# Essential IT Monitoring: Top Five Priorities for Network Security

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SolarWinds

April 2016

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

## Table of Contents

# Essential IT Monitoring:
# Top Five Priorities for Network Security

## Essential Security

Comprehensive visibility into all essential technology configurations, performances, changes, and status is fundamental to achieving effective enterprise IT security management. To create a consolidated view, these monitoring practices cross multiple management disciplines. With each organization comes a different set of requirements that drive which tools are accepted. In many organizations, the security budget is either assigned as a portion of the other operations' budgets or, in the worst cases, is not apportioned or assigned, but must be carved out of other budgets. Thus, other operations teams see security as a budget drain. Therefore, to acquire funding to meet its own requirements, security must identify tools that meet both security and operational requirements, creating champions from within other IT groups. To do this, security must identify tools that meet not only its own needs but can also fulfil other operations requirements. By meeting the broader needs, security helps the business to help itself and creates valuable alliances within the other disciplines with the tools that align most appropriately. Therefore, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts recommend the adoption of management solutions that are modular and fully integrated, allowing each organization to select the most appropriate combination of administrative capabilities to establish a complete view of its distinctive support stack from a "single pane of glass."

EMA's series of Essential IT Monitoring white papers identifies core elements that enterprises of all sizes must target in particular management disciplines in order to rapidly identify and resolve issues to optimize performance across IT infrastructures. Readers are advised to adopt integrated, automated monitoring solutions that bring visibility to all the identified elements in the topic areas most applicable to their IT implementation.

## Top Five Priorities for Network Security

*Given that there is no perfect security, and any control may fail at any time, leaving assets open to some sort of harm, security professionals must keep several paradigms in mind.*

Most security programs start with the goals of Confidentiality, Integrity, and Availability, the famous CIA triad of information security. However, as appealing as these goals are, real-world practitioners know they are just that – goals. The day-to-day business of information security is not about the high-level goals; information security is about all of the individual steps taken to achieve those goals. This is done programmatically recognizing that systems, which are composed of hardware, software, storage, and network components, will not be perfectly secure. Security professionals are charged with delivering as close to perfect security as is achievable in the face of a continually changing threat-scape, limited budgets, and business operations demands. Information security is the business of risk management and just like buying insurance, security spending is often buying insurance. It is purchased hoping that the effects of an incident will never be incurred. Without infinite resources, security professionals must prioritize their efforts and play the odds. Given that there is no perfect security and any control may fail at any time, leaving assets open to some sort of harm, security professionals must keep several paradigms in mind:

1. Decide which risks have the highest combination of probability of occurrence and loss, and address those first.
2. Do not spend more on implementing and maintaining the control than the perceived value of the protected asset.
3. In the case of cyber-attacks or malicious activity, the job of the security organization is to make it take longer for a control to fail than the information will be valuable OR make it take more resources to overcome the control than the perceived value of the asset.

If the security professional accomplishes any of these three paradigms, the attacker will go elsewhere and the business wins.


Networks are indispensable in today's business environment; unfortunately, attackers know this all too well and are ready to take advantage of them. Defending corporate data begins with strong protections starting with the network that shield the systems. For security professionals, awareness and prevention are the first lines of defense; however, visibility provided by ongoing monitoring creates the foundation for delivering appropriate and timely detection and response, which are the keys to a successful program.

The principle here is simple – given enough time and skill, all prevention-based controls are susceptible to failure. To maintain a margin of safety, security programs backstop prevention technologies, like firewalls and antivirus, with monitoring systems that report on the efficacy of those controls, the resiliency of the system, and any threats and vulnerabilities that will jeopardize the systems.

Standard IT monitoring is focused on performance and reliability. Reliability is the accidental failure of one or more parts of a system that causes an impact on performance and/or harm to IT assets. Security monitoring adds another dimension to standard IT monitoring. It is focused on the intentional failure of the same components. There are two factors in security monitoring that make it a particularly advanced challenge for the practitioner: first, ongoing triage of new vulnerabilities and second, the need to correlate seemingly unrelated events to identify multi-stage reconnaissance and attacks by intelligent and/or persistent adversaries. To meet these challenges, security tools must be attuned to the monitored environment.

