PROTECT YOUR IT ASSETS: ENHANCING PATCH, REDUCING SECURITY VULNERABILITY AND OPTIMISING ASSET MANAGEMENT

Executive Summary ▶

The consequences of overlooking even a single security vulnerability can be severe. If a computer on the enterprise network gets infected with malware or is exposed to a root exploit, it can be expensive to fix, expose client details and/or intellectual property and may also prevent users from being productive while the problem is being addressed. Staying on top of security vulnerabilities and compliance requirements in today's complex IT environments requires tools that can automate the checking processes and increase visibility.

Traditionally, enterprise IT Security Management (ITSM) tools have been one of the most common ways to provide such monitoring and management capabilities. However, the cost of these enterprise management solutions is high both in terms of software licenses and the extra cost of specialised administrators as well as the training needed to take full advantage of the tools.

threeisquared
Infrastructure Insight Meets Innovation

www.threeisquared.com

Executive summary ▶

Some businesses have chosen to avoid these high costs by instead using point solutions for their most important ITSM needs and augmenting the tools with manual tracking and reporting methods. While this is a cost-effective way to enable some ITSM capabilities such as patch and asset management, it also puts a greater burden on IT support teams because of the manual steps involved.

Fortunately, there are other options and this whitepaper focuses on how I-Insight can be used to achieve the following business benefits:

1. Reduced exposure to risk — Proactive management of assets and an automated rule checking processes will help reduce the risk that security vulnerabilities will go unnoticed.

2. Greater efficiency — The integrated approach saves time and resources through automated checking of servers during each data collection. This means that the view of any exposure is current and doesn't drift from the real picture over time as spreadsheets do.

3. Expedited issue resolution — The visibility offered by I-Insight expedites resolution of security vulnerabilities or patching. A task can be assigned to an individual Systems Administrator (SA), enabling a controlled measurable workflow and visibility of progress toward resolution.

4. Greater management control — Managers can have real-time visibility of all of the vulnerabilities each server is exposed to, as well as the speed with which they are resolved. Audit and compliance requirements are also simplified through flexible reporting on status of assets, software licenses, etc.

Introduction ▶

To manage IT assets and properly understand patch levels and security risks, IT support teams need to have easy access to the latest configuration and status information for all of the organisation's servers. In some cases, there are thousands of systems to monitor, making manual methods of tracking this information too inefficient to be practical.

IT support teams also need to work efficiently, and that requires real-time visibility into the following types of information for every system:

1. The location and ownership or responsible party for all hardware and software components

2. All software components installed

3. The currently installed patch levels for the operating system and key software components

4. The latest security and update patches that have been made available from OS software vendors or internal engineering departments but not yet installed

These capabilities can be provided by a cloud-based patch and asset management environment, but in most cases, this is not enough. The patch and asset management solution can identify vulnerabilities, but provides minimal oversight for their resolution. When patch and asset management is integrated into a single tool, ownership is assigned as soon as an issue is identified, enabling issues to be tracked with the kind of visibility and control that assures proper and timely resolution.

WHY USE I-Insight? ▶

Unlike complex enterprise management tools that include many capabilities that IT support teams won't use, the approach of single highly focused operational tool such as I-Insight provides the visibility and control needed to stay on top of security vulnerabilities without the high cost for software licenses or the extensive training that is often associated with enterprise management solutions. Tools used for this purpose need to be able to be scaled quickly and cost-effectively as the IT infrastructure grows and I-Insight has previously worked in extremely large enterprise environments.

Using a highly focused operational tool enables a comprehensive approach, giving IT support teams the ability to:

1. Manage and track servers, in all data centers globally

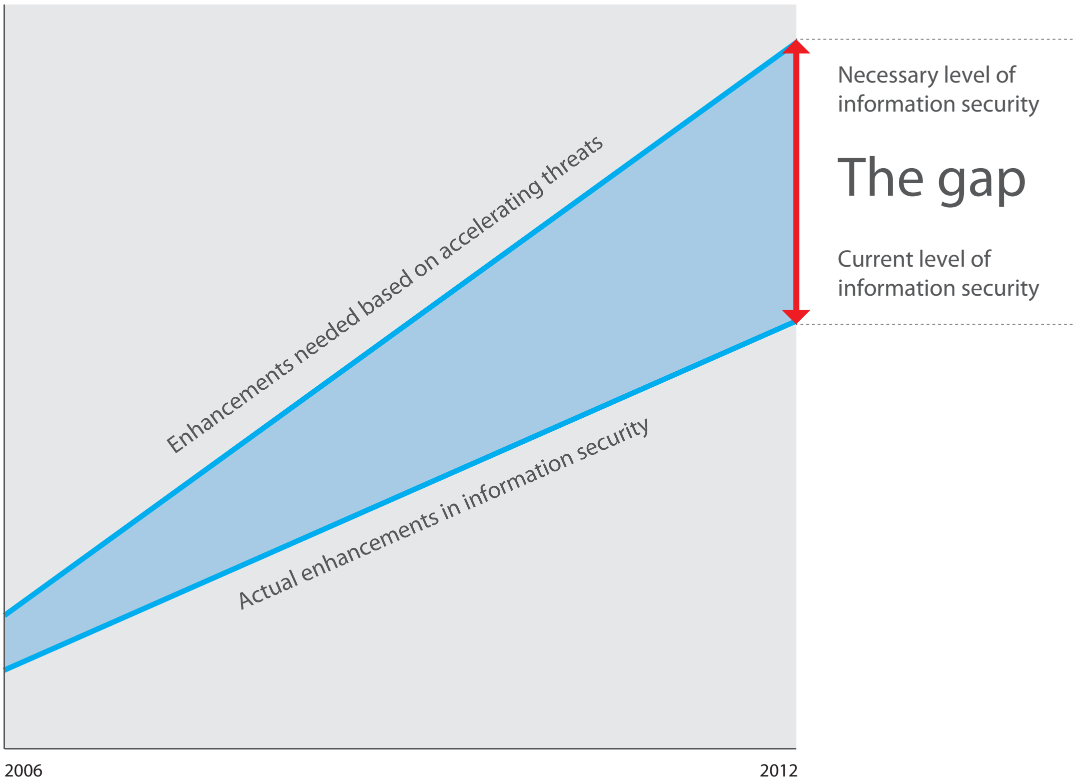
2. Track patching against an engineered or vendor build

