

Vulnerability Management Made Easy



A FROST & SULLIVAN WHITE PAPER IN PARTNERSHIP
WITH OUTPOST24

TABLE OF CONTENTS

TABLE OF CONTENTS	2
INTRODUCTION	3
CHALLENGES IN VULNERABILITY ASSESSMENT AND MANAGEMENT	4
APPROACHES AND SOLUTIONS	6
THE GAP BETWEEN CURRENT SOLUTIONS AND ORGANISATIONAL NEEDS	8
HIAB – THE OPTIMAL VULNERABILITY MANAGEMENT SOLUTION ..	10
Case Study: Enabling Simple and Efficient Vulnerability Management in Grupo Salinas	12
Case Study: British American Tobacco Meets Efficient, Affordable and Flexible Vulnerability Management	13
CONCLUSION	14
ABOUT OUTPOST24	15
ABOUT FROST & SULLIVAN	16

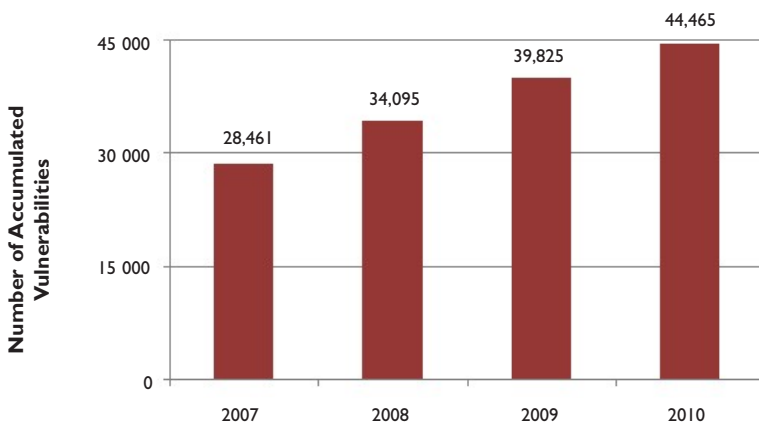
INTRODUCTION

Organisations are generating and storing an increasing amount of data. IDC estimate that the global storage requirements have increased by 500% over four years from 161 million terabytes in 2006 to 988 million terabytes in 2010. These data are sensitive and essential for organisations' operations, and therefore it is critical to keep the data secure. With this trend showing no sign of abating, organisations that do not actively seek to address their vulnerabilities are prone to security breaches that can lead to both direct and indirect loss of income. The increased threat stems from several factors, including:

- Hackers are getting smarter and more sophisticated in their methods to penetrate systems and gain access to sensitive data;
- Mobile devices are presenting a new attack vector and;
- Designer malware which is often advanced and persistent is becoming increasingly effective.

The number of threats has increased significantly in the last 15 years. The USA Computer Emergency Readiness Team (CERT) detected 417 vulnerabilities in 1995 – this increased to 4,640 in 2010, and Frost & Sullivan expects this trend to continue.

Figure 1: Accumulated Vulnerabilities Increased Year on Year



Source: CERT, 2011

As the companies are trying to react to the increased security challenge, so are governments. Governments are imposing various legislative frameworks upon organisations requiring them to protect data by imposing various levels of security to their systems through legislative frameworks such as Solvency II and PCI DSS. As a result of the increased threat of security breaches and increased level of regulations, vulnerability management has moved up the organisational agenda. Vulnerability management can help organisations overcome major challenges by:

- **Ensuring regulatory compliance.** Failure to comply with regulations can result in significant fines.
- **Reducing the risk of security breaches.** Major security breaches can have very damaging effects, including lawsuits, fines, and loss of customer trust.
- **Effectively managing the increasing number of network utilities and applications that needs to be guarded.**

“A vulnerability is a state in a computing system (or set of systems) that either: a) Allows an attacker to execute commands as another user; b) Allows an attacker to access data that is contrary to the specified access restrictions for that data; c) Allows an attacker to pose as another entity; and d) Allows an attacker to conduct a denial of service.”

