CASE STUDY

TANIUM

AutoNation speedily addresses hygiene and improves endpoint security

AutoNation

Tanium use cases

- Cyber Hygiene
- Incident Response
- IT Operations Management

Challenges

- Limited visibility — getting environmental information took days
- Hundreds of thousands of missing patches – some dating back to '07
- Many machines were missing six or more critical patches
- SCCM agents broken on large percentage of machines
- Long delays to update patches and inability to ensure all patches were completedd

Benefits to IT

- Real-time visibility and greatly reduced incident response times
- Patching success rate of over 99 percent and faster time to patch systems
- Assessed SCCM presence and fully deployed enterprise wide
- Overall increased IT administrative productivit

"When we got full visibility across our entire environment we discovered we had a significant problem with patch currency that wasn't visible using our previous tools," said Ken Athanasiou, CISO for AutoNation.

Visibility and patching challenges for the largest auto retailer in the U.S.

AutoNation employs about 26,000 people in over 300 locations nationwide. Although all of AutoNation's locations are connected to a central IT network, the company had struggled to meet the CISO's patching expectations. As a result, critical patches weren't getting deployed in a timely manner and objectives were not being met. Ken's team knew they had a problem; however, Tanium allowed them to see how big the problem actually was and to track in real time the effectiveness of remediation activities.

AutoNation first used Tanium to deploy a large scale update of Microsoft BitLocker (a disk encryption feature) across its environment – and do it within 30 days – the AutoNation team was skeptical that it could be done in that timeframe without massive manpower resources. Leveraging the skills of the Tanium Technical Account Management team and the extensible capabilities of the Tanium platform, AutoNation accomplished the deployment on schedule without additional manpower requirements. This success saved AutoNation tens of thousands of dollars just for this effort and demonstrated the potential of Tanium's unique capabilities within AutoNation's environment.

Patching

Using Tanium, the AutoNation team accomplished a comprehensive cyber hygiene assessment that validated the suspected patching deficiencies of the existing software deployment process. This confirmed that the current management tools were less than fully effective. In fact, hundreds of thousands of patches had not been correctly applied, including some dating back to 2007. Additionally, 91 percent of endpoints had an outdated version of Adobe Flash. "We can now get real-time answers from our entire environment in seconds," Ken said. "In my career, I've never seen this level of real-time visibility." With more than 300 locations dispersed across the country, it has been tricky to push through patches effectively. Using Tanium, AutoNation is now able to deploy patches at a first pass success rate of over 99 percent.

> “In my career, I’ve never seen this level of real-time visibility.”
>
> **Ken Athanasiou**
> CISO, AutoNation

SCCM

AutoNation also utilized Tanium to increase the effectiveness of Microsoft SCCM (System Center Configuration Manager). After pairing Tanium with SCCM they discovered that SCCM was not fully functioning on a large percentage of the environment. The AutoNation team used Tanium to remediate this issue by re-deploying the SCCM agent to the non-responsive endpoints. Victor Pena, Client Architecture Engineer at AutoNation, was highly impressed by Tanium’s speed throughout the process: “SCCM would take sometimes an hour or two just to deploy a package to a user’s machine. Now we can type in that machine and deploy in minutes. That’s how the operations team here at AutoNation got onboard.”

Improving current endpoint security

Jeff Johnson, Information Security Operations Director at AutoNation, has also leveraged Tanium to help improve the company’s endpoint security strategy. Implementing a new third-party anti-virus (AV) software would normally take months to install on all of AutoNation’s 20,000 machines, with Tanium, the team was able to do it in four days.

In addition to deployment capabilities, Tanium helped with incident response time. “When we got to an infected workstation, the previous AV software was either broken or corrupted through a bad installation,” Jeff said. “Tanium allows us to quarantine suspect or infected machines for remediation. This has reduced our response time to less than an hour rather than days and better yet, we no longer need to send an engineer out to the store.”

Future use cases

As part of their continued focus on advancing their cyber security functions and capabilities, the AutoNation team has continued to leverage Tanium to explore and deploy new use cases and processes that would have been difficult or even impossible without the platform. One that Jeff is most excited about is Tanium Comply: “The new Comply module is going to be revolutionary. Tanium provides near real-time visibility to determine compliance with auditors’ ever-increasing regulatory requirements and immediately satisfy auditors requests.” Tanium Comply checks endpoints against standard security benchmarks and vulnerability definitions, providing near instant results enterprise-wide. Armed with these complete results, organizations can improve overall security hygiene and simplify preparation for audits such as PCI, HIPAA, and SOX.