

A PROACTIVE SECURITY POSTURE:
THE BENEFIT OF A PARTNERING WITH A SECURITY SERVICE PROVIDER
IN A DIFFICULT BUSINESS ENVIRONMENT



A Frost & Sullivan White Paper

Author: Jarad Carleton, Principal
Consultant ICT Practice

Sponsored by EDS and EMC Corporation

TABLE OF CONTENTS

TABLE OF CONTENTS

Constant Business Goals for Any Economy	3
The Global Business Environment	3
The Challenge of Best of Breed Security Solutions	4
Partnering with a Security Service Provider	5
EDS, an HP Company – Enterprise Security Event Management	5
Illustration of EDS ESEM with the RSA enVision® Platform	7
EDS ESEM Dual Network Architecture Illustration	8
In Summary	9

Constant Business Goals for Any Economy

Free trade agreements, regional trade organizations, and the World Trade Organization (WTO) have played a major part in the creation of a globally interconnected business environment. As barriers to trade have been lowered and information technology has allowed nearly instantaneous global communications, economies have become inextricably linked across geo-political boundaries in ways that the world has never seen before. Many businesses now face global competition and need to find ways to achieve two critical goals:

- Position the business to ensure continued growth
- Secure the IT infrastructure that allows the business to function

Depending on the industry, a company may be under the misconception that these two goals are mutually exclusive, but they are not. In the business-to-business (B2B) side of the economy, collaboration at regional and global levels is on the rise as is the sharing of business-critical data. Even in industries such as retail, B2B data sharing is a daily part of business in order to keep shelves stocked and to receive payments from customers that use credit or debit cards.

As collaboration and data sharing within and between organizations continues to rise, businesses will need to protect sensitive data now more than ever before. If an organization cannot assure its customer base that strong security measures are in place to protect credit card information and other types of personal and sensitive data, customers will vote with their feet and flee to a competitor. Since the cost of acquiring a new customer is estimated to be between 5 and 10 times the cost of keeping current customers, in challenging economic environments it's in the best interest of an organization to take the extra steps necessary to improve its security posture.

However, while considering the issue of security as a necessary component of a business growth plan, it is also important to maintain a balance between the need for a strong security solution and ensuring secured the IT infrastructure doesn't inhibit legitimate business functions.

The Global Business Environment

The current global economic environment is the most challenging for businesses since the 1930s. A recession of global scope has spread around the world and is forcing businesses to focus on core competencies and find areas of the organization that can be made more efficient.

In addition to the challenging economic environment, cybercrime rose by 33 percent¹ in 2008 and is expected to continue rising in 2009 due in part to the increase in staff layoffs. These layoffs will increase the number of disgruntled current and former employees with

¹Associated Press. "Reports of Internet Crime Jump 33 Percent." San Francisco Chronicle, 30 March 2009
<<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/03/30/national/w111230D44.DTL>>

sufficient inside knowledge to develop a targeted attack against a business. Furthermore, employees facing salary cuts or other difficult financial situations are susceptible to bribes from organized crime in return for login IDs and passwords. When this happens, organized crime is able to improve the efficacy of targeted attacks against businesses worldwide, making it even more important for a business to quickly identify and follow up on suspicious activity within the IT infrastructure.

The global recession, coupled with an increase in cybercrime and targeted attacks against businesses worldwide, will put organizations in a difficult position. As financial pressures force businesses to reduce the size of their workforce to stabilize the organization, that very act weakens the security posture of an organization and pushes businesses to increase their security budgets rather than keeping them at current levels.

These potential threats have not gone unnoticed. In the McAfee Unsecured Economies Report published in 2009, 42 percent of survey respondents said that laid off employees are the biggest threat to the security of their business during the current economic downturn.²

The Challenge of Best of Breed Security Solutions

As organizations worldwide have taken measures to improve their security posture, they are driven to implement best of breed security solutions. As a result, organizations must manage multiple security point solutions from several vendors rather than a single vendor. Because best of breed point products are frequently what IT departments have implemented, different components in the solution come from different vendors which means that the point products don't easily communicate and often require separate management interfaces. While multiple solutions can at times be necessary for an organization to enhance security, ensure regulatory compliance, and minimize outside liability risk, they do create a management problem that clearly increases costs for the organization.

The implementation of multiple security solutions that are independently managed puts IT security professionals in the difficult position of protecting business assets with disjointed security solutions. These solutions can create so many alerts and false positives that it is impossible to keep up with the workload. As a result, businesses tend to lack a clear vision of their security risk, which makes a strong security posture difficult and costly to proactively maintain.