CVE, 2011

CHALLENGES IN VULNERABILITY ASSESSMENT AND MANAGEMENT

Vulnerability management has been in existence since the 1990's, albeit in a simpler form. While original products lacked enterprise features and reporting capabilities, they have evolved over time. Improved products were introduced in the early 2000s, offering new functionality such as scanning capabilities, reporting options, centralised management, greater scalability and improved usability. Today, we have identified four key trends in vulnerability management:

- **Increase in automated tools.** Organisations of all sizes have long recognised the need to move away from consulting engagements and toward automated tools due to benefits such as cost savings, time savings and flexible/regular scheduling.
- **Increase in internal and external vulnerability assessment tools.** The best practice is to conduct both internal and external scans. Internal assessment tools have to be fully credentialed and deployed on the organisation's network to produce a list of vulnerabilities. External scanning solutions are often easier and more affordable as they tend to be provided as SaaS offers.
- **Tools that enable cost reduction.** Utilising a SaaS approach to provide relatively low cost vulnerability assessment capabilities.
- **Increase in the need to assess web applications.** Organisations are increasingly deploying web applications to gain flexibility and agility in their IT required to compete effectively.

Because vulnerability management solutions have evolved and become more sophisticated over the past two decades, they can now - better than ever - help organisations overcome critical security challenges. Frost & Sullivan has, however, identified a number of challenges associated with vulnerability management. The negative implications for choosing the most current solutions include:

- High costs due to testing professionals' high hourly rates;
- Increased risk due to more people knowing the vulnerable parts of the organisation's system – especially external people; and
- The trade-off between many features and capabilities versus ease of use.
- High internal costs and complexity in implementing and managing a sound vulnerability management program.

Frost & Sullivan does, however, believe that these challenges can be overcome by investing in solutions and working with vendors that demonstrate an intention to do the following:

- **Reduce cost.** To fully understand the risk level, the solution must be capable of active, credentialed scanning. This requires an appliance to be deployed and thus, raises costs and maintenance duties.

“The three key trends in vulnerability management are: Increase in automated tools, increase in internal and external vulnerability tools and an increase in tools that enable cost reduction”.

- **Improve accuracy and reduce false positives.** Customers can be discouraged from vulnerability scanning if it creates an unmanageable number of false positives. More attractive solutions could involve methods for reducing number of false positives, intelligent prioritisation, whereby vulnerabilities that need to be dealt with immediately are labelled differently than those that do not need immediate attention.
- **Ensure that the solution does not interfere with operations and is easy to deploy and use.** Solutions must not interfere with the operations in terms of preventing users from accessing the system, using functions or slow down the system otherwise the solution will not be used. Similarly, organisations must be able to efficiently implement and enforce a good process for managing vulnerabilities and the solution should be easy to use.

Frost & Sullivan believes that the threat of security breaches will only increase. Hackers are getting smarter, requiring organisations to invest in tools that highlight the weak spots in their network on a routine basis. It will become increasingly difficult to track and scan for vulnerabilities without a combination of internal and external automated tools.

To ensure organisations gain appropriate support, we believe that vendors must be more effective in helping their customer to identify their real requirements, and prioritise those needs. This may, in some cases, mean an expansion of the solution to a multi-function remit that can be adapted to the individual organisation's needs.

Furthermore, top ICT decision makers tend to focus on revenue-generating projects, and sometimes take a "check the box" mentality towards security. However, merely checking the box and meeting baseline requirements rarely translates into an effective security programme. Because a security programme is not directly revenue-generating, it can often be challenging for the security, IT infrastructure, or network team to secure funding for projects – especially in the current poor economic environment. To overcome this challenge, Frost & Sullivan believes that vendors should focus on educating their customers. Improved education would promote a better understanding of the potential threats, the implications of a breach, and the tools and services available to prevent these from occurring.