For any solid security program to deal with the continually changing threat-scape, it must implement a layered defense, also known as defense-in-depth, which deploys interlocking or overlapping controls to maintain the security of the environment. The best analogy is that of a brick wall. The foundation must be laid before the wall can be built. For a security program, that foundation would be traits like policy, awareness and training. Without these as a foundation, solid controls cannot be successfully implemented. Each layer of the wall is made up of multiple bricks overlapping other bricks. Staggering the bricks is the key factor in the wall's structural strength. The same is true of a security program. There are elements of each control that strengthen the others, so if one fails there is feedback of the failure, but another compensating control will continue to be enforced to maintain the overall security integrity. The mortar that holds it all together is the middleware: the monitoring, reporting, processes, and procedures used to make the program integrated and operational. The ultimate goal would be to have all of these controls reporting to and from the same data repository.

In this paper, EMA is focused on network security. EMA found that these five components are consistently at the core of network security and key to getting the job done right. Please note that the five topics are listed in no particular order; they are heavily dependent upon each other to create a successful program.

1. ***Identity and access management*** – Provide structure and reporting for authentication services for personnel and systems throughout the enterprise.
2. ***Vulnerability management*** – Identify and address vulnerabilities across all enterprise systems and applications.
3. ***Change monitoring*** – Identify changes, both authorized and unauthorized, to your infrastructure and who performed them.
4. ***Correlated, centralized event management and analysis*** – Maintain continuous monitoring for anomalous, unusual, noncompliant, and malicious activities with a centralized repository for collecting and displaying all recorded events with out-of-the-box and user customizable intelligence and reporting.
5. ***Incident response*** – Regularly updated and tested conglomeration of documented manual and automated response processes and procedures available to the security personnel.

## Priority 1: Identity and Access Management (IAM)

Understanding the proper context for IAM starts with understanding how identity is established in not only a single system, but throughout the environment. Something or someone that requests authorization to access a system is called a user. These can be people, other systems, or applications. To gain access, the external entity needs a token, such as a user or account id, to identify itself to the target system and an authenticator, such as a password, to validate that the request is coming from the owner of the credential. Once on the target system, the user id is considered a principal. The principal makes requests in the system on behalf of the user. The requests are known as subjects. Subjects interact with the object/resources on the system to achieve the users' objectives. Subjects may also make additional calls to generate other subjects for this same purpose.

Identity management prepares the userid for use in the system. These types of systems perform account registration, provisioning, propagation, profile updates, password resets, group/role membership, separation of duties, and de-provisioning. The majority of identity-related tasks are tracked as part of compliance regulations and audit best practices so visibility into identity provisioning is a key requirement for network security engineers.

Access management systems are concerned with receiving identity and authentication credentials and enforcing authorization decisions based upon the credentials presented. The access management systems report on the identity using the system and what they are doing. Access management systems make for excellent security checkpoints. By design, they should not be able to be bypassed. Moreover, all the decisions that access management systems make, whether access is granted or denied, are by definition interesting security events.

Since a user is not limited to being a person, knowing exactly who or what an identifier represents is imperative. When new personnel arrive, they have to have an ID to access the network and its associated resources. Administrators and security personnel agree that leaving the default accounts in operating systems and applications enabled is an unwarranted risk. We need to follow the same paradigm with systems that attach to our networks. In many environments, DHCP is enabled so that any new computing device that attaches to the network, wired or wireless, is given an IP address to begin operation. This is giving those systems a guest account on the network. We need to track activities of systems as well as people. Managing user identities and access within the enterprise ecosystem is crucial.

Organizations of all sizes suffer from user "access creep." As users change positions (roles) within the business, administrators often just bolt on their new access privileges without regard for the old. Generally, when this is done it is a function of administration work overload. Characteristics of new systems introduced to the environment must be considered to determine proper authorization and access. Being able to identify inappropriate "user" activities is impossible without proper Identity and Access Management (IAM). A solid IAM provides the capacity to associate all activities within the environment with a specific user and report on those activities on a level appropriate to the individual requesting the report, from very macro levels for business leaders, to very granular levels for administrators and security.

Access logging is not strictly a passive exercise. Access logs allow the security team to respond to security and availability events either manually or, in some cases, with automated response. Actions here may include modification of access privileges, whitelisting or blacklisting usage of sites, servers, or protocols, or blocking users based on policy or usage patterns.

