EventTracker

Actionable Security Intelligence

SIEM Simplified

Answering the 4W's – Who, What, Where and When

White Paper

Abstract

Security incidents such as successful hacks or breaches are not easily defined or understood because the evidence of the anomalous event is co-mingled within thousands, even millions of other routine (and cryptic) audit logs and security data. It is hard to determine whether you are actually collecting this data, let alone analyzing and reacting in a timely manner. To support security, compliance and operational requirements, specific and fast answers to the 4 W questions (Who, What, When, Where) are very desirable. These requirements drive the need for Security Information Event Management (SIEM) solutions that provide detailed and one-pane-of-glass visibility into this data, which is constantly generated within your information ecosystem. This visibility and the attendant effectiveness are made possible by centralizing the collection, analysis and storage of log and other security data from sources throughout the enterprise network. Given the voluminous nature of log and security data, the need for aggregation, analyzing and correlation is imperative. Else, how can you hope to identify genuine problems? Once automation of the collection is in place, basic analysis can be automated but it is quite often the case that review and analysis requires human analysts with domain knowledge. Your choices then become – spend time doing it yourself, or obtain the services of an outside specialist.

Outsourcing IT functions of large, medium and small organizations is common based on practical decision-making driven by strategic, tactical and financial considerations. However, despite the *growing recognition by senior management that SIEM is a critical necessity* it is often viewed by IT as a tactical effort to satisfy a checklist that addresses a specific compliance or security requirements. SIEM as a Service is a path to improve security, compliance postures and bottom-line results all at the same time.

This whitepaper discusses the SIEM Simplified service that can help you achieve these goals.

Introduction

Every element of your IT infrastructure - network device, operating system, application, etc. has recording/logging capability. The first step in the process is figuring out what sort of log/event information is to be generated, transported, and processed and stored. However, the volume of security data generated is far too large for any human being to process. Even small networks of a few dozen servers generate millions of log records daily which can result in dozens or hundreds of "alerts". The lack of standardization in format and transport protocol is another challenge. Once you have it, how to leverage it? This is the point where SIEM begins and basic log management ends. Security Information and Event Management (SIEM) is a term coined by Gartner in 2005 to describe technology used to monitor and help manage user and service privileges, directory services and other system configuration changes; as well as providing log auditing and review and incident response.

The challenge is to sift through all these logs, events and alerts and identify the critical ones that need your time and attention The core capabilities of SIEM technology are the broad scope of event collation/aggregations and the ability to correlate and analyze events across disparate information sources. Simply put, SIEM technology collects log and security data from computers, network devices and applications on the network to enable analyzing, alerting, archiving and reporting.

SIEM technology is routinely cited as a basic test practice by every regulatory standard and its absence has been regularly shown as a glaring weakness in every data breach post mortem.

Critical aspects about logs:
• Answers the 4W's
• Early Warning
• Addresses Compliance
• Proactive vs. Reactive
• States facts
• Do not lie

IT Security Purchasing Intentions 2013 Europe published by ComputerWeekly.com in 2013

"Why are technologies such as data leakage or loss prevention (DLP), security information and event management (SIEM) and network access control (NAC) not seeing a stronger uptake?

Almost two-thirds of IT security professionals said they do not use Security Information and Event Management (SIEM) technology. Of those that do use SIEM, 22% said they used it for compliance and proactive security response and 10% used it for compliance only. Significantly, 4% said they had used SIEM but had abandoned it. Although 22% of firms claim to use SIEM proactively, Andrew Rose, principal analyst for security and risk at Forrester Research said there is likely to be a wide variance in the level of pro-activity in each organization.

Rose said Forrester has seen a surge in interest in SIEM and many conversations revolve around the selection of a suitable third party to either manage the work, or partner with, to deliver the service.

Just over a third of IT security professionals polled in Computer Weekly/Tech Target's security purchasing intentions survey said Security Information and Event Management (SIEM) was too complex and time consuming to deploy. It is unsurprising to see that SIEM is held back by a fear of complexity, said Andrew Rose, principal analyst for security and risk at Forrester Research."

AT a RSA Conference in 2014 it was pointed out that SIEM solutions have the highest "shelfware" (products being abandoned).
The primary reasons for this were:
• Lack of staff to use the product properly
• Not enough time or expertise to implement properly
• Lack of clarity of use and business alignment
• Customer only purchased it to satisfy a compliance / regulatory requirement
• Unable / afraid to enable important features

In reviewing breaches (Verizon/Forrester, etc.) proper review of audit logs would have detected anomalous behavior right away or before serious damage was done in over 90% of the case studies. There is no denying it is time consuming, tedious and difficult to manage and requires specific expertise to yield value.

