connect the monitoring function to other parts of your IT estate – like your service desk – for optimized management. Open source software is often even more customizable – perfect for the experienced sysadmin – but it is possible to over-customize your solution for a single user's very specific purposes, which complicates training and scalability.

Features

A user-friendly GUI can dramatically shorten configuration time. Other time-saving features include auto-discovery, which identifies all the devices you need to monitor, and templates, which are pre-defined service checks that enable fast implementation.

Business Services

Certain solutions offer advanced capabilities to save you time. Business Service Monitoring, for example, groups together all the services that serve a particular part of your business for high-level monitoring.

WILL NON-IT USERS SEE THE INTERFACE?

Clean graphics make it easier to visualize your network, especially for management or clients. Easy-to-read dashboards and reports improve the perception of your company, while a confusing or overly technical display could make your business look low-rent or dated.

Function vs. Form

If no one outside the IT department will ever see your monitoring solution, cosmetics will probably matter much less compared to functionality. At the same time, a well-designed monitoring solution could still save you time through ease of use.

High-Level Views

Many monitoring solutions can offer high-level dashboards to visually represent your network for easier problem identification, though the quality and functionality of these dashboards will vary greatly.

Out-of-the-Box Reporting

Many off-the-shelf solutions include reporting out-of-the-box, so you can easily pull up a network status or health report to show your boss whenever asked. Open source solutions can offer reporting, but you may need to do some customization work first.

DO YOU NEED ENCRYPTION?

Encryption is a somewhat new consideration for IT monitoring, but it's one that sysadmins - particularly those in finance and retail, where there are compliance requirements - shouldn't overlook. Cyber attackers will always search for the path of least resistance. Your IT monitoring platform could be the unlocked door leading to the rest of your network.

WHY ENCRYPTION?

Encryption is a fairly unique offering in IT monitoring – most platforms don't put as high an onus on how they store, handle or transport data. This could be a major oversight for sysadmins presiding over highly secure networks, specifically in the verticals of retail, healthcare and finance. For these sysadmins, it's not necessarily emerging threats they should be concerned with, but rather hefty compliance requirements around how they manage and store sensitive information.

The compliance standards these sysadmins follow – as laid out by the Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) – are stringent and constantly evolving, and noncompliance could expose companies to financial penalties and reputation damage.

HOW ENCRYPTION WORKS

When sensitive network data are stored in plain text in the GUI or the database, that information isn't safe. An attacker could break into the network tunnel between the central server and whatever is being monitored – and gain access to your network crown jewels.

By encrypting traffic to and from your central server and the servers and devices you're monitoring, you'll shield the information from attackers. Most importantly, even if an attacker is able to breach one corner of your network, they won't have access to everything.

The highest level of encryption – AES256 – covers all passwords and sensitive data used within the monitored IT estate. This level is so secure that it's used by the U.S. government to encrypt data in files classified as "Top Secret."