## Priority 2: Vulnerability Management

The goal of vulnerability management is simple – find the weak spots and remediate them, or at least mitigate their risks as much as possible, before the attackers exploit them. Security personnel are responsible for finding all of the vulnerabilities (attack vectors) in their environment to maintain security. Attackers only have to find one vulnerability to exploit. In its most basic implementation, a vulnerability management program is centered on regularly scanning environments to look for unpatched systems and then deploying patches as they are released by vendors. A mature program includes other activities such as penetration testing, and regularly reviewing security controls, systems, and configurations for excessively permissive, inaccurate, or outdated rules. The latter activities are applicable to vulnerability management because if the attackers can't get to it, they can't exploit it. These activities are generally performed in organizations where compliance to some regulation or standard is required but not done regularly in organizations where there is no compliance driver. The findings should be reported and communicated to a central management system for triage and remediation.

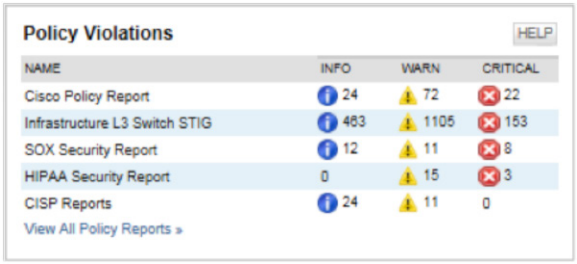
The goal of vulnerability management sounds simple, but achieving the goal in a complex enterprise environment can become complicated. Scanning systems is generally the easy part of the equation. Several challenges follow:

- Filtering out false positives before passing vulnerabilities on to administrators
- Determining remediation priority based upon the environment
  - A vulnerability ranked as critical on a limited access system does not generally need attention as quickly as a vulnerability ranked as high on a public-facing system.
- Coordinating a deployment window on the key systems
  - Most systems are not an issue; however, getting permission to patch a legacy system running a critical application or a high volume transaction system can be very difficult.

Vulnerability management falls under the purview of many audit requirements, so reporting and dashboards for vulnerability lifecycle are critical. Ongoing, end-to-end vulnerability management is a highly distributed process, but the management is best handled and reported on from a centralized console.

Security is very often perceived externally as a reactive function. However, vulnerability management is one area where security teams can be proactive, not just reactive. Vulnerability scans, triage, and remediation can and must be done on a regular, ongoing basis, and together these activities give the security team a chance to stay ahead of the threats.

## Priority 3: Change Monitoring




The core functions of change management such as review, approval, and scheduling are more readily addressed in a systems management white paper of this series called "Essential IT Monitoring: Ten Priorities for Systems Management." However, the critical aspects applicable to security revolve around identifying the fact that a change was made. Was the change authorized? Did it violate existing security policies including compliance requirements? Did it reduce the overall organizational security posture? Additionally, it is important to know who made the change and when, so accountability can be assigned with a timestamp to determine if it aligned with other invasive or possibly hostile activities. Most attacks involve some sort of privilege escalation in order to accomplish the end goal of systems compromise. The sequence of change can often tell the security analyst or investigator the intent of the instigator. Identifying which configuration files or account permissions change is fundamental to a forensic investigation and remediation plan.

## Priority 4: Correlated, Centralized Event Management and Analysis

Maintaining visibility to activities within your scope of control or management is crucial. Every application on every system in an environment has the capability of sending operating and audit log data concerning its users, interactions, and health. That is just the beginning. When other control systems such as firewalls, intrusion sensors, mobile security, data management, etc. are added in, the burgeoning data swell creates three problems for the security practitioner:

1. Centralized event capture for complete visibility. Even in most small to medium business (SMB) environments, the sheer volume of information coming in is tremendous and humanly unmanageable. Due to greater levels of interaction as the organization increases in size, the data collection expansion is non-linear and becomes significantly greater in midmarket and enterprise level IT and security groups.
2. Correlation of events allows organizations to gain a complete picture of activities in the environment, making them better at addressing common and directly related issues.
3. Security Analysis of alerts to identify advanced threats. To identify and stop advanced threats, it is not sufficient to just collect and correlate events to use them for reactive investigation. Security and IT operations need advanced analysis capabilities to isolate and respond to today's advanced threats.