More significant problems may arise for organisations that choose to do nothing. By remaining passive and choosing neither to deploy nor subscribe to vulnerability solutions or services, organisations expose themselves to internal and external security attacks that may lead to the destruction of systems and/or the compromise of data. The business, consequences of security breaches are severe. Customers and investors lose faith in the brand and share prices tumble, when major breaches occur reducing both top and bottom line.

“Decision makers must be convinced to avoid the “check box” mentality in the combat against the rapidly increasing security threat to ensure that effective solutions are being deployed”.

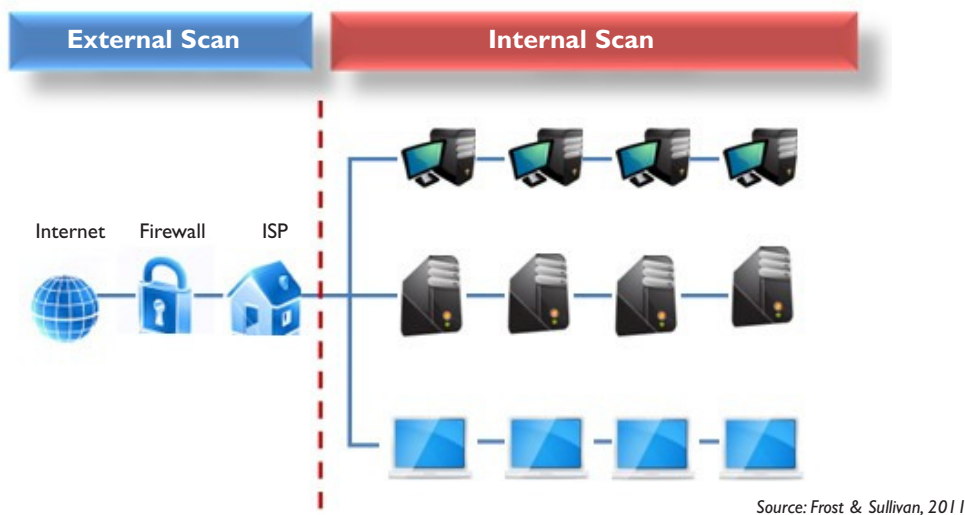
APPROACHES AND SOLUTIONS

Most vulnerability management solutions consist of multiple appliances depending on number of endpoints and network segments.

Frost & Sullivan believes that the ideal vulnerability management solution should entail two systems –an internal and external. The internal system tries to take information out of the organisation. It contains a centralised management console deployed within the client’s own network is required to perform the internal scans. Software on the console enables scans of all devices and systems inside the organisation’s network be it servers, computers, mobile devices, etc. The ideal vulnerability management solution should also provide strong capabilities for discovering web related vulnerabilities in both application and server layers.

“Frost & Sullivan believes that the ideal vulnerability management system should entail both an internal and external component.”

Figure 2: The Ideal Vulnerability Management Solution



The second system is the external – meaning a system that “attacks” the organisation from outside, trying to detect a way into the network. This will provide a list of vulnerable systems from an outside perspective. We believe the best practice is to conduct internal and external scans. However, these functionalities can be delivered in several ways. At present, there are two main approaches to achieve the same objective:

- **Security consultants:** A series of one-off engagements with specialists to determine the state of the organisation’s security architecture. We judge this too expensive to do often, but necessary to do frequently.
- **Automated tools:** These tools scan all network-attached devices, databases, operating systems, and, web applications. We judge they will provide remediation guidance and even trouble ticketing capabilities. More advanced solutions provide integration capabilities with e.g. patch management solutions and there are also approaches to integrate with related endpoint security products such as antivirus software.

To ensure that the organisation chooses a vulnerability management solution/service that best meets its needs, we believe that organisations must consider their own objectives and assess their specific security credentials.

There are no drawbacks for having both internal and external solutions. The only risky part is having a report of the organisation's vulnerabilities on an external device. If an external device performs an assessment and leaves the report outside the organisation, there is always a risk that someone will obtain the report and use it maliciously.