EventTracker's offering to address this predicament is *SIEM Simplified* [SM].

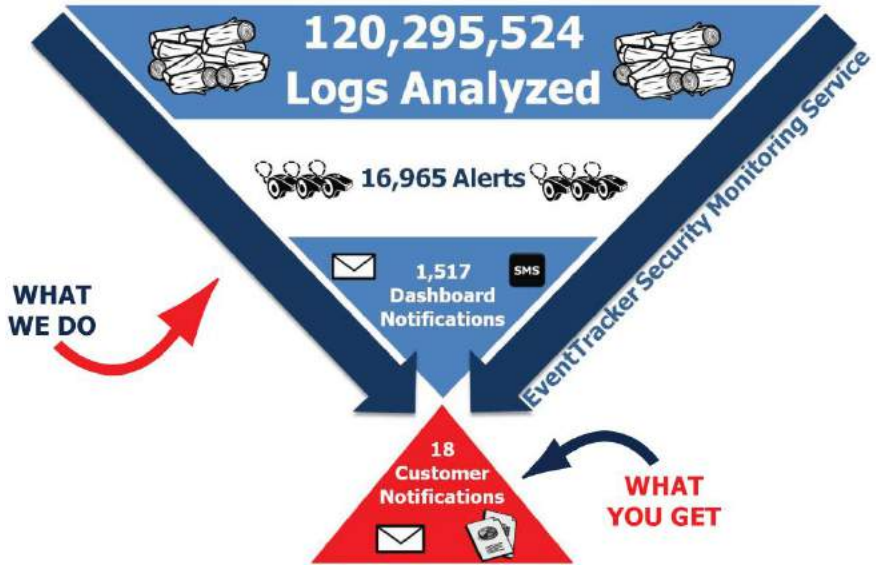
Gartner's - Predicts 2013: Cloud and Services Security has the following key messages:

- For smaller organizations, requirements to deploy and manage security information and event management (SIEM) technology, as well as assess and react to alerts, will exceed the expertise or availability of security staff.
- By 2015, over 30% of SIEM deployments will include service-based event monitoring or SIEM management components, up from less than 5% today.

Gartner analyst Anton Chuvakin "Think about this for a second: a lot more people will engage professional services to help them RUN, not just DEPLOY, a SIEM. However, this is not the same as managed services, as those organizations will continue to own their SIEM tools."[1]

Gartner's Magic Quadrant for Security Information and Event Management 2014 states:

- SIEM is a $1.5 billion market that grew 16% during 2013 - with an expected growth rate of 12.4% during 2014