*Having numerous point solutions to deliver the various logs is better than nothing, but lacks the ability to gain a full context view providing real event correlation. Getting all events managed through a single user interface is a key operations requirement.*

Having numerous point solutions to deliver the various logs is better than nothing, but lacks the ability to gain the full context necessary to provide solid event correlation or security analysis. Managing all events through a single user interface is a key operational requirement. It is not possible to gain proper operational or security management of an environment of any significant size without a single pane of glass management tool. Security Incident and Event Management (SIEM) tools are one of the means to gather the data centrally and should be considered as a first step to achieve the single pane of glass operations requirement. Analysis systems need data to do their jobs and many of them rely on SIEM to aggregate, deduplicate, and normalize data feeds before analysis can take place.


Once all information is presented into the "single pane of glass," both security's and operation's ability to respond increases significantly. Having everything in one place only helps if events can be filtered out based upon priority, event context, or job function. In the most basic context (job function), security administrators do not focus on application performance, network administrators do not focus on storage alerts, and application administrators do not focus on web content filtering. However, during a major or chronic event, any or all of those groups may want to pull into context any of the other organization's alerts to understand how those alerts are affecting the situation. An example of that is when the application personnel get a call that their application is slow and, not seeing anything in the application logs, incorporate the network performance events to see if they are being affected by a network event.

At its roots, threat management is about identifying the threats relevant to the environment before they can be exercised against vulnerability, thereby reducing the window of opportunity it has to act on assets. A common example is that of a lake being held back by a dam. Below the dam is a town. The lake represents a threat. It is not a problem so long as it has no vulnerability to exploit. If the dam develops a crack, that is a vulnerability. If it is not addressed in a timely manner, the lake will begin to exploit that vulnerability until it is repaired or fails. If it fails, the town, representing one or more assets, will be damaged.

Correlation takes into account the fact that many threats and their associated attacks are not identified by a single event but through multiple events. To realize there is an issue, the collection system must evaluate numerous events and tie them together to identify the more complex attack vectors. To do this, the system has to have an intelligence engine behind it that has signature-based analytics and/or anomaly- and pattern-based analytics. The difference between a signature and a pattern is that a signature is a defined sequence of network packet data in a protocol stream that is matched using some form of Boolean logic with regular expressions. A pattern is made up of multiple events created at multiple layers of the OSI model, generally 3–7, that are identified by an analytics engine rather than a packet sniffer. The patterns are more difficult to identify since they can be strung together from multiple sources and data types.

Correlation and analysis are significantly different. Correlation is the grouping of alerts based upon a policy or rule set created from known patterns or events to show operators their relationship and, often times, invoke a reaction. The correlation works only on presented data working on known or previously identified issues (identification may be done by the technology creator or consumer).

In security analysis, the system does not rely on predetermined rules or policies to identify events or activities that are not standard for the environment. Using advanced algorithms, the analysis engine is able to extract information that is indicative of a security incident or that suggests a security incident will occur.

Most advanced security analysis today is based on machine learning. Security analysis is broken out into three areas:

1. User behavioral analysis (UBA) – Identifies user activities that are different than either the user behaved in the past and/or how the user is behaving differently than others performing the same role(s).
2. Anomaly detection – Similar in concept to UBA but is not focused on user activities. It analyzes events and outcomes that are out of the norm for the environment and alerts on them.
3. Predictive analytics – Uses the sum total of events to identify malicious activities that are likely to take place based on known information. This often manifests itself in situations like a spike in data aggregation by a user being alerted as either malware preparing for data exfiltration or a malicious user preparing to steal data.

Adding correlation for known bad events to represent higher priority threats is a crucial first step. However, correlation often provides too many "top priority" alerts. Security Analytics can provide deeper insight into not only new attacks but abnormal activities that are indicative of a compromised or malicious insider. Without the ability to apply domain knowledge to create proper context around identified anomalies, security analytics can provide a high rate of false positives.

The real issue is the difficulty being able to identify the low and slow or other complex multistep attacks and put the various pieces together in a timely manner, preferably before the attacker gets a foothold in your environment or achieves his or her other objective(s). New sophisticated attacks such as Advanced Persistent Threats (APT), Advanced Targeted Attacks (ATA), and never before emerging threats (zero day), are designed to bypass common signature checking tools like IDS/IDP, antivirus, etc. and being "new," they do not have correlation rules or policies created for alerting. These sophisticated attacks leave less of a trace for an automated tool to pick up requiring security analytics to ferret them out. To identify something that happened, is occurring, or has a high probability of occurring, security analytics tools are used to identify individual or sequences of activities that indicate a security breach.

## Priority 5: Incident Response

Priorities 1–4 are about tools and processes, but tools and processes for daily implementation and management are not enough when there is an incident. If the operations team is not prepared for how to respond when security events arise, the lack of preparation can be devastating to the enterprise. Just as faults in daily operations can cost money, so can the inability to respond quickly after a security incident, particularly breaches.

When an incident occurs, the security team needs tools that provide the best visibility into how the event is unfolding. Real-time notification from within seconds to a few minutes of an identified event is key. The longer the system takes to detect/notify an incident, the greater the head start an attacker has, thus increasing that attacker's chance of success.

For organizations that are not normally under all-out attack, an incident response plan is a necessary tool to assist the operations personnel to conduct an effective response. Such a plan would discuss who takes control of the investigation and recovery process, who provides internal management and external customer communications, and answers the key question as to which is more important: recovery or forensics. Depending on the level of virtualization in the environment, these can be two very conflicting requirements. It often means wiping a system and restoring it from the last known good backup, which

rebuilds the revenue stream but erases all of the forensics data on the system. The data on the system is required for understanding the progression of the attack and facilitating prosecution or restitution. If the focus is on forensics, the priority will be on the investigation and will delay restoration. With virtualization, snapshots can be taken to collect state data on the system and only sacrificing the live forensics data while accelerating restoration, essentially providing the best of both worlds.

However, effectively using the plan takes practice and coordination. There are several options for testing and training. "Live fire" exercises that extend from penetration testing and similar exercises are very helpful but can be disruptive. Planned scenario drills are a good second as they are more controlled but still provide valuable feedback on the state of documentation for recovery. In any case, documenting the processes and procedures and conducting these exercises before an actual event occurs is invaluable preparation. The heat of battle is no time for doing a proof of concept.

Automated response technologies supplement manual incident response processes by immediately responding to threats identified by a SIEM system, while at the same time alerting IT security personnel and triggering human intervention. Responses might include blocking an IP address, detaching a USB device, killing a process, logging a user off, removing a user from groups, and/or shutting down a machine. Automated response is particularly important in organizations without 24/7 IT security staffing.

*Automated response technologies supplement manual incident response processes by immediately responding to threats identified by a SIEM system, while at the same time alerting IT security personnel.*

Incident response processes benefit from iterative learning, ongoing process improvement, and automated response implementation. Threats evolve and defenders should, too. This includes periodically updating techniques for event identification, escalation and remediation, and the scope of automated response. The goal for incident response programs is to accumulate knowledge and hone in on the right tool for the right job.

## EMA Perspective

Information security is one of the most challenging disciplines. It affects or is affected by application, systems, network, and change management, as well as every other discipline in IT. It also requires a range of different tactics to be successful – dealing with evolving threats, new vulnerabilities, identity and access management, and monitoring change. Security is generally perceived as a system-level property that practitioners must try to deliver one project at a time. In reality, it is an environmental- or organization-level property that should be broken down into composite parts like the construction of the brick wall. For many organizations, it is difficult to keep the big picture strategy of what that final wall will look like while they are in the middle of assembling all of the pieces over the course of years.

Many organizations began building this environment with tools like those available from SolarWinds, a provider of IT management technologies including security. In recent years, SolarWinds significantly expanded its portfolio through product development and acquisition. With that drive, it created a broad portfolio of products that not only addresses the top five network security priorities, but also provides many of the other components needed by security professionals to build their defense in-depth "brick wall" and address many other IT management needs.

Reviewing the five network security management areas, EMA finds that a number of products SolarWinds provides fit in nicely. For identity and access management, SolarWinds provides a useful user and device management application called User Device Tracker that can locate and track devices

that require your special attention by whitelist, hostnames, and IP and MAC addresses, and identifies the users on the network associated with each. It also shows the node or access point, port or SSID, and VLAN through which a tracked object is connected.

