



One of the world's largest accountancy firms now has a better view of their IT Security Risk thanks to Flexeye's Dashboard solution.

Accountancy firm can count on its IT Security

Managing IT security is a serious responsibility. Even more so than when you are managing the infrastructure for a company that offers IT Security Management and Risk Management solutions to their customers. So when the IT Director at one of the world's largest accountancy firms took on the task, he did so with an eye on improving efficiency. He didn't realise the process would, over time, fundamentally change his entire approach to managing IT security.

The company appeared to have effective security solutions and processes in place including: asset and patch management, virus protection and intrusion detection among others. What it lacked, however, was a way of measuring the effectiveness of these tools in improving the company's security posture.

MULTI-VENDOR INCOMPATIBILITY

The firm had one solution for patch management and anti-virus protection for their servers and a different one for their desktop assets. They were also working with Symantec™ Managed Security Services to manage their network intrusion detection systems remotely.

Each of these systems had reporting capabilities of their own, but none produced

reports compatible with the other vendors. Furthermore, each product's reports were generic and it wasn't immediately clear how to translate the results into something meaningful to the business.

The team did use the information from these systems, but found that collecting, adapting, combining and reformatting took a lot of their time. As a result, reports of the company's security posture were expensive and infrequent.

DELIVERING IMMEDIATE VALUE

The firm knew that if they could cost-effectively increase the frequency of these reports, they could better manage their security resources. Knowing exactly which machines, operating systems, applications, networks or locations that present the greatest risk to the company would enable them to focus on problem areas. But waiting until the end of the reporting period to measure results and reset priorities wasn't good enough: they needed daily, not quarterly, reports.

Flexeye recommended a solution powered by the Flexeye Engine, to put it all together and speed things up. After capturing the accountancy firm's requirements and building a tailored IT security dashboard, Flexeye's security expertise and rapid development capabilities soon paid off, delivering an extraordinary amount of business value from the very beginning.

Flexeye's security expertise and rapid development capabilities delivered an extraordinary amount of business value.

REAL-TIME REPORTING

The firm uses an in-house classification scheme to assess the vulnerability status of any given device.

Grade-A machines have been:

- Updated with all the approved application and OS patches
- Updates with the latest virus definition file and have had a full virus scan performed

- Reviewed by the company policy scanner to ensure they comply with all requirements.

This makes it easy to spot serious IT security risks on the network. By encoding details of the company's in-house scheme into the Flexeye solution, the firm can generate real-time reports in an appropriate and user-friendly format without the need to make changes to internal processes or nomenclature.

THE THREAT OF ZERO-DAY EXPLOITS

With the reporting issues resolved, Flexeye focused on the next stage of the solution, which was to improve the company's patch deployment.

Patch deployment is now more critical than ever. IT security managers used to have weeks or even months to patch newly discovered software vulnerabilities before cyber attackers were able to exploit them for mischief or criminal activity. Today, viruses can be developed and spread across the Internet almost as quickly as the weaknesses themselves are reported. Software vendors have responded by producing patches more quickly and more frequently. However, these rapid and frequent patches have little value if companies cannot deploy them just as efficiently.

Through the Flexeye Engine the company were able to get a complete view of the patch status of their assets, but soon noticed that some machines patched more quickly and others took longer, despite being managed by the same

automatic patch deployment tools. Flexeye worked with the firm to provide a clear picture of why.

By noting the location date and time for each asset as it is patched, Flexeye helped the firm visualise, nearly in real-time, the deployment of the latest released patch across all of their locations. They can now quickly identify bottlenecks in the process and get those systems patched before they become security problems.

THREAT BAROMETER

Knowing that an ounce of prevention is better than a pound of cure, the firm wanted to explore ways of stopping threats getting into the network in the first place. So, working with the Flexeye team, the firm integrated Symantec's Firewalls and Intrusion Detection Systems (IDS) into the Flexeye solution.

Symantec's managed security service uses advanced event correlation technology to spot important security events—often external attacks—on the company's perimeter. Daily reports are sent to key staff outlining the previous day's events. These reports are useful in themselves, but by plugging them into the Flexeye Engine, the daily results become powerful tools. Results for any previous day are available for review or comparison, and more importantly, the results can be displayed as trends over time. This enables the firm to monitor the level of external threat pressure against their boundaries, as well as the overall effectiveness of their perimeter security controls.

AN INDISPENSIBLE TOOL

The Flexeye Engine has become an indispensable tool that presents security data from multiple sources in a meaningful way, and introduces new, derived information that the team couldn't even see before.

Thanks to Flexeye's support, advice and solution, this leading accountancy firm has had the opportunity to gradually transform and continuously improve the way it manages IT security.



For more information please visit www.flexeye.co.uk