BAE Systems gains visibility into endpoints to reduce risk and defend against security threats

BAE SYSTEMS

Industry
Aerospace, Arms industry,
Information security

Size
90,500 employees

Headquarters
London, United Kingdom

Tanium solutions
Tanium Core, Endpoint
Management,
Risk & Compliance,
Incident Response

Applied Intelligence, a business within BAE Systems now known as Digital Intelligence, needed visibility into its fleet of laptops, virtual machines (VMs) and other digital endpoints. The group's leaders knew that what you can't see, you can't protect.

Digital Intelligence had thousands of devices that it wanted to be able to scan for potential vulnerabilities. With this information, the team would know whether any of their endpoints were vulnerable to ransomware, computer viruses and other hostile attacks. The IT & Security teams also sought an effective way of quarantining or otherwise remediating infected systems should an attack occur.

> "Without the visibility that Tanium supplies, we wouldn't be able to grapple with the ever-presentsecurity threats."
>
> **Tom Barker**
> Chief Security Officer of BAE
> Digital Intelligence

The Tanium solution

To achieve this solution, the BAE Digital Intelligence team brought in Tanium. Founded in 2007, Tanium offers software solutions that can find unmanaged endpoints, scan for vulnerabilities, manage and control compromised devices, and more. Tanium's solutions are used by half the Fortune 100, eight of the top 10 financial institutions, and five branches of the U.S. military.

The implementation of Tanium was assisted by Tanium's technical experts, who worked closely with the IT & Security teams at Digital Intelligence. Together, they installed the Tanium platform, trained employees to use it, and crunched the numbers generated by Tanium's software. "

Results and benefits

The first scan using Tanium identified a number of potential vulnerabilities, including out-of-date patches, open ports and more. Within a matter of months, the team used Tanium to significantly reduce these vulnerabilities. In the following months, the team further reduced the number of remaining vulnerabilities to within the business's risk threshold. "Even though there's been an increase in the number of endpoints we deploy,and we are fighting against a continual tide of newly released CVEs [common vulnerabilities and exposures], our overarching vulnerabilities and risk posture have remained low," Whibberley says.

BAE Digital Intelligence also benefited fromthe huge amount of time they were able to save. Prior to implementing Tanium, the Digital Intelligence team compiled a monthly report of potential cyber vulnerabilities. The report was compiled manually, a process that took more than two weeks each month. Now, with Tanium implemented, the vulnerabilities report is generated automatically and provided weekly.

Thanks to Tanium, the business is safer,and more efficient. If and when a vulnerable endpoint is identified, the device's owner is requested to remediate the issue in a set number of days. "Now our users are responsible for keeping their VMs patched", says Whibberley.

That's been a real cultural change for the BAE team. "Our engineers and IT staff are security-savvy, but at first, they didn't see what was in it for them," Barker explains. Now Tanium lets them see individual systems in detail. That kind of granular data shows individuals why it's relevant for them. "Tanium lets us connect the dots, and really improves our security posture," Barker adds.

A future capability, now being developed, will empower the IT team to quarantine a system using Tanium, ensuring thatany potential compromise is blocked from spreading across the company's network. That way, the IT and Security teams will not only have greater visibility into their endpoints, but also the ability to manage them.

TANIUM.

The Power of Certainty.™

Visit us at **www.tanium.com** and follow us on **LinkedIn** and **X**.

© Tanium 2025