The biggest benefit of external scan is the relatively small initial investment that is required – enabled by a SaaS model. This model also offers the benefit of being flexible in terms of the frequency of scans, thereby helping the organisation to better meet legal and regulatory requirements.

THE GAP BETWEEN CURRENT SOLUTIONS AND ORGANISATIONAL NEEDS

While vulnerability management solutions have advanced significantly since the 1990's, there are still three key gaps between what organisations need, and what is offered. We believe these are as follows:

- Lack of ability to scan web applications.
- Lack of flexible delivery models.
- Report a high number of false positive incidents.

Lack of ability to scan web applications: Cloud computing and web-based applications are becoming increasingly common. However, some existing solutions lack the ability to scan web applications. This has created a market gap; several vendors have taken advantage of this, and have started offering solutions with this functionality. The gap mainly exists because the application assessment process is very different from the network vulnerability assessment. Consequently, not every vendor is able to develop a solution.

Lack of flexible delivery models: Many organisations use vulnerability management on a project-by-project basis. Indeed, many smaller organisations do not see the benefit of investing heavily in a solution; they would rather have the functionality available on a more ad hoc basis. As a result, more flexibility is needed in the way vulnerability management solutions are supplied. To accommodate organisations better, SaaS offers can offer the flexibility, and the affordability, but at this stage not many vendors offer SaaS solutions.

Report a high number of false positive incidents: Even though solutions are getting increasingly sophisticated, many still report a high number of false vulnerabilities. This often frustrates users as they feel they are wasting time on many false incidents. In addition, many solutions do not prioritise the vulnerabilities on the report. As a result, users have to work through the entire report, without knowing which incidents are false, which are critical and need to be rectified immediately and which are less critical.

Organisations may have concerns as to where the security vendor stores the reports, and whether the security level is appropriate. SaaS solutions that are currently available tend to report this data back to the vendor and store the data at the vendor's site. The notion of storing sensitive data outside the organisation, and out of the customer's control is a worrisome prospect for many customers.

“It is pivotal to choose the appropriate vulnerability management solution to ensure that technology support business goals, security is optimised and the organisation is compliant.”

Frost & Sullivan has identified three key challenges with sub optimal vulnerability management solutions:

- **The inability to support business strategy and remain ahead of competition:** The inability to secure web applications will force organisations to make a tough decision: to utilise this technology and accept the potential security risks, or not implement emerging technologies and as a result, lag behind the competition.
- **The inability to find affordable and appropriate solutions:** The option of SaaS gives customers the ability to implement a vulnerability management solution with relative ease and affordability.
- **The inability ensure efficient processes:** A high number of false positives cause inefficiency, because it is very time consuming for the user to go through a high number of false positives.

Sub optimal solutions will introduce undesired complexity and hamper the security process. The key implication of a sub-optimal vulnerability solution is that if it fails to prevent intrusions it is a poor investment; customers have not only paid for the solution but may still have suffered a costly security breach. As previously outlined, security breaches are costly – both directly and indirectly. Moreover, security coverage gaps can result in legislative non-compliance and, ultimately, fines and penalties.

Frost & Sullivan believes that, at this stage, all solution contains some gaps. However, we believe organisations can make informed choices. When evaluating which type of solution best suits the specific organisation, it is important to consider the trade-off of between functionality and usability. Being clear on key objectives enables the organisation to better identify which functions are critical, and which are nice to have. This enables the organisation to choose a solution that matches its key requirements. Prioritisation is also important, as the current trend is to add functionality and therefore increase complexity. For example, web application scanning is more time consuming and many scanning and management options increase the time that the user spends on tasks.

“Frost & Sullivan believes that organisations should look for solutions where there is an appropriate balance of functionality and ease of use.”