3. Monitor a single view of status information that presents a high-level as well as an individual server level view

Managers can also use the reporting capabilities to watch trends over time or to monitor for improvements after making process changes. For example, it may be useful to monitor trends in metrics such as the number of outstanding issues for a particular OS, time to resolution, and number of high severity issues. Patch and asset management tools don't generally provide this visibility into aggregated data for monitoring trends.

Reducing risk of security vulnerabilities ▶

A 2012 report by Ernest and Young shows that more needs to be done in all organisations to address the risk from security breaches and vulnerabilities



To keep server based security vulnerabilities under control and reduce risk, organisations need two different kinds of IT management capabilities. IT support teams need the right tools to identify security vulnerabilities, and a way to assign these vulnerabilities to individuals to track and manage each issue so that vulnerabilities get fully resolved in a timely manner.

A best-of-breed tool for patch and asset management such as I-Insight can simplify the process of identifying vulnerabilities because the tool is designed just for that purpose.

For example, an automated scan can be run at regular intervals and set up to identify the following types of vulnerabilities and bring them to the attention of the IT support team:

1. Systems that have missed patch updates for known issues

2. Systems that have missed patch updates for security vulnerabilities

3. Systems that are out of step with engineered builds

4. Systems that have known configuration weaknesses

5. Systems without proper password protection

For maximum efficiency, it's best if this kind of information can be presented graphically. This allows IT support teams to quickly identify the most urgent issues and also easily find the server(s) that need attention.

For Example: A security exploit is found on a particular version of Samba, which allows root access and is remotely exploitable. This is an enormous security risk and needs to be resolved as soon as possible. In a large environment finding out where Samba is installed and which servers are exposed to this exploit is a complex problem, which requires many pieces of information to be combined to get a complete picture of the exposure. The use of automated checks rather than a static spreadsheet will allow the real-time tracking of progress and the assurance that the vulnerability has been completely resolved.

Improving the efficiency of IT support teams ▶

In addition to reducing the risk of vulnerabilities, an operationally focused solution such as I-Insight also helps IT support teams work more efficiently, thus reducing support costs. The proactive scanning of all servers within an organisation enables IT support teams to cost effectively monitor the environment for more complex scenarios than those normally handled by standard monitoring tools with very little manual effort.

Detailed data about the system can be automatically collected through an agent less collection routine, providing context and technical details that can be very useful to IT support teams. Crucial information such as the platform OS and version, installed application(s) software, hardware information, and even a link to remote access consoles can give IT support teams a head start because they have immediate access to all the information they need as soon as they inspect the servers details. In addition, the tool will continue to collect more information after the vulnerability is remediated. Thus if the status of a server changes for the worse causing the same problem to be an issue again, identification is immediate and automatic.

Automated collection of device status information is especially helpful for user-initiated tickets. When users call an IT hotline, they often lack a basic understanding of IT terminology and may have difficulty explaining the issue to the IT support teams. In many cases, the user may not even know what operating system or applications a server is running. An operational focused tool such as I-Insight collects all of the pertinent information about a system and can make communication easier for both users and IT support teams.

Expediting issue resolution ▶

Once an issue or vulnerability is discovered, whether automatically or by a user, the tracking of resolution can be managed through a configurable automated workflow that helps speed up resolution and minimize risk.

Using an operational focused tool such as I-Insight aids and expedites resolution by:

1. Identifying an owner and tracking each issue
2. Providing automatic escalation for issues that do not get addressed in a timely fashion
3. Improving management visibility into how well IT support teams are doing at resolving issues
4. Tracking progress on outstanding issues.

Operations in action ▶

The capabilities described in this whitepaper are not just a theoretical vision about the future. A cost-effective operationally focused tool is available today from threeisquared and the techniques described in this whitepaper have already been used in very complex infrastructure environments utilising thousands of servers with great success.

About ThreeiSquared ▶

Threeisquared is a leading provider of innovative operationally focused tools to improve the management and visibility of a large infrastructure server estate. Learn more about I-Insight and threeisquared please visit us at **www.threeisquared.com**