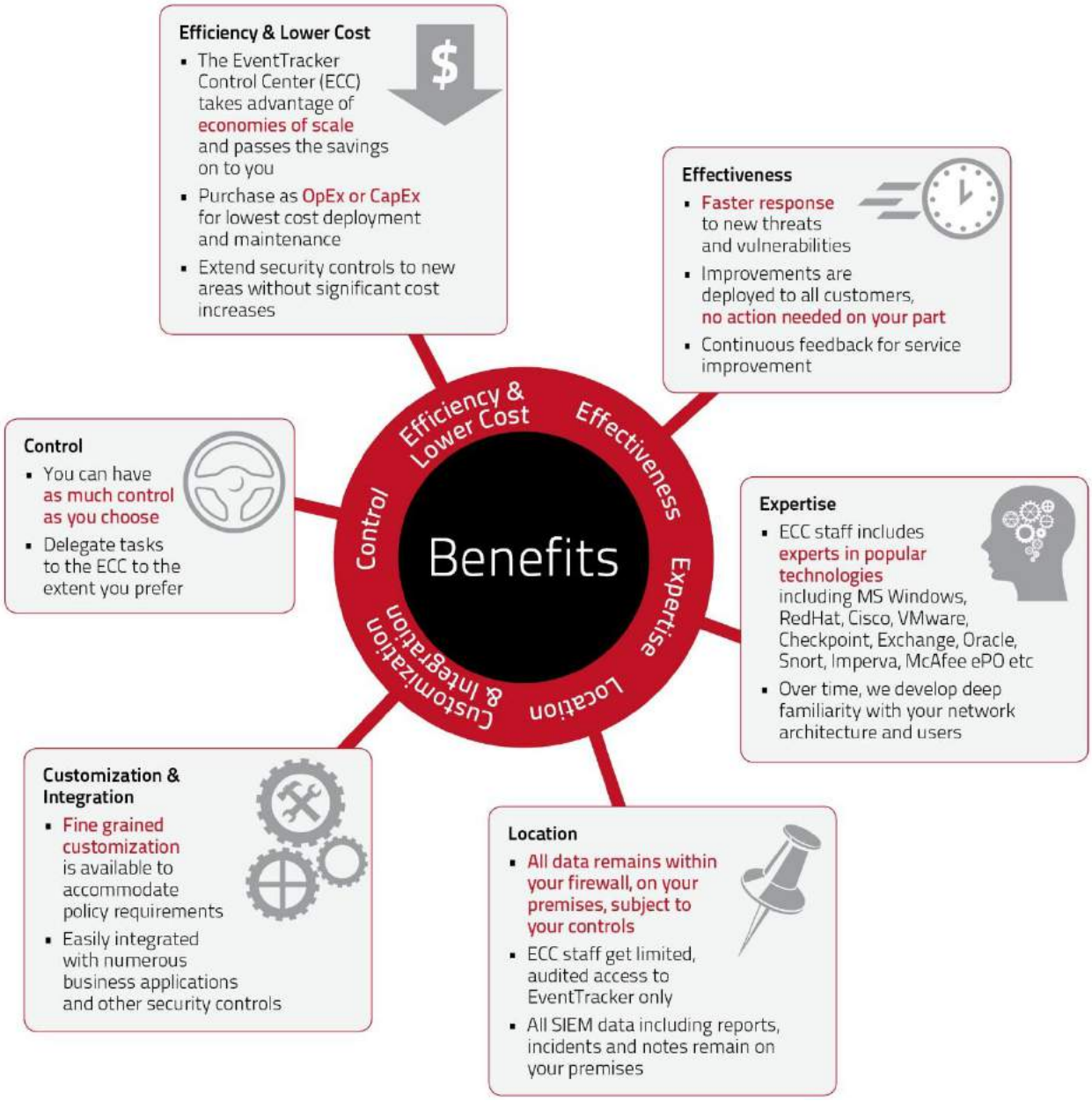
SIEM Simplified [SM] - Benefits of on-premise SIEM with remote monitoring and alerting

[1] "**Services: A MUST for SIEM**" with allusion to the **Annual Gartner Predict 2013**

After deploying security monitoring technology, the next step is to develop activity reports and define a monitoring process that is overseen by experts with suitable domain expertise. Developing and maintaining such expertise in-house is not only expensive, but challenging, especially for small and medium enterprises (SME). Remotely managed services for event monitoring not only satisfy compliance obligations but also help with skilled experts focusing on security every day.

Primary benefits of deciding for a remotely managed log monitoring solution include:	There are nevertheless, inhibitors to keep in mind while making a decision:
Access to personnel with expertise across popular or diverse technologies, security knowledge and threat intelligence	Perceived lack of control
Data remains within your firewall subject to your controls, meeting privacy requirements	Ownership and accountability
Efficient processes and automation to increase time for remediation	Lack of full service capabilities from service provider in terms of remediation
Discipline and rigor in monitoring operations	
Cross-device/cross-vendor correlation to improve security awareness and reduce risk	
Scalability achieved by outsourcing time-consuming manual correlation and analysis	

SIEM Simplified SM — Efficiency, Scalability and Intelligence



Anton Chuvakin in the Gartner Risk Management Summit 2014 shared these in his presentation for "Technical Professionals - SIEM Architecture and Operational Processes":

"You can buy a SIEM tool — but you cannot buy a security monitoring capability"

"Security monitoring is an eternal commitment"