HIAB –THE OPTIMAL VULNERABILITY MANAGEMENT SOLUTION

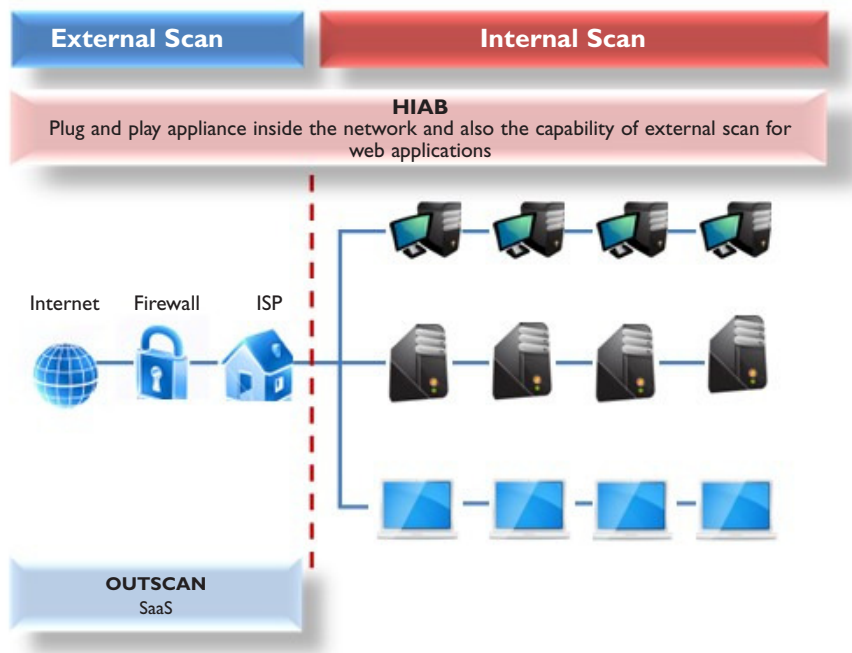
Frost & Sullivan believes that Outpost24’s HIAB solution complemented with the OUTSCAN offers an appropriate mix of functionality and usability.

The HIAB is the internal component which takes the form of a plug and play appliance. The solution is deployed inside the organisation’s network. As the device is inside the organisation’s own network, sensitive vulnerability reports never leave the internal network. The report is securely stored on the HIAB device. The solution is aligned with Common Vulnerabilities Exposures (CVE) standards for effective naming and severity scoring. Otherwise, vulnerabilities can be overlooked or duplicated, creating either security risks or an unnecessary increase in workload. In addition, HIAB’s unique architecture provides the capability of scheduling and conducting scans in the cloud enabling organisations to securely gather both internal and external scanning data on the appliance.

OUTSCAN is the stand-alone external component delivered as a SaaS solution. The solution is more affordable, mainly due to its SaaS delivery format compared to the HIAB. This delivery format ensures the organisation incurs only operating expenses as opposed to capital expenditure. The similarities between the HIAB and the OUTSCAN solutions are ease of use and the ability to operate without any negative implications on other systems.

Both HIAB and OUTSCAN offers easy to use and cost-efficient functionality for assessing web applications including both application and server layer scanning.

Figure 3: The HIAB Solution in Conjunction with the OUTSCAN Solution



Sources: Outpost24, 2011 and Frost & Sullivan, 2011

“Frost & Sullivan believes that Outpost24’s HIAB solution offers an appropriate mix of strong functionalities such as the ability to scan web applications and ease of use.”

Frost & Sullivan believes that solution can meet the need for both internal and external scans in accordance with best practice. The main benefit of the HIAB solution is the appropriate mix of security functionality and ease of use, as outlined below:

- **Privacy:** The solution offers a high level of privacy through its ability to store vulnerability information on the device. The organisation avoids the risk of having its vulnerabilities stored on the vendor's server (or in a third party data centre) – only the organisation has access to its own vulnerability data. This alleviates the organisational concern about controlling sensitive data.
- **Ease of use and deployment:** HIAB can be easily deployed due to its plug and play function. It is easy to use, and it can be configured to run at defined intervals or on an ad hoc basis. In addition, it can run without any implications for the user in terms of system access, speed, etc.