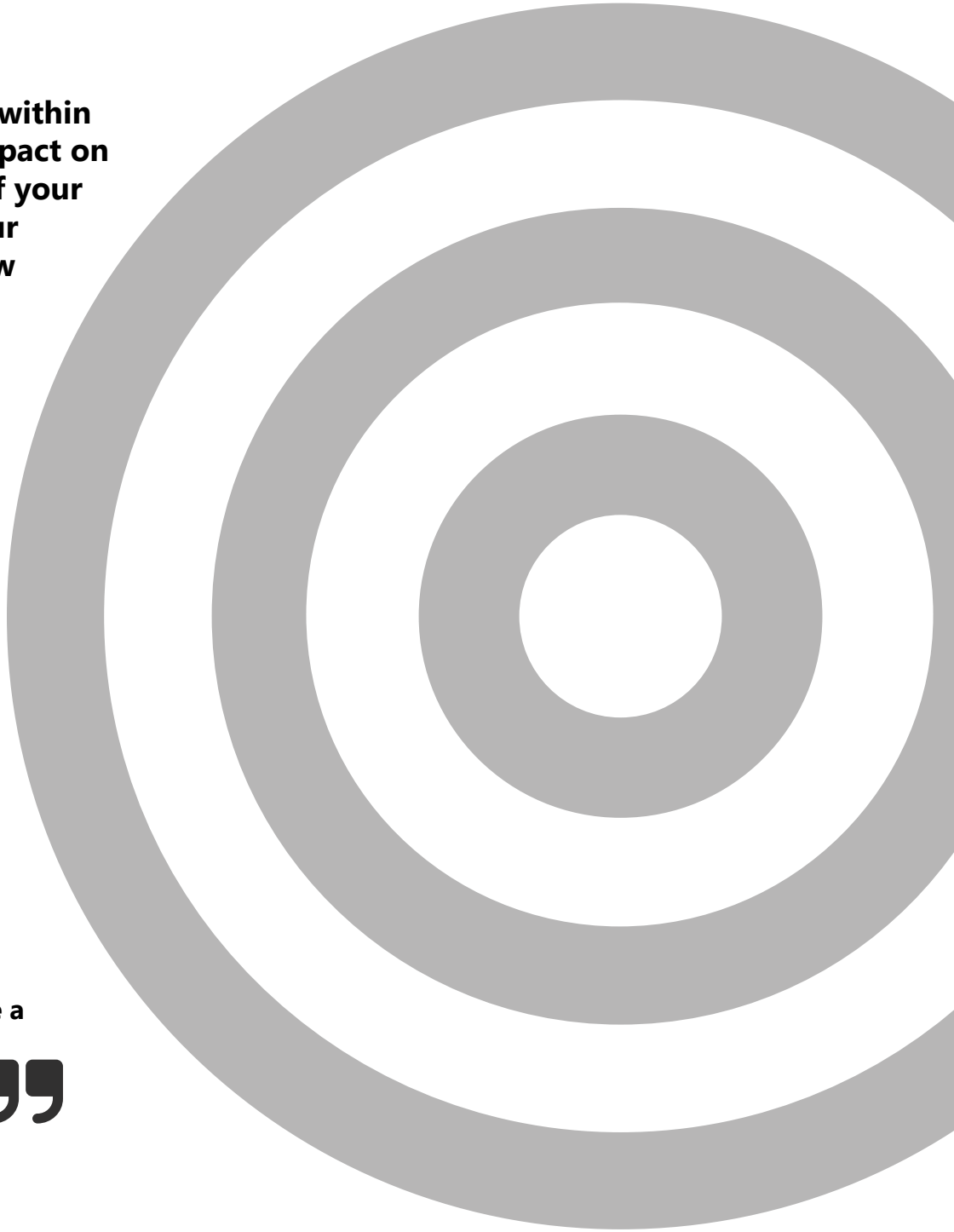
With this degree of protection, sysadmins will be able to encrypt SNMP, database connection and web authentication credentials, as well as attributes – everything that could have previously been vulnerable.

WHAT IS YOUR END GOAL?

What do you need to monitor? The technology within your IT environment might have the biggest impact on your buying decision, and knowing the scope of your IT estate will help you establish the goals of your purchase and determine what problem your new monitoring solution is meant to solve.

Start by describing your current environment – and the challenge of monitoring it – in a one- or two-sentence problem statement. Your statement might look something like this:

> **I have a lot of servers, databases and other equipment in the network, but I do not have a way of monitoring everything at once.**
>
> **I provide a service to my clients, but I currently have no way to know if I've suffered a service interruption unless problems are reported by my clients.**
>
> **I monitor IT infrastructure through the use of a lot of specialized solutions that require a lot of specialists to support.**



FACTORS TO CONSIDER

Preferred Number of Tools
Do you want to have multiple tools to serve specific functions, or would your rather have one that does everything?

Your Architecture
Are you monitoring physical or virtual servers? What operating systems are you running/plan to run?

Technical Competency
Can your team customize anything under the sun? Do you have highly specialized sysadmins with experience with specific operating systems?

Extendibility
Do you plan to scale? It's probably better to have a solution that lets you easily add new devices and integrations.

CASE STUDY

Heartland Unifies Monitoring with One Tool

Heartland Payment Systems found its existing monitoring solution could monitor its Windows-based systems, but struggled to provide adequate coverage for Linux-based systems. Rather than purchase a second tool, Heartland replaced its existing solution with Opsview Enterprise to monitor the entire IT estate with one tool.

THE LAY OF THE LAND

Different types of monitoring solutions address different challenges, and while one form is not necessarily any better than the others, it's good to know how each varies so you can make the right decision for your business.

Niche Monitoring

Some niche vendors focus solely on monitoring a specific technology or product. For example, you may encounter a niche monitoring platform that proclaims to be the very best tool for monitoring VMware. Or, one that offers application performance monitoring, specifically for cloud apps. If your monitoring requirements are highly specific, you might be able to find exactly the right fit among these solutions.