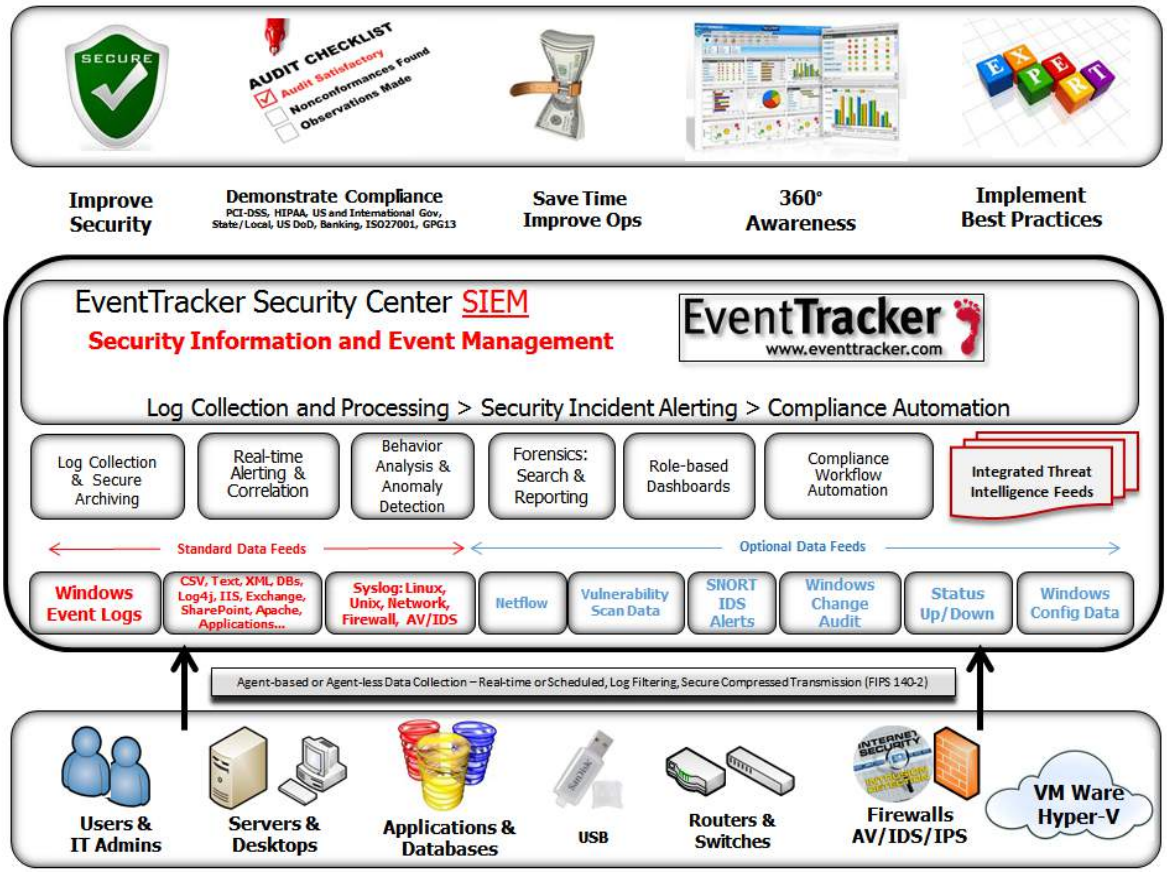
SIEM Simplified SM

Your Need: Complete Coverage, Zero Hassle

Barriers to the effective implementation of a SIEM and log management solution include a lack of in-depth knowledge, and insufficient time or resources to effectively extract the actionable information concerning your IT infrastructure. Monitoring all the log sources in your IT environment is a time-consuming task, even with a SIEM or log management solution. Sifting through hundreds or thousands of incidents every day pulled from millions of logs and dozens of reports requires discipline, patience and expertise. How can you do this effectively at a reasonable cost?

Your Solution: SIEM Simplified SM

SIEM Simplified SM is our managed services offering to enhance the value of the EventTracker range of products. Our experienced staff accepts responsibility for all SIEM related tasks including incident reviews, log reviews, configuration assessments, incident investigation support and audit support. We can do this for you daily or weekly depending on your need.



SIEM Simplified [SM] augments your existing resources for IT security and regulatory compliance. By co-sourcing your SIEM and log management responsibilities with *SIEM Simplified* [SM], you can leverage the expertise and experience of skilled security professionals without having to increase the size of the IT staff or incurring additional capital expenditures.

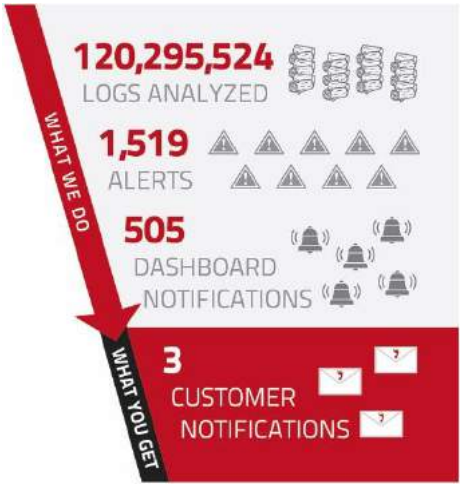
The *SIEM Simplified* [SM] value proposition

SIEM Simplified [SM] is a Managed Service delivery of EventTracker. By co-sourcing your SIEM and log management responsibilities, you leverage the expertise and experience of skilled professionals without having to increase the size of your IT staff.