Of course when a security posture and policy is difficult to maintain due to budgetary and personnel constraints, it's also hard to enforce uniformly, which in turn creates weak spots that can be taken advantage of by criminals and disgruntled former and current employees. In addition, as many IT security professionals know, if and when security measures become a hindrance for business users of the network, those users will find ways to circumvent security measures even if they know their acts could put company resources and

- Unemployment in the largest economy in the world (the United States) reached 8.1% in February 2009 with some states reporting unemployment above 10%
- 42% of enterprises believe that laid off employees are the largest threat to the security of their business
- 39% of enterprises believe that outside data thieves are the biggest threat
- Cybercrime rose by 33% in 2008
- With no room for growth in the area of credit card fraud and identity theft, intellectual property theft has emerged as the new favorite for criminals.

² "Unsecured Economies: Protecting Vital Information." McAfee, Inc. 20 March 2009.
<<http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>>

intellectual property as risk.

The fact is that many business users perceive IT security beyond simple firewall and virus protection as a nuisance that prevents them from efficiently executing certain day-to-day business tasks. This is why any security solution that is implemented in an organization should achieve two key goals:

- Secure the organization's assets
- Empower business users to efficiently execute necessary business tasks

Too frequently in business environments there is an “us against them” attitude between business users and IT security professionals that puts an anchor around the business rather than helping to propel it forward. This situation can be avoided with the right services and tools and the right IT security management team.

Partnering with a Security Service Provider

IT security is a sensitive topic for companies and many IT departments lobby their executive team to implement, host, and manage each layer of security internally. In short, it can be a challenge to get an IT department to willingly initiate a strategic partnership with a security service provider. However, creating a strategic partnership with a provider that has expertise in managing and improving the security posture of businesses in multiple industries around the world has clear advantages.

Partnering with a security service provider is a proven way to expand an organization's group of trained IT security personnel, while avoiding the problem of employee turnover and lack of qualified IT security professionals. Not only does a partnership with a security service provider expand the number of trained and certified IT security professionals for a business, it also enables the organization to leverage the experience of the same professionals that support and protect clients in countries around the world 24 hours a day.

EDS, an HP Company – Enterprise Security Event Management

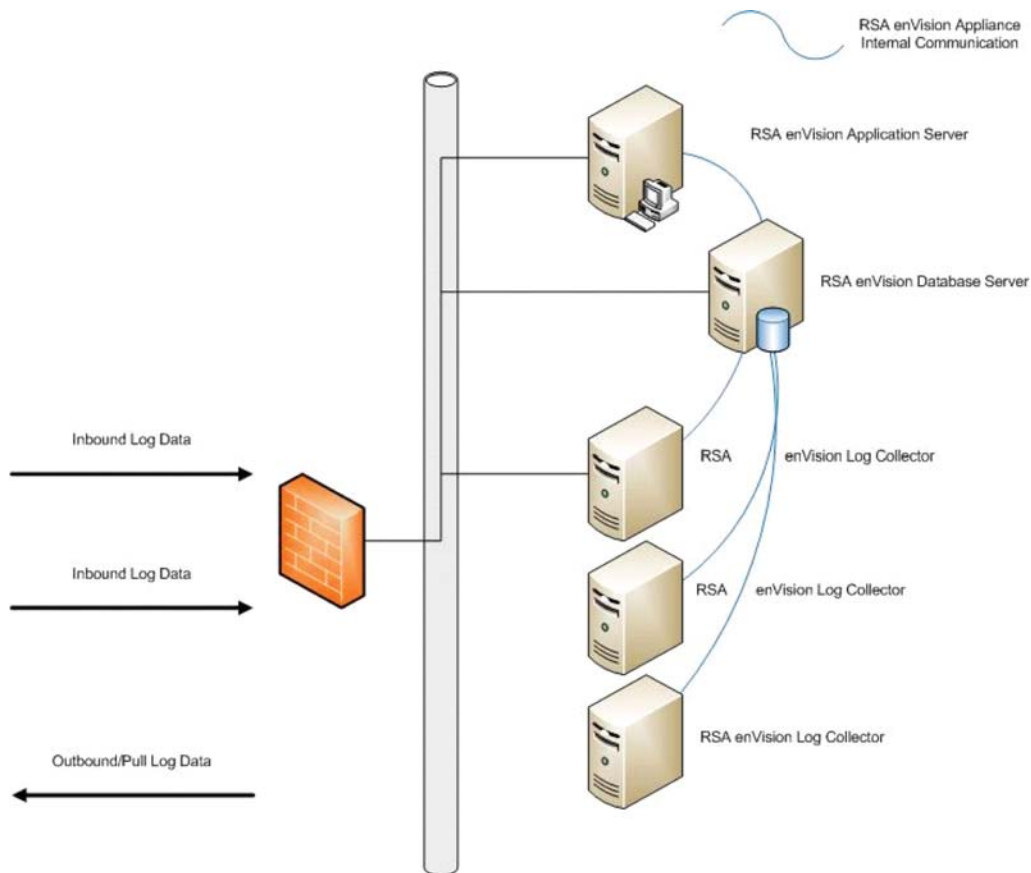
Depending on the size of a business, an IT department is frequently faced with so many logged security events that it becomes extremely challenging to filter out the noise from actual security risks. Unfortunately, in this situation IT security specialists are always in a reactive posture trying to keep up with alerts. Sometimes the alerts reveal that the IT infrastructure has been penetrated for a period of time before the alert was investigated and resolved. Other times, IT professionals are overwhelmed, can't keep up with the workload, and trust that nothing major has slipped past their defenses.

EDS Enterprise Security Event Management (ESEM) Services, which leverages the RSA enVision® platform, changes the rules of the game by giving client organizations a clear view of the current risks across the entire IT infrastructure. The service works by monitoring activity across the IT infrastructure such as file servers, network switches, web servers, applications, and databases and tracks events that could be considered normal until patterns are identified that appear abnormal. These abnormalities across the IT infrastructure are logged as security events by different layers of an organization's security defenses, which are then passed on to the RSA enVision platform where event data is given additional context by combining it with data from vulnerability assessment tools and configuration management systems.

This process enables IT departments to prioritize security alerts across the organization based on the value of the asset under attack and its potential vulnerabilities. It also provides enough contextual data to allow organizations to make educated decisions about how to respond to the security event. Leveraging its Enterprise Security Information System (ESIS) EDS is able to easily customize RSA enVision for static and emerging security threats. EDS ESEM Services using ESIS information enable client organizations to quickly identify risk, eliminate and/or significantly reduce windows of exposure, and compile reports that support legislative compliance. This makes the RSA enVision platform an even more powerful component of the EDS ESEM Service with watch lists easily created and updated by EDS for its clients based on organizational needs. ESIS is constantly updated from multiple sources including, but not limited to:

- The End Point Threat Management Database
- The iDefense Intelligence Feed
- The Department of Homeland Security's National Vulnerability Database
- The Forum of Security and Incident Response Teams (FIRST)
- US-CERT
- CERT\CC
- Information from point security product vendors

Illustration of EDS ESEM with the RSA enVision® Platform



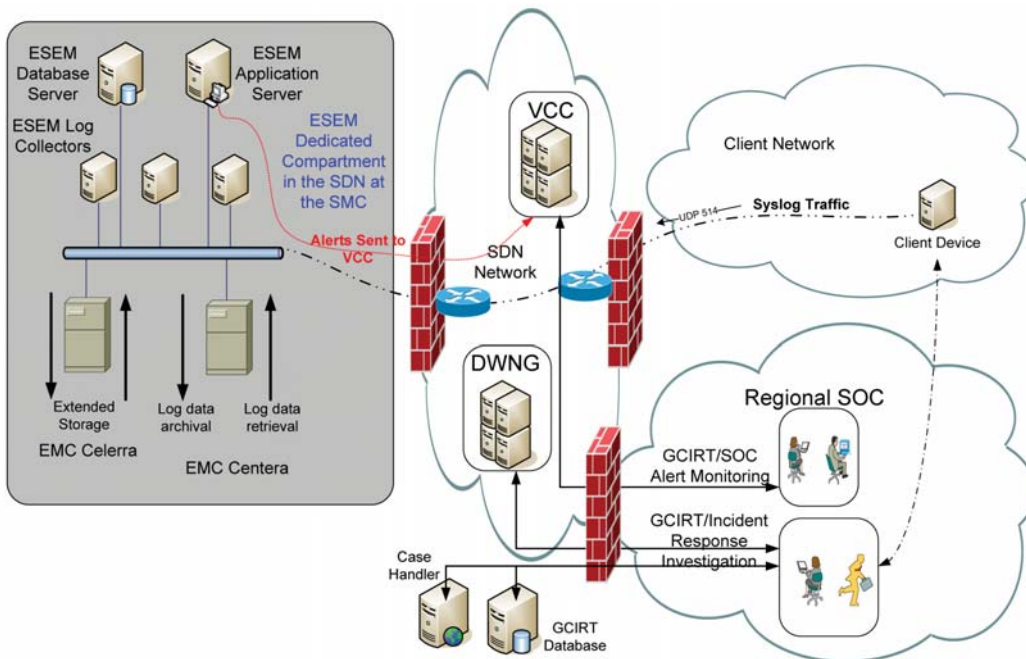
All of these features combined have been shown to reduce false positives and alerts while enabling a client organization or the EDS Security Incident Response (SIR) Service to focus its efforts on incidents based on priority rankings. EDS ESEM also provides IT security teams with timely detailed reports including:

- Inbound/outbound firewall traffic denied, by port number
- Blocked URL events
- Inbound IP spoofing denied
- Top URL destinations
- Top 20 alarms by port number

- Top 10 source-destination pairs for alarms
- Bandwidth usage by port
- Super-user access
- Failed super-user attempts
- Failed logons

Further, EDS ESEM Services allow organizations to leverage the economies of scale that can only be obtained by partnering with an IT security service provider. A service provider with multiple global clients has the necessary experience to manage complex infrastructures and rapidly optimize security deployments that ensure higher levels of protection and risk minimization, at lower cost, than most organizations can accomplish in-house.

EDS ESEM Dual Network Architecture Illustration



In addition, for organizations struggling to keep budgets under control, partnering with a service provider such as EDS will have the immediate effect of expanding IT security staff and achieving enhanced 24/7 monitoring and protection without the challenges associated with employee turnover and a lack of experienced personnel. When combined with the added protection of a dual network that prevents a denial-of-service attack masking another hidden attack, EDS ESEM Services and the associated EDS SIR Services give organizations a cost-effective means of strengthening IT infrastructure through rapid detection and prioritized response to security threats.

- EDS, an HP Company employs more than 2,500 security, compliance, and continuity professionals worldwide
- EDS ESEM Services support more than 5.4 million desktops and laptops, and 380,000 servers out of more than 180 data centers around the world
- 2.7 billion daily events are collected, stored, and processed by EDS ESEM Services every month
- EDS has secured over 1 million applications globally and 2.6 billion lines of code
- EDS ESEM Services handles over 3,600 security events each month

EDS ESEM and EDS SIR Services can control the daily management of RSA enVision, providing detailed reports as well as legislative compliance reports for the European Privacy Act, the UK Data Protection Act, PCI security, HIPAA, and Sarbanes-Oxley. IT departments can then focus their efforts on other business-critical projects rather than manual report creation, analysis, and resolution. As a result, this has a direct impact on outside liability risk minimization, while limiting damage to company assets and reducing overall security event management costs.

Organizations that take advantage of EDS ESEM Services gain the ability to apply increased focus on the core competency of the business in order to continue its growth, while simultaneously strengthening the security posture for both corporate governance and legislative compliance. Leveraging the expertise of EDS ESEM Services and the RSA enVision platform, organizations are able to utilize a cost-effective security event management service that provides IT departments with a centralized view of IT vulnerabilities across the entire organization. EDS ESEM Services provide businesses with a way to circumvent the challenge of disjointed security solutions with an experienced and trusted services partner, using experienced and certified professionals working 24/7 to apply their depth of knowledge for the benefit of client organizations.

In Summary

With the constantly changing IT security landscape, the challenge of disjointed best of breed security solutions, the number of enterprise assets to protect, and the overwhelming number of events that take place during the course of day-to-day business, it is easy to understand why many IT security teams struggle to keep pace with the investigation and resolution of reported events. The unfortunate fact is that regardless of the business environment, economic challenges, or the increase in cybercrime, customers, partners, and governments still expect businesses to protect sensitive data.

With so much at stake, an organization can't afford to drop the ball with IT infrastructure security because when it does, negative publicity, brand erosion, fines, and criminal or civil litigation consequences can be expected. For enterprises whose core competency lies outside of IT infrastructure security, relying on a trusted name in security solutions that can keep a business secure and compliant with regulations around the globe may be the best option available.

In today's challenging business environment, outsourcing tasks that your team struggles to stay on top of is not only a good business decision, it can also be a contributing factor to long-term survival and laying the foundation for future growth and success. Hundreds of organizations around the world in industries ranging from regional and national government, to petrochemicals, consumer products, financial services, transportation, and manufacturing use EDS ESEM Services, RSA enVision, or a combination of both to efficiently identify vulnerabilities. Used in combination with EDS SIR Services, organizations are able to pass the responsibility of security event mitigation to a trusted name in security services

while lowering costs by eliminating the management challenge of disjointed security solutions.

There isn't any reason to continue struggling to keep pace with enterprise security event management when EDS, an HP company, and a trusted name in IT services, can give your organization the edge it needs. Partnering with EDS ESEM and SIR Services will enable your organization to get the most out of your IT security budget.



RSA, enVision and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies. <http://www.rsa.com/>



EDS and the EDS logo are registered trademarks of Electronic Data Systems Corporation. All other brand or product names are trademarks or registered marks of their respective owners. EDS is an equal opportunity employer and values the diversity of its people. Copyright © 2008 Electronic Data Systems Corporation. All rights reserved. <http://www.eds.com/>

CONTACT US

Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Delhi
Dubai
Frankfurt
Kolkata
Kuala Lumpur
London
Melbourne
Mexico City
Milan
Mumbai
New York
Oxford
Paris
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sydney
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave.
Suite 100 Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from over 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.