Broad Coverage

Many tools promise broad technology coverage. This can include common IT like Windows- or Linux-based software, or emerging technologies like VMware and Hyper-V. Some solutions do a pretty good job of letting you monitor anything, while some more or less check the box on the most popular technologies.

Customizable Solutions

Open source, by nature, is completely customizable, generally allowing you to monitor any new or previously unheard of technology if you have the expertise to do so. At the same time, plenty of commercial offerings are extendable, although flexibility depends greatly on the vendor you choose.

APPLICATION VS. INFRASTRUCTURE

Keep in mind the distinction between **application performance monitoring** – which involves the monitoring of specific apps – and **IT infrastructure monitoring**, which involves the monitoring of the resources and systems – both hardware and software – that support applications.

APPLICATION PERFORMANCE MONITORING

Goal	Popular Solution Examples
Monitoring application resource utilization	New Relic®, AppDynamics®, CA® Application Performance Management, Riverbed®, Compuware®, Dynatrace®, Boundary®
Monitoring app user experience factors	New Relic®, AppDynamics®, CA® Application Performance Management, Riverbed®, Compuware®, Dynatrace®, Boundary®
Mobile application monitoring	New Relic®, Perfecto Mobile™, HP® Mobile Apps, Compuware®, Riverbed®, Dynatrace®, Boundary®

IT INFRASTRUCTURE MONITORING

Goal	Popular Solution Examples
IT infrastructure modeling	Opsview, Nagios®, Zenoss™, Zabbix®, PRTG®, Solarwinds®, CA Spectrum®, Pingdom®, GroundWork™ CA® UIM (Nimsoft)
Monitoring network data transfer	Opsview, Zabbix®, PRTG®, Solarwinds®, Nagios®, Plixer™
Network capacity planning	Opsview, Zabbix®, PRTG®, Solarwinds®, Zenoss™, Nagios®

