CASE STUDY

Barclays: A Platform for the Future

How Barclays Improved IT Ops and Security with the Tanium Communications Architecture

With more than 300,000 endpoints across 40 countries, Barclays was dealing with a plethora of point tools, patch management challenges, and a frustrated incident response team. The Tanium platform allowed the organization to consolidate all those point tools, find an effective way to manage patching, and speed up incident response time to minutes.

Since the 2008 financial crisis, global banks have faced increasing regulatory pressure across all aspects of their business. Barclays, the world's seventh largest bank with 48 million customers worldwide and more than $2.42 trillion in assets, is no exception. Against the backdrop of CBEST, the Bank of England's vulnerability test, and other regulatory requirements, Barclays decided to invest in new tools to enhance the speed, agility, and scalability of their security response.

In 2016, they turned to Tanium. Barclays' IT leaders were impressed by Tanium's promise to provide clarity and management over their vast network of more than 300,000 endpoints across 40 countries. They also needed a complete solution that could interoperate and drive performance of existing security tools. Since acquiring Tanium in July, they haven't looked back. "Operating on a global scale provides a lot of challenges when it comes to knowing your environment," said Troels Oerting, Group Chief Security Officer at Barclays. "For the first time, we've been able to get a fast and accurate picture of our environment with Tanium."

Tanium Use Cases

- Security Hygiene
- Endpoint Detection & Response

Challenges

- Visibility and control at global scale
- Time to detect, contain, and remediate security incidents
- Patch deployment measurement and completeness
- Endpoint tool sprawl and the need for consolidation

Benefits to IT

- Speed up security incident remediation to just minutes
- More complete patch deployment than previously possible through real-time measurement
- Confident in visibility and control over 300,000 globally distributed endpoints
- Improved line-of-business confidence and reduced costs

One Platform to Unify Them All

Barclays suffered from a common problem facing large businesses: too many tools performing specialist functions with limited interoperability. Beyond the lack of coordination, these tools often produce data that is hours, days, or even weeks old.

Tanium's platform provides a sensor and actuator capability across the vast majority of compute endpoints operated by Barclays. This means Tanium can make other security tools smarter by providing timely and context-rich data.

Another attribute of the Tanium platform is its ability to take future growth into account. Barclays can utilize Tanium's simple deployment platform to add new security tools in a matter of clicks, compared to the significant engineering and implementation efforts required for a traditional bespoke approach.

Working in the Dark

The team at Barclays diligently patch their Windows Server estate, yet the process is not always smooth. If compatibility issues are encountered, server performance could degrade—or even worse, an outage might occur. Of course, patching is a critical activity in order to actively secure their environment and prevent attackers from leveraging software vulnerabilities.

Historically, the team had to wait until the end of the deployment run before they could measure the success or failure of the patch deployment. With Tanium, a patch deployment is measured in near real-time, so any server compatibility issues are immediately detected and remediated.

Incident Response in Minutes

Barclays Cyber Incident Response team needed to gain visibility into potential threats, query by any artifact, scope an incident, and remediate in near real-time across their entire environment—visibility and reactivity that was not possible before Tanium. Previously, the team could take several hours to gather logs before hunting could begin. Post-Tanium, the Barclays team can go directly to the log source—the endpoint itself.

This speed at scale has led the IR team to develop entirely new processes for handling threats. Thanks to Tanium, Barclays is able to see and address issues in near real-time, speeding up the remediation process to just minutes and significantly reducing the risk of negative impacts to the organization.

Working with Tanium to Design for the Future

While Barclays has already adopted multiple product modules to date, the team looks forward to adding Tanium Comply to help meet regulatory requirements. Tanium Comply's ability to expose endpoint vulnerabilities will help with software inventory and risk analysis.

Enabling a Tanium module is as simple as clicking a button, and doesn't require costly deployment. This will allow Barclays to efficiently expand and develop the platform to meet specific needs as they arise. Since the general operation of Tanium's platform is consistent across modules, Barclays expects to save time and money on retraining staff as it continues to add Tanium modules over time.

In a short time, the bank has already seen tremendous benefits not only for their IT security teams, but also for their business. They've trimmed costs and boosted customer confidence in their ability to protect data.

About Us

Tanium is a unified endpoint management and security platform proven in the world's most technically demanding organizations. Providing unparalleled speed, visibility, and scale, we serve half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces, which rely on Tanium to make confident decisions, operate efficiently, and reduce risk. Tanium recently ranked 7th on the Forbes list of "Top 100 Private Companies In Cloud Computing For 2019," 10th on FORTUNE's list of the "100 Best Medium Workplaces" in the U.S., and 18th on the UK's Best Workplaces list. Visit us at www.tanium.com or follow us on LinkedIn and Twitter.

TANIUM