HIAB and OUTSCAN is a strong and highly cost efficient choice for large and mid-sized organisations that want to remain secure, and perhaps is faced with having to comply with legislations such as PCI DSS through the following:

- **High levels of privacy:** Strong privacy functionality by storing vulnerability data on the device.
- **Leading technology:** Leading vulnerability technology that enables strong scanning performance in terms of low false positive incidents and discovery tools that enable automated evaluation of all endpoints. Excellent coverage for web related vulnerabilities on application and server level.
- **Flexibility and openness:** Broad range of support for various operating systems, applications, browsers and network types and an open architecture enabling good integration capabilities.
- **Ease of use:** Intuitive web-based user interface, familiar to the user and therefore requires limited training to operate.
- **Scalability:** The solution supports an unlimited number of users and enables central management for several appliance clusters. This enables the organisation to reduce operational costs. In addition, the permission control system can be managed by groups for ease of use.

“The HIAB solution's main selling points are the high level of privacy, ease of use/ deployment and cost effectiveness.”

Case Study: HIAB Enables Simple Vulnerability Management in Grupo Salinas

Grupo Salinas has always been proactive in keeping its network secure. However, as the business grew, this task became ever more complex requiring the architecture team to run four different scans which generated an enormous amount of false incidents. As a result, the team needed to take action to remain secure in a simpler and more efficient manner.

The most important criteria for the new vulnerability management solution were as follows. It had to:

- Cover all layers of security, from patches that may not be fully installed to major system faults;
- Be easy to use; and
- Support the team to become more efficient by reducing the number of false incidents and help simplify work processes.

After considering several solutions, Grupo Salinas selected a combination of Outpost24's HIAB and OUTSCAN solutions. The decision was based on Outpost24 solutions' abilities to:

- Detect vulnerabilities at all levels.
- Be easy to use.
- Help the team simplify and centralise processes by enabling one scan for the entire organisation due to its ease of integration with various systems.
- Produce a limited number of false incidents through an automated report system, therefore enhancing efficiency.
- Avoid taking up larger shares of the system capacity when operating, enabling users to run the solution without any implications for other systems.
- Provide flexibility by being delivered via a security as a service model, enabling Grupo Salinas to run the scan anytime, anywhere.

After successfully deploying the solutions, Grupo Salinas realised additional benefits. The HIAB solution was easy to deploy. The company is now only paying for one tool as opposed to the previous four, contributing to lower costs. The team is satisfied; they no longer have to waste time analysing long lists of false incidents and can instead focus on critical tasks, and devote more time to other projects.

Grupo Salinas believe that the HIAB and OUTSCAN solution is an optimal choice for the organisation because it contains a good balance between ease of use and relevant functionalities. The organisation remains secure in a cost efficient, simple and effective way, as all the benefits expected have been realised – the HIAB solution has even provided additional ones.

About Grupo Salinas

Grupo Salinas owns a range of retail, banking and communication enterprises in terms of the following brands: TV Azteca, Azteca America, Grupo Elektra, Italika, Banco Azteca, Seguros Azteca, Afore Azteca and Iusacell. The group operates in Mexico and across six Latin American countries with these 8 brands.

Case Study: British American Tobacco Meets Efficient, Affordable and Flexible Vulnerability Management

The rise of worms and malicious code and the downtime and expense they bring has prompted British American Tobacco (and other organisations) to focus on vulnerability management. The desired result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems reduce or eliminate the potential for exploitation involve considerably less time and effort than responding after an exploitation has occurred. As a result, the IT Architecture and Security team put a business case together to purchase a new tool to help them mitigate the risks of unwanted attacks. The team needed to find a cost efficient, easy to manage and highly effective solution.

British American Tobacco opted for Outpost24's HIAB solution. The solution provides network mapping support. It is based on proprietary technology; enables cross platform support; maintains network availability; is aligned with the CVE standard and facilitates a multi user environment. British American Tobacco chose the HIAB solution to due to the following benefits:

- Cost efficiency;
- Scalability;
- Strong support;
- Flexibility; and
- Advanced technology (both internal and external and the CVE standard).

