Tanium for Unified Endpoint Security (UES)

A fast, flexible, and end-to-end solution for securing end-user, server, and cloud endpoints at any scale.

More security doesn't mean better security.

Organizations have continued to layer endpoint tools into their security stack in an attempt to defend against ever-evolving cyber threats and meet privacy regulations. These siloed point solutions make the IT environment more complex to manage without fundamentally improving security to the organization. Vulnerability assessment tools fail to provide results at the speed needed to remediate critical issues completely. Next-generation prevention products help by incrementally improving detection, but there remains no focus on recovery.

Why is it that despite more budget, tools, and focus, most organizations still struggle with the basics of hygiene, much less more advanced security tasks like detection and response? 71% of organizations lack end-to-end visibility of endpoints and their health.[1]

Endpoint security needs a new approach that begins with immediate visibility into every endpoint. Such security also requires a unified platform that connects end-to-end security with a modern endpoint management architecture. This architecture should inevitably bring teams together, streamline workflows, and shorten the time to investigate.
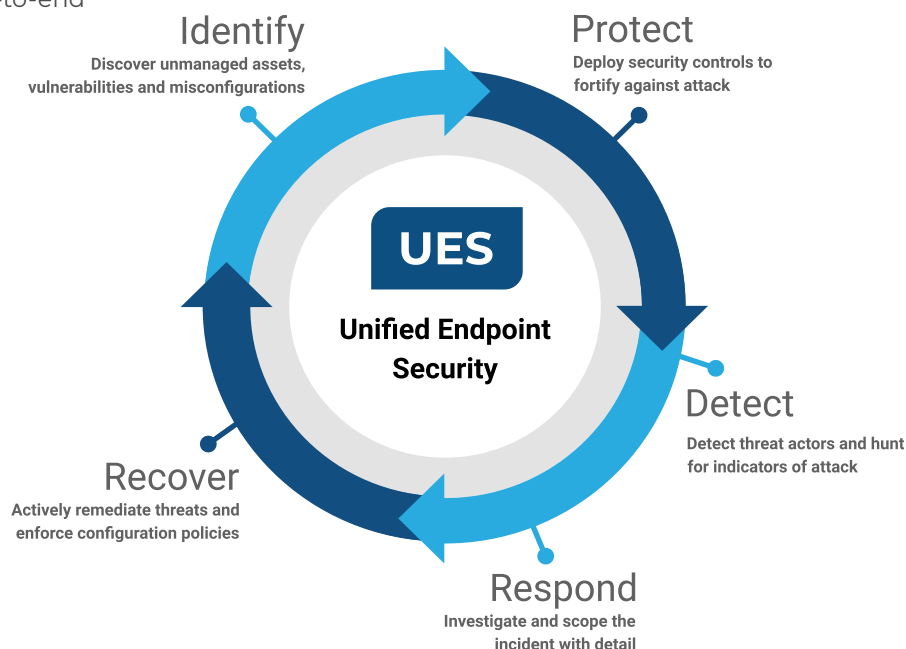
Rethink the endpoint with Unified Endpoint Security (UES).

Unified Endpoint Security (UES) is the process for securing and fortifying all of an organization's endpoints from a unified platform. It allows security teams to identify, protect, detect, respond to, and recover from threats affecting cloud and virtual instances, servers, and end-

user devices running both legacy and modern operating systems.

UES doesn't rely solