

---

# Justifying a System Monitoring Solution

A White Paper



## Abstract

---

Justifying the purchase and implementation of a system monitoring solution can be difficult, since IT department software purchases are faced with more scrutiny than ever in today's extremely competitive marketplace.

IT Managers and CIOs are asked – or forced – to cut costs wherever possible and requests for new software investments require clear justification and evidence for an immediate return on investment.

The purpose of this document is to explain why an economical monitoring solution such as EventSentry© makes business sense by reducing downtime, helping with software license evaluation, saving valuable IT staff time and much more. Downtime means money lost,<sup>1</sup> and implementing a pro-active monitoring solution provides the necessary foundation to streamline and optimize your IT infrastructure.

Further we will illustrate how server downtime affects your organization and we will provide a model for estimating the cost of downtime. We will show how a system monitoring solution like EventSentry© can recover this cost by preventing disruptive and expensive downtime scenarios – whether hardware or software related.

**The prevention of a single failure incident is likely to recover the entire cost of the software package.**

---

<sup>1</sup> <http://www.datacenterdynamics.com/critical-environment/one-minute-of-data-center-downtime-costs-us7900-on-average/83956.fullarticle>

## Key Return on Investment (ROI) Benefits

---

Most NETIKUS.NET customers achieve a 100% return on their EventSentry© investment within just a few months, if not sooner. Once deployed, EventSentry© immediately becomes an invaluable tool in your IT department that benefits the entire organization.

EventSentry© significantly reduces critical downtime, saves money, prevents business disruption, and decreases customer dissatisfaction in the following ways:

- Increases IT personnel productivity by consolidating and aggregating critical logs from a variety of sources, thus significantly reducing the time spent on log management.
- Reduces IT trouble tickets by identifying problems before they escalate. This translates into more satisfied customers, internal as well as external, and reduces unnecessary downtime and frustration ([more](#)).
- Produces critical trending reports that project potential problems far in advance, giving the IT staff the opportunity to take preventative action early ([more](#)).
- Satisfies important compliance requirements such as PCI, SOX, HIPPA, GLBA, and more, and generates reports that help with auditors, so that your organization can save time on audits and avoid costly fines ([more](#)).
- Improves security by monitoring and alerting on critical security events as well as tracking security-related system activity.
- Provides a single viewpoint into various aspects network activity, ranging from raw events to software & hardware inventory.
- Interprets and correlates raw Windows™ security events in real-time and provides easy to understand security and compliance reporting.

## Analogy: Driving a Car without a Dashboard

Managing a Windows network without pro-actively monitoring essential system components such as the event logs, services, disk space and performance is similar to electing to buy a car without a dashboard, just to save a few dollars.

Without a dashboard you would drive without being able to see the current speed or the fill level of your gas tank. Of course you would also miss any service or problem indicators, such as engine problems or low oil status. Quantifying the risk and cost associated with the lack of information is pretty straightforward.

The table below shows some the risks associated when driving a car without a dashboard; some of the recovery cost is of course not accurate (it is impossible to assess the cost of an accident before it happens) and is only provided to illustrate our point.

| Missing Indicator | Potential Risk        | Risk Recovery   | Recovery Cost |
|-------------------|-----------------------|-----------------|---------------|
| Speedometer       | Exceeding speed limit | Speeding Ticket | \$100         |
| Speedometer       | Exceeding speed limit | Accident        | \$7000        |
|                   |                       |                 |               |
| Ice Warning       | Skidding              | Accident        | \$2500        |
|                   |                       |                 |               |
| Fuel Gauge        | Run out of fuel       | Gas Delivery    | \$100         |
|                   |                       |                 |               |
| Engine Problem    | Engine Damage         | Repair          | \$5000        |

**Table 1**

When looking at table 1, you can easily see that a single accident while speeding or driving in winter can cost as much as five times the amount a dashboard would have cost. This table of course assumes material cost only without injuries, and does not take downtime into account when the car gets repaired or when you have to wait for gas delivery because you forgot to manually check the fuel level.

With this example, one can quickly see how initial cost savings often translates into much larger costs, even with a device as simple as a car. Networking and server infrastructures are significantly more complex and much more prone to glitches and failures than a modern car is.

## Supporting a Lean IT Staff

---

With the reduction or freezing in IT hiring and the difficulty of finding IT talent, ensuring an efficient, economical and smooth IT operation has become an absolute. The key to running a lean team, while still providing exceptional service to your customers, is actionable real-time information.

A monitoring solution like EventSentry© is designed to assist your IT staff by providing them with all the relevant information they need to do their job as efficiently as possible, whether those are real-time alerts or historical usage information.

- Without the information that a hard disk in a servers' redundant disk array just failed, the SysAdmin cannot call the hardware supplier and order a replacement disk in time.
- Without performance history, a SysAdmin cannot gauge the hardware resources being utilized by a particular server and its applications. A bottleneck down the road is inevitable.
- Without knowing that a particular CPU or process is consuming all available CPU time, a SysAdmin cannot immediately investigate and resolve the problem. Instead, users will lose productivity and, eventually, complain to the IT team.
- Without the information that your database server is logging several run-time errors to the event log, a subsequent problem might not be fixed in time and/or troubleshooting will take significantly longer.
- Without the information that a critical service wasn't restarted after a patch installation during non-business hours, the SysAdmin cannot connect remotely and fix the problem before users utilize the service again the next day.
- Without historical disk trend information, a SysAdmin has no efficient way of knowing when a particular disk will be full, resulting in costly efforts when no available space is left.
- Without extensive interpretation and correlation of security events, the IT staff will be unable utilize critical security information available in security event logs.

## Quantifying License Cost

---

Even though EventSentry® licenses are calculated on a per-server basis, the cost for a business to implement EventSentry® is better measured on a per-user basis.

Consider this example: ACME Inc. has 30 production Windows servers that are serving business applications to 600 employees. If one or more services running on these servers were to become unavailable for 30 minutes, a certain number of users – let us assume 100 – would be affected by this downtime.

Whenever a server or application fails, we need to keep in mind that it's not only the users of the service who are negatively affected, but other business applications that depend on or interact with the failed application.

So even if only 20 users were directly accessing the problematic server in our scenario, users affected by an outage will also negatively influence other users that depend on them.

For a problem that could have been prevented with a system monitoring solution like EventSentry®, the total license cost for this particular incident might as well be divided by 100 users, and not 30 servers.

Currently, a 30-host license of EventSentry® costs USD 1968, which amounts to USD 65.60 per server. However, it would have **only cost USD 19.68 per user** to avoid this incident.

The question is simple – would you pay USD 1968 – or USD 19.68 per user - to keep 100 users working for 30 minutes? When thinking about the answer and calculating the average hourly pay rate of your employees, also consider the impact your (temporarily unavailable) business applications have on customer service, employee satisfaction associated recovery cost.

So for ACME Inc., dividing the license cost of USD 1968 by the total number of employees would end up costing **\$3.28** per user.

## Information in Real-Time

---

Real-time monitoring is a crucial feature for any server monitoring suite that many centrally based agent-less solutions do not provide. EventSentry© has been designed from day one to monitor all critical system components in real-time with as little resource consumption as possible.

By using sophisticated agents, EventSentry© intercepts system problems immediately when they occur, and forwards alerts to the appropriate recipients in real-time, whether that may be an email recipient, SNMP monitoring station, or a custom recovery process (e.g. VBScript, Perl, etc.).

The EventSentry© agents are developed in C++ and do not rely on the .NET Framework or any other software components. This ensures that the agent will use the least amount of resources on the host system without interfering with the Operating System and its business applications. The small agents are easily deployed from the multi-threaded management console.

## Low Bandwidth WANs Environments

---

Even with decreasing bandwidth costs and affordable VPN solutions that can utilize affordable Internet connections such as DSL, managing bandwidth wisely is still a priority for many organizations. After all, the last thing you want to do is use 25% or more of your bandwidth to support your monitoring infrastructure.

With its agent-based design, EventSentry© works well in all environments with limited bandwidth<sup>2</sup>. Since all the monitoring logic is performed directly at the host with the EventSentry© agent, only relevant information is transferred across the WAN. Additionally, most monitoring aspects of EventSentry© are highly configurable and can be optimized to reduce bandwidth consumption.

## 3<sup>rd</sup> Party Integration

---

With 16 different notification types<sup>3</sup>, EventSentry© integrates seamlessly with a wide variety of 3<sup>rd</sup> party software, including ticketing, chat and GSM notification systems.

Event data is easily submitted to 3<sup>rd</sup> party systems either through HTTP(S), custom applications or customized emails.

---

<sup>2</sup> <http://www.eventsentry.com/kb/80>

<sup>3</sup> <http://www.eventsentry.com/features/notifications>

## Conclusion

---

When considering any system software purchase, it is important to analyze what existing problems the software is going to solve and/or which processes it can improve. Dismissing new system software purchases without taking the resulting cost savings into consideration can be a bad business decision.

Many software products, including monitoring solutions and virtualization software, will often bring a ROI in a short time.

Monitoring solutions such as EventSentry©, which integrate several monitoring capabilities into one product, are preferred over separate island solutions which require more maintenance and usually result in a higher price tag.

By providing your IT professionals with both real-time and historical information, you can eliminate the time-consuming manual labor processes and reallocate staff resources more wisely.

## About NETIKUS.NET Ltd

---

NETIKUS.NET Ltd is a customer-oriented growing software company that has been developing system software to monitor, support and optimize IT infrastructure since 2002. NETIKUS.NET Ltd develops the award-winning server and workstation monitoring solution EventSentry© and several freeware applications as well as operates two IT community sites.

EventSentry© has won several awards since its first release in 2002, and has been reviewed up in several print and online articles.

NETIKUS.NET Ltd clients also include end-users, consultants, small businesses, government & military institutions, universities and large Fortune 500 companies<sup>4</sup>.

All NETIKUS.NET Ltd software is developed and supported in the United States.

---

<sup>4</sup> <http://www.eventsentry.com/about/our-customers>



## ROI Quantification Details

---

Referenced by "[EventSentry Return on Investment](#)":

1. Systems downtime can be quantified by multiplying the average pay rate of all affected users by the duration of the downtime and adding any potentially lost revenue (i.e. credit card processing server, email exchange server, website downtime). Also see "[Quantifying License Cost](#)".
2. Reducing trouble tickets can be quantified by multiplying the estimated reduction of trouble tickets by the average ticket time and the IT personnel pay rate.
3. Increased efficiency can be quantified by multiplying the estimated increase in production by the IT personnel pay rate.
4. Unsatisfactory compliance requirements can be quantified by multiplying an IT personnel's pay rate by the time it takes to spend with auditors due to insufficient reporting. This can also be quantified by fines or higher credit card fees incurred for non-compliance.

NETIKUS.NET Ltd believes that all information in this document is accurate and is not responsible for errors. All information contained in this document is subject to change without notice.

All calculations and example scenarios provided in this document are for illustration purposes only and do neither imply nor suggest results for any organization or company.

EventSentry is a registered trademark of NETIKUS.NET Ltd. All other trademarks are property of their respective owners.

Copyright 2008-2015 NETIKUS.NET Ltd. All rights reserved.