After deploying HIAB, British American Tobacco has reaped more benefits than initially expected. The HIAB has proven to be cost efficient in terms of enabling higher productivity. All team members can manage and use the solution anywhere across the entire global network. Furthermore, HIAB enables the team to perform scans without having to deploy and run HIAB in several locations, therefore increasing productivity.

The flexible design of the solution has helped the company to utilise the solution exactly to the purpose intended. British American Tobacco needed the solution for specific projects, as opposed to on a weekly basis, (for which the HIAB solution can also be configured). While the solution has proven to possess the scalability expected it has also been easy to deploy and run.

The HIAB solution is ideal for British American Tobacco. It enables the company to manage its IT infrastructure security risk in an efficient and affordable manner. It ticked all the boxes the company needed: cost efficient, productive and scalable. Furthermore, it provided additional benefits that have further enhanced the value proposition of the solution.

About British American Tobacco

British American Tobacco is the world's second largest tobacco group, with products sold in more than 180 countries. With a portfolio of more than 250 brands, it has 50 cigarette factories in 41 countries. 1 in 8 cigarettes smoked globally are from British American Tobacco's portfolio.

CONCLUSION

Having compared the HIAB solution with organisations' security needs, Frost & Sullivan believes that Outpost24's solution provides the following benefits:

- Cost efficiency, enabled by a low number of false positives and centralised management and operations;
- Scalability;
- High level of privacy by storing data on the device inside the organisation's network;
- Flexibility in terms of being easy to integrate with different systems and the ability to enable scans anytime, anywhere;
- In line with CVE standards to effectively communicate with users;
- Advanced technology enabling scan of all layers of the system including web applications; and
- Ease of use and deployment.

The HIAB solution is well placed to help large and mid-sized organisations remain secure, as it offers both internal and external scans in accordance with best practice. Furthermore, it stores the organisation's vulnerability data directly on the device, eliminating concerns relating to third party storage.

Frost & Sullivan believes that the HIAB solution is a strong cost efficient vulnerability assessment and management solution due to its good mix of functionality and ease of use.

ABOUT OUTPOST24

Outpost24's on-demand vulnerability assessment and management solutions are used by over 1,000 corporate and government customers worldwide, including Travelex, Europcar, Delta Lloyd Group, ING Life Limited, Deutsche Postbank, Arcelor Mittal and Banco Multiva. Outpost24 is headquartered in Sweden with a global network of local sales offices.

Outpost24 delivers security solutions in a Software-as-a-Service (OUTSCAN® & OUTSCAN PCI®) or Appliance (HIAB®) form factor. Outpost24's solutions provide fully automated network vulnerability scanning, easily interpreted reports, and vulnerability management tools. OUTSCAN PCI® is the ideal tool for businesses of all sizes to achieve and demonstrate PCI DSS compliance.

Outpost24's solutions can be deployed in a matter of hours, anywhere in the world, providing customers an immediate view of their security and compliance posture.

Outpost24 – Vulnerability Management Made Easy

For information, please contact:

Outpost24

Bastionsgatan 6A
371 32 Karlskrona
Sweden

Telephone: +46 455 612 300
Fax: +46 455 13 960
Email: info@outpost24.com

CONTACT US

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

Oxford

4100 Chancellor Court
Oxford Business Park
Oxford, OX4 2GX, UK
Tel: +44 (0) 1865 398600
Fax: +44 (0) 1865 398601

London

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

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

enquiries@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan is a global growth consulting company with over 47 offices across the world. We have been partnering with clients to support the development of innovative strategies for 50 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies and the investment community by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics and demographics. For more information, visit <http://www.frost.com>.

For information, please contact:

Frost & Sullivan

Sullivan House
4 Grosvenor Gardens
London SW1W 0DH
UK

Telephone: +44 (0) 207 343 8383
Fax: +44 (0) 207 730 3343