For vulnerability management, SolarWinds Patch Manager provides patching automation and delivery services for both Microsoft and third-party applications from a single point of control. Additionally, Patch Manager delivers centralized visibility into the patch status of systems and includes an extensive collection of easy-to-use, built-in reports for patch compliance reporting, along with the added ability to schedule reports and create custom reports. With these reports, users can get key information, such as missing or failed patches, security-related group policy settings, and how they are configured enterprise-wide, or the updated status of anti-virus definitions.

Switching context a little and moving to the broader view of environmental, rather than just system, vulnerabilities, SolarWinds offers two solutions that address other vulnerability and threat vectors. One is their USB Defender technology, which is a feature of the company's SIEM product, SolarWinds Log & Event Manager, and delivers the ability to log, monitor and control the introduction of USB devices in your environment. If a device is inserted into a machine, USB Defender can disable user accounts, quarantine workstations, and automatically or manually eject USB devices. It can also provide audit reporting on USB device usage/introduction within the environment. The other useful tool is SolarWinds NetFlow Traffic Analyzer. In most cases, the network operations teams use this tool to see which users, stations, or protocols are the bandwidth hogs and analyze when the high and low usage times are as a part of capacity planning. It can also be used to identify rogue machines operating outside normal time windows or communicating excessively; it can identify chatty applications and the ports they are using, which may indicate poor application performance or worse, like malware infections scanning the network, communicating for command and control, or relaying company data to the outside on allowed protocols.

Another tool that meets both security and operational requirements is SolarWinds Network Configuration Manager, which manages device configurations, tracks real-time changes, and generates out-of-the-box compliance reports for routers, switches, firewalls, and load balancers from the top vendors. Additionally, Network Configuration Manager ensures consistency of policies across all network devices, identifies network devices with vulnerable software, and includes multi-level change approval support.

The core of the SolarWinds IT Security solution is the Log & Event Manager. This SIEM solution ingests data from a wide range of data streams, then provides real-time, in-memory event correlation for immediate threat detection. It can analyze millions of events and deliver customizable automated responses for the identified events. It also provides advanced search capabilities and visual data exploration tools to facilitate forensic investigation, as well as pre-packaged templates for regulatory compliance reporting. Additionally, the Log & Event Manager includes hundreds of built-in filters, rules, searches, and reports that are already categorized for ease of use.

Just as it is important to identify the security problems, you must be agile in your ability to respond. As previously mentioned, in some cases you may want SolarWinds Log & Event Manager to provide an automated response. In many cases, the event requires further investigation from an analyst to deliver an appropriate response. For these scenarios Web Help Desk, a service desk management product from SolarWinds, can help with your incident response workflow.

The SolarWinds solutions can appear at first glance as an amalgam of point solutions. They can be used individually to achieve results quickly. This makes them appealing to SMBs that need to find something to plug a specific "hole in the dam." For larger enterprises, the ability of these individual solutions to work together should not be underestimated. SolarWinds provides a highly modular suite of products that can stand alone or integrate into the "single pane of glass" methodology, placing event management and reporting in one place. With the competition for budget dollars faced by security organizations, cost is a key factor in the decision process. Though ROI and ROSI are not part of the top five network security priorities, they are part of the top five business priorities. SolarWinds licensing plans are very cost effective and many of SolarWinds' products have a fully-functional free trial download available, which is great if you are in a bind and need to try before you buy.

## About SolarWinds

SolarWinds provides powerful and affordable IT management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies, and educational institutions. SolarWinds is committed to focusing exclusively on IT Pros, and strives to eliminate the complexity that they were forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on-premises to the Cloud. SolarWinds' solutions are rooted in their deep connection to their user base, which interacts in their thwack® online community to solve problems, share technology and best practices, and directly participates in their product development process. Learn more today at http://www.solarwinds.com/.

## Additional Reading…

For information on optimal monitoring practices in other management disciplines, please see EMA's other White Papers in the Essential IT Monitoring series:

*Essential IT Monitoring: Five Priorities for Cross-Domain IT Management*

*Essential IT Monitoring: Ten Priorities for Systems Management*

*Essential IT Monitoring: Seven Priorities for Network Management*

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

---



**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2775.032816