- You leave the heavy lifting to us. We augment your IT team, allowing you to remain focused on the unique requirements of your enterprise.
- You have access to personnel with knowledge across varied technologies. Our team includes experts in various technologies including Windows, Cisco, VMware, Checkpoint and many security solutions, such as Snort, McAfee, and Imperva etc.
- We apply defined and tested monitoring processes meticulously and thoroughly, for you.
- We manage the service delivery model with process discipline and operational rigor.
- We ensure discipline and adherence to standardization to facilitate productivity.

The Process

- We consult and coordinate with your team to configure and deploy EventTracker to meet your needs.
- We tune the system to your needs. Tune behavior analysis dashboards and setup alerts on out of ordinary/new enterprise level activities.
- We learn "normal" behavior during a baseline period and draw the attention of a knowledgeable user to 'out of ordinary' or 'new items'.
- Our experienced staff assumes responsibility for all daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation and audit support. The 4 W's of Who, What, When, Where are always the key when filtering or investigating alerts.
- We deliver Incident Analysis, Log Report Review, and Annotation of Findings with Remediation Recommendations.
- The result is an end-to-end annotation of logs and change audit review with findings and remediation steps recommended.



Alert Response Procedure	
Level	Activity
1	Classify all events – Errors, Alerts, Warnings, logon Failures, New Activities, New IP Addresses and Out of Ordinary Activities, Flag qualified alerts
2	Investigate flagged alerts. Acknowledge and Annotate incidents
3	Alert / escalate to client

Anton Chuvakin in the Gartner Risk Management Summit 2014 shared the below, in his presentation for "**Technical Professionals — SIEM Architecture and Operational Processes**".

SIEM Maturity Road Map

State No.	Maturity Stage	Key Processes That Must Be in Place
1	SIEM deployed and collecting some log data	SIEM infrastructure monitoring process Log collection monitoring process
2	Periodic SIEM usage, dashboard / report review	Incident response process Report review process
3	SIEM alerts and correlation rules enabled	Alert triage process
4	SIEM tuned with customized filters, rules, alerts, and reports	Real-time alert triage process Content tuning process
5	Advanced monitoring use cases, custom SIEM content use cases	Threat intelligence process Content research and development

With *SIEM Simplified* [SM], you start day 1 of operations at maturity stage 3 of the above road map. Our existing and time tested processes are available to you through Operational Run Books delivered to you through trained EventTracker Control Center personnel. Subsequently, we work together to move forward into the subsequent stages of the road map.

