TANIUM™

SECURE POINT OF SALE DEVICES
ADVANCED CYBER DEFENSE AT THE SPEED OF BUSINESS

TO DEFEND POS DEVICES AGAINST THE LATEST ATTACKS, YOU NEED TO KNOW WHAT'S TARGETING THEM NOW, ACROSS ALL OF YOUR LOCATIONS, AND REMEDIATE WITHIN SECONDS.

Considering the release of targeted malware such as BlackPOS and Backoff, IT security pros at some of the largest retail firms across the world are in a race against time. They need to find, fix, and investigate any and all threat indicators on POS devices before they have a chance to make an impact on the business.

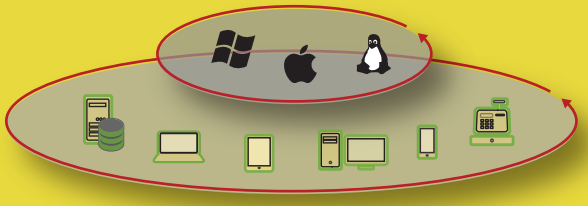
Hiding in plain sight. The malware that targets POS devices can easily bypass traditional security controls such as anti-virus, and can remain in place long after the initial installation. The longer it remains in place, the more credit cardholder data it can steal… so moving quickly is essential.

The need for speed. And precision, at scale. IT security pros need tools that can automate key aspects of threat detection, investigation, and remediation. Additionally, they need to know with certainty and precision which devices have been compromised, no matter how distributed their network. Fixes need to be applied within seconds in order to combat device compromise and data leakage, even at scales as high as hundreds of thousands of endpoints.

Traditional approaches are no longer sufficient. Legacy security tools that rely on cumbersome and brittle client-server architectures just can't keep up with the pace of these POS attacks. To make matters worse, they're also very costly and difficult to maintain, and can't accommodate the dynamic nature of today's advanced threats.

Thankfully, Tanium delivers instantaneous threat detection and remediation for all of the endpoints in your network, including POS devices. Within seconds, Tanium can hunt for the presence of hundreds of indicators of compromise (IOCs) across all your endpoints, delivering the instant visibility and control that IT security pros have long needed.

Support for Windows, Mac, and Linux
across laptops, desktops, servers and other devices.



Customer Spotlight

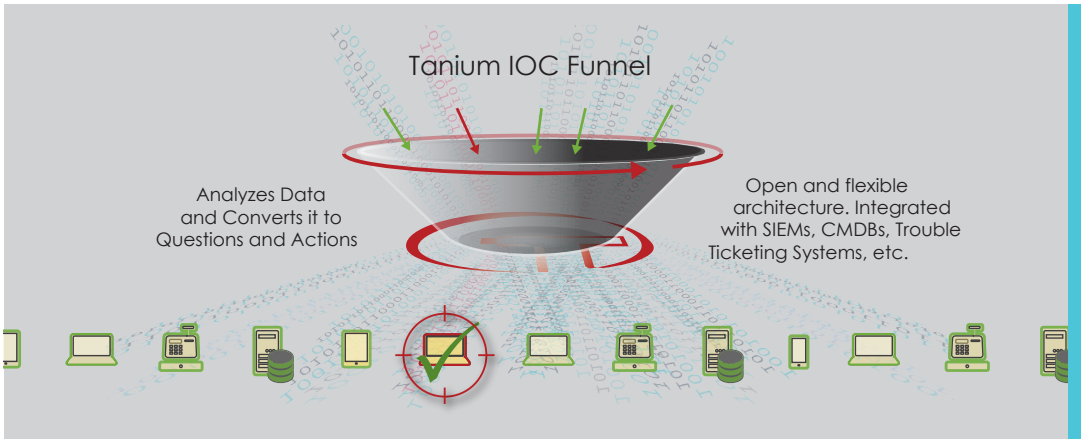
A large global retailer was struggling to pinpoint and resolve a malware outbreak they discovered in one of their South American offices. Out of 15,000 endpoints connected to that office, they guessed that 2,000 were infected, and their IT security team struggled to contain the outbreak. They were in a race against time, and their existing toolset had a stalled engine. With Tanium, they were able to verify the infected machines within minutes, quarantine them, make registry repairs to roll-back the threat tem- porarily and then push out an updated DAT file once it was released from their AV vendor.

TANIUM IOC DETECTION: HOW IT WORKS

Tanium provides advanced cyber defense by automating the hunt for IOCs, containing and investigating threats and executing remediation at scale. Powered by the Tanium Platform, the Tanium IOC Funnel ingests IOCs in a variety of formats such as OpenIOC, STIX, and Yara and then scans the entire enterprise – across all of the endpoints – returning results in seconds. Seconds later, Tanium pinpoints compromised endpoints, and then executes remediation at the same speed.

Unlike other enterprise technologies, Tanium doesn't rely on a centralized, hierarchical server infrastructure to provide data collection, aggregation, and distribution. It is based on an efficient, patent-protected, linear peer-to-peer communications topology designed for fault tolerance, transient endpoints, and the global WAN segments typical of today's retailer networks.

Through a lightweight and adaptive agent, Tanium exchanges management intelligence and key compromise data directly with the computing devices themselves. This key innovation results in radically faster, more accurate, scalable, and more adaptive security than traditional solutions. Delivering the highest value at the lowest TCO, a single Tanium server can manage 500,000 endpoint devices, resulting in a level of resilience and efficiency not possible with alternatives.



Key Features

- Gathers live results from hundreds of thousands of endpoints in seconds
- Uses a single server to support 500,000 endpoints vs hundreds of servers with incumbent solutions
- Detects attacker behavior as well as malware
- Supports more industry standard IOC formats than incumbents, including OpenIOC, STIX and Yara
- Integrates with your existing enterprise security infrastructure (SIEM, GRC, CMDB, and more)
- Consumes IOCs from any internal source or external threat intelligence provider

TANIUM™

1625 Shattuck Avenue, Suite 200
Berkeley, CA 94709

info@tanium.com
www.tanium.com