DATA SHEET

Tanium + Google Chronicle

Enterprise-class Unified Endpoint Security (UES) paired with massively scalable, cloud-native security analytics

The ideal solution combines an enterprise-class platform for endpoint security with a best in breed solution for telemetry storage and analytics at a predictable and affordable cost.

Sophisticated attacks are often long lived

Although less common than the average incident, advanced persistent threats (APT) are harder to detect, potentially more costly, and much longer lived – often leading to 200+ days of dwell time. APTs penetrate networks through targeted and difficult-to-detect means including spear phishing, credential theft, or web app vulnerabilities. Once inside, they use native operating system functions, credential dumping, and human error to opportunistically seek higher value targets and data. These types of attacks can be extremely damaging and difficult to remediate.

In these cases, incident responders struggle with a lack of sufficient historical data. The prevention and investigative tools in their arsenal seem archaic in comparison to the offensive techniques they seek to counter. Mean time to recover suffers, regulatory fines mount, and customers lose confidence.

Why existing EDR point solutions miss the mark

The security industry is flooded with a myriad of Endpoint Detection and Response (EDR) point solutions. These tools might achieve adequate defense against many attacks. However, no solution can detect or prevent every attack – especially against a long-lived APT. And if your organization is unfortunate enough to face one, EDR telemetry becomes too limited both in terms of scope and volume – usually maxing out at 7-30 days. EDR point solutions also fail to provide the flexibility needed to search for threats previously unknown and therefore, not recorded. And EDR point solutions typically don't provide necessary remediation of the compromise such as deploying a required patch or correcting a misconfiguration.

Thus, many organizations often pivot to try to store historical endpoint telemetry in a security information and event management (SIEM) solution – outside of their EDR tool. This approach provides the added benefit of enabling the correlation of multiple forensic sources of network and endpoint telemetry for analysis (i.e., XDR). What most organizations then discover is that for high-volume endpoint telemetry, SIEM becomes too costly or requires cold storage that might take weeks to search – time that responders can't wait in the case of an incident.

A better approach is needed. The ideal solution combines an enterprise-class platform for endpoint security with a best in breed solution for telemetry storage and analytics at a predictable and affordable cost. Enter the partnership between the Tanium platform and Google Security Operations security analytics, powered by Google infrastructure.

The new endpoint security model

Tanium and Google Cloud have created a transformational partnership to bring together expertise along multiple dimensions of distributed computing. A critical aspect of distributed enterprise endpoint security is the ability to detect, respond, and recover from security incidents with speed at scale.

Through the partnership the Google Security Operations platform is pre-integrated with competitive pricing from Google for long term storage. The best-in-class integration solves the problems of endpoint security with unmatched speed, scale, and efficiency.

Tanium and Google Security Operations work in harmony to accelerate detection, minimize disruption, and provide the ability to investigate and scope long-lived attacks captured from one year of telemetry.

Alert

Accelerate time to detect with proactive alerting on full endpoint state, historical telemetry, and network event correlation.

Hunt

Find unknown mallicious activity through live enterprise-wide questions and across petabytes of historical telemetry.

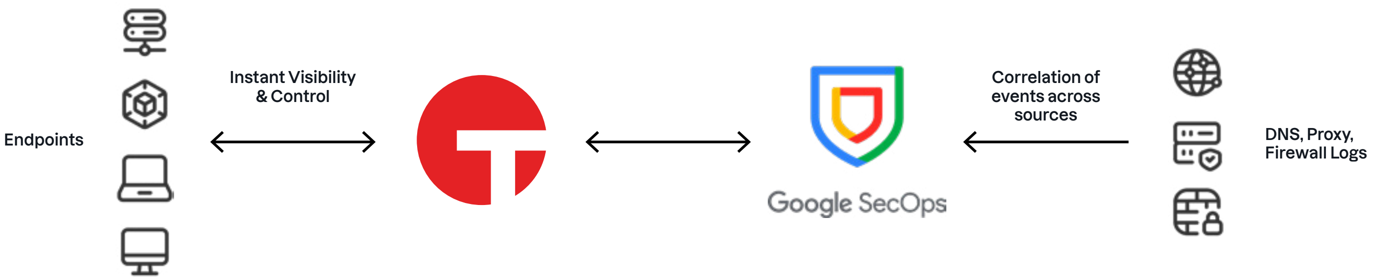
Investigate

Collect evidence and scope long-lived attacks using live data and over 1-year of historical telemetry.

Remediate

Minimize disruption and impact to the business using powerful endpoint control from Tanium.

Minimize Disruption by accelerating and improving detection & Response


Endpoints
Instant Visibility & Control
Google SecOps
Correlation of events across sources
DNS, Proxy, Firewall Logs

Tanium benefits

Converged platform: One platform for end-to-end endpoint management and security

Identify the unknown: Find unknown endpoints, sensitive data, and identify lateral movement risk

Improve hygiene: Find and help eliminate vulnerabilities and misconfigurations in a single solution

Visibility, control, speed at scale: Alert and remediate based on a patented architecture

Google Security Operations benefits

Disruptive pricing: Google offers competitive pricing for long term storage — please contact Google for details

Infinite elasticity: Backend built on core Google infrastructure

Instant search: Find indicators across full year of security telemetry to uncover latent threats

Cloud-native: Built to auto-scale and eliminate data management overhead

Business benefits of the combined solution

Reduce risk

Maintain one year of historical telemetry to safeguard and enable incident response teams in the case of a long-lived attack. Improve overall endpoint detection and response with a proven, enterprise-class Autonomous Endpoint Management approach.

Increase resource effectiveness

Flexibility and speed to adapt to new threats or remediate at scale. The ability to correlate endpoint telemetry with network sources (DNS, firewall, proxy) to achieve XDR.

Reduce costs

Cost-effective cloud-native storage backed by Google infrastructure provides a more efficient, scalable, and robust model for security analytics and telemetry storage. Remove the need for a multitude of endpoint agents using the single agent architecture of Tanium for Autonomous Endpoint Management and security.

TANIUM

The Power of Certainty.™

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