Sample Report

Critical Observations Summary

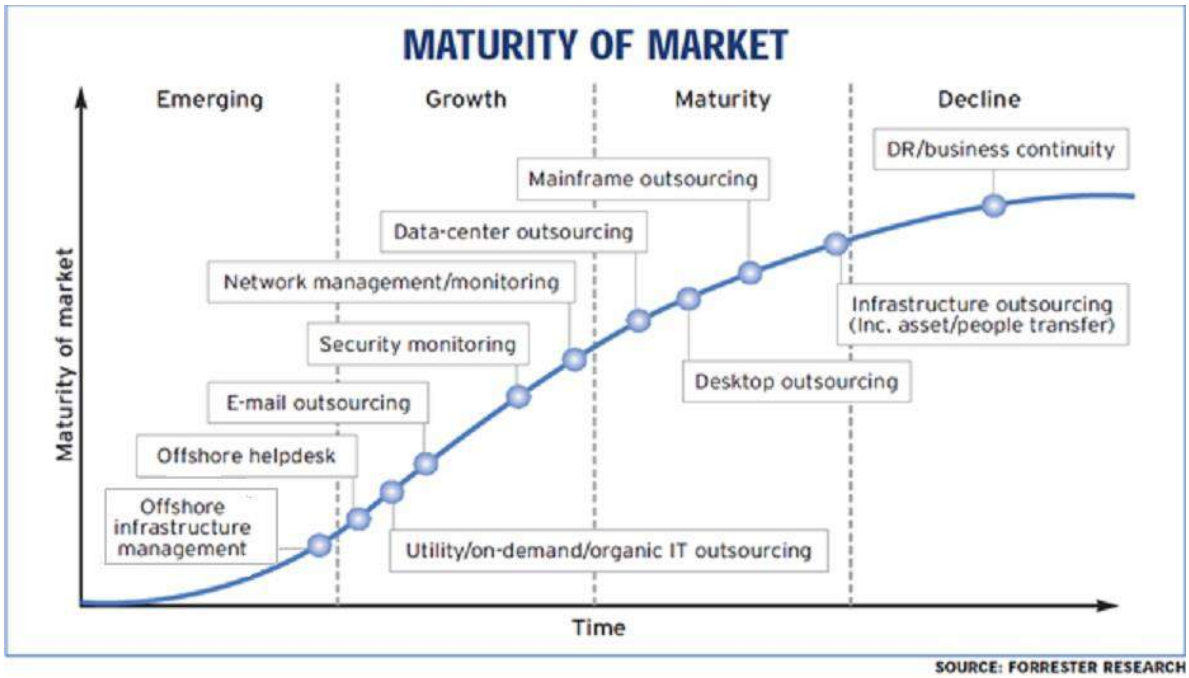
RISK Code	MONITORING ACTIVITY	OBSERVATION	Details
	Privileged User Monitoring	5 login failures were observed	Hyperlink
	Monitoring for Changes to Identity and Access Policies	9 configuration change events in syslog device were observed User was added to domain administrator group A password was set to never expire	Hyperlink
	Identity/Role Context in User Activity Monitoring Reports	A service account had a successful type 2 log on event A service account had successful log on event with log on type 10	Hyperlink
	Change Management Reports to Identify Resource Access Exceptions	Unauthorized files were added Files were deleted. These are unauthorized changes.	Hyperlink
	Data Access	Users accessed critical files. Users tried and failed to access critical files	Hyperlink
	Application Activity	Errors in the system were observed	Hyperlink
	Behavior Analysis and Threat Intelligence for SIEM	An abnormal amount of logs were generated for the day	Hyperlink
	System Resource	No concerning observations to report	Hyperlink
	Monitoring for changes to Identity and Access Policies	No concerning observations to report	Hyperlink

Outsourcing

Outsourcing began in the manufacturing industry and is now a standard offering in the services sector. Initially there was resistance to outsourcing IT functions because of their sensitivity and tactical significance to enterprises, but the outsourcing market has been growing at about 60 percent annually.

In their International Business Report 2014 ***"Outsourcing: driving efficiency and growth"*** Grant Thornton state that main outsourcing drivers are:

- "Globally, businesses which outsource are principally looking for efficiencies (57%) and to reduce costs (55%). In North America, 70% cite reducing cost and 69% improving efficiencies"
- "The drive for process efficiencies – where the focus is on doing things better and faster, rather than simply cheaper – is a major driver in North America (44%)"



Information security is a critical function however it is no longer necessary to do it all in-house. There is a growing consensus that outsourcing components of security is a viable option for many. Any good Managed Security Services Provider (MSSP) will provide a comprehensive suite of offerings including:

- Firewall management
- Log monitoring, management, and retention
- Security incident and event monitoring and management
- Security event analysis and correlation
- Intrusion detection and protection management
- Distributed denial of service protection
- Web filtering and monitoring
- Virus, spyware and instant messaging protection

Services are clearly split into two distinct set of activities (1) the actual monitoring of your enterprise network and (2) remediation. Under the umbrella of SIEM falls: log monitoring, management and retention; security incident and event monitoring and management; and security event analysis and correlation.

Gartner have noted in their **Magic Quadrant for Security Information and Event Management 2014** that SIEM product vendors now offer remote management or monitoring of their SIEM products. The also state that **"**Real-time monitoring and alerting, as well as log collection, query and reporting, are available as a service offering from MSSPs. Gartner clients indicate a growing interest in using MSSPs to monitor a customer-deployed SIEM."

About EventTracker

EventTracker's advanced security solutions protect enterprises and small businesses from data breaches and insider fraud, and streamline regulatory compliance. The company's EventTracker platform comprises SIEM, vulnerability scanning, intrusion detection, behavior analytics, a honeynet deception network and other defense in-depth capabilities within a single management platform. The company complements its state-of-the-art technology with 24/7 managed services from its global security operations center (SOC) to ensure its customers achieve desired outcomes—safer networks, better endpoint security, earlier detection of intrusion, and relevant and specific threat intelligence. The company serves the retail, hospitality, healthcare, legal, banking and financial services, utilities and government sectors.

EventTracker is a division of Netsurion, a leader in remotely-managed IT security services that protect multi-location businesses' information, payment systems and on-premise public and private Wi-Fi networks. www.eventtracker.com.