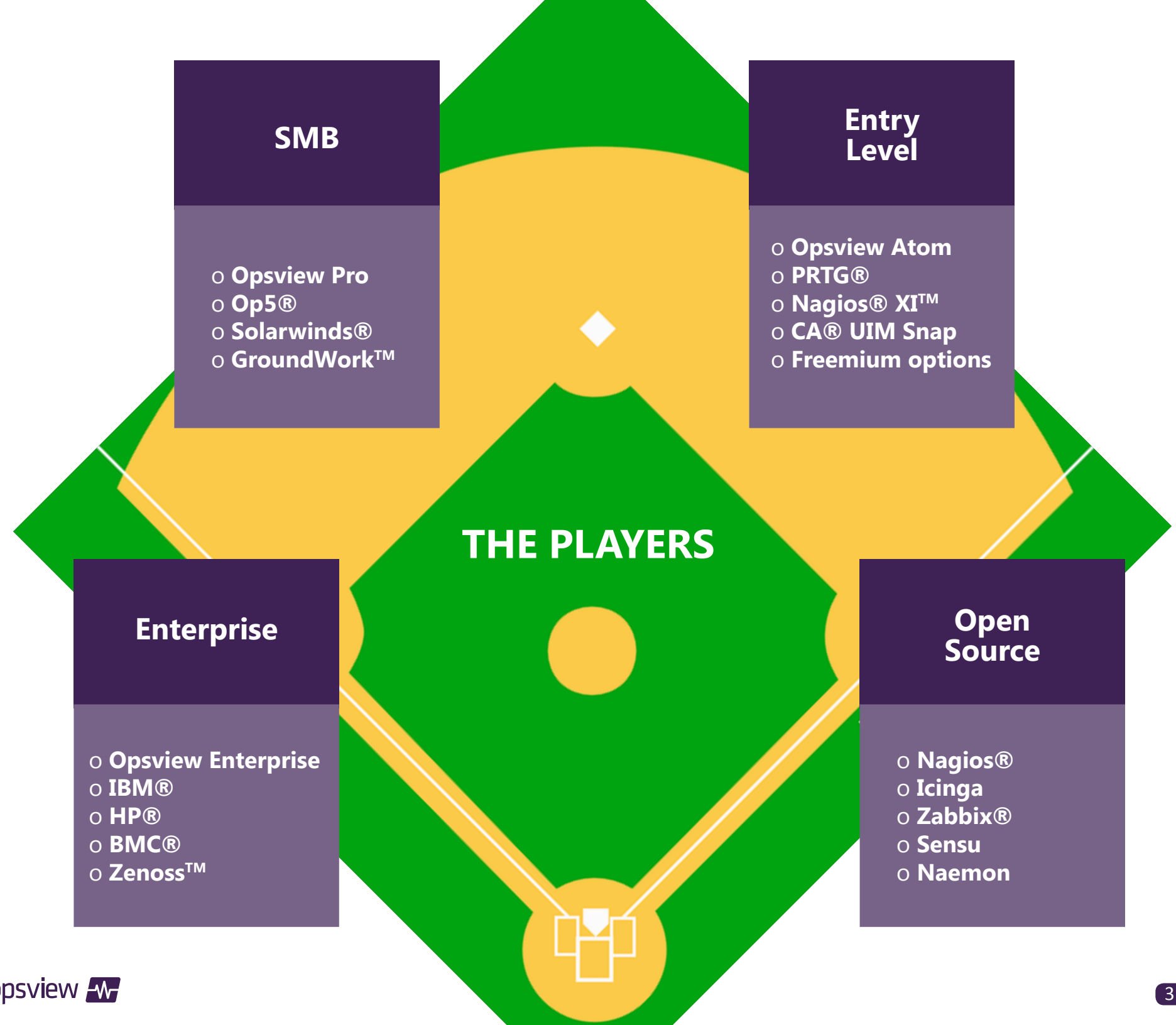
IN SEARCH OF AN ANSWER

If you're in the market for IT monitoring, you have a lot to think about. Many tools might check the box in terms of capabilities, but as the IT department becomes increasingly aligned with overall business objectives, sysadmins have more to consider with each new IT investment.

As a result, you need to ask yourself how the purchase of your next IT monitoring solution will:

- **Address current deficiencies and gaps**
- **Affect IT hiring and training**
- **Fit in your budget**
- **Free your time for other important tasks**
- **Impact future IT investments**
- **Improve network visibility and administration**
- **Be secure and safe to use**
- **Plug into your current infrastructure**
- **Support overall business growth plans**

Finding a tool that satisfies most or all of your requirements is a matter of establishing a goal ahead of time and evaluating how each solution helps you meet it. There's an ideal IT monitoring solution out there for you – now you need to find it.


SMB
o Opsview Pro
o Op5®
o Solarwinds®
o GroundWork™
Entry Level
o Opsview Atom
o PRTG®
o Nagios® XI™
o CA® UIM Snap
o Freemium options
THE PLAYERS
Enterprise
o Opsview Enterprise
o IBM®
o HP®
o BMC®
o Zenoss™
Open Source
o Nagios®
o Icinga
o Zabbix®
o Sensu
o Naemon

- How Opsview Sizes Up -

Opsview is on a mission to simplify IT monitoring. Our solutions help you find IT problems within your infrastructure before they become a problem, allowing you to embrace a more proactive and strategic IT management approach.

Though we're a commercial solution, our roots are in open source, which means we're highly flexible, easy to configure and highly extendable. We also include all of the powerful features and integrations you expect from enterprise-grade monitoring. Our top features include:

Ease of Configuration and Use

o Advanced auto-discovery and integrated GUI
o Drag-and-drop dashboards
o Platform scales with your IT estate

Advanced Features

o Out-of-the-box support for most common applications
o Super-fast auto-discovery
o 3,500+ community plug-ins available

Cost

o Enterprise levels of service, features and support
o All at a manageable cost, compared to competitors

Visibility

o Customizable dashboards configured how you want
o Upload your own images and overlay performance labels

Centralized Monitoring for Anything

o Monitoring no matter size of estate or mix of technologies
o Easy organization of monitoring, however you want

www.opsview.com
info@opsview.com

DOWNLOAD A FREE TRIAL TODAY

EMEA Sales
+44 (0)118 324 2100

North American Sales
+1 866 662 4160

1 "Deloitte CIO Survey 2014 CIOs: At the Tech-junction" Deloitte, 2014
2 "Coverity Scan Report Finds Open Source Software Quality Outpaces Proprietary Code for the First Time" Coverity, 2014
3 "Open Source vs Proprietary Software: There is No Clear Winner" Virginia Backaitis, CMSWire, July 17, 2013
4 "'How many sysadmins?' redux." Tom Limoncelli, Usenix LISA list, Feb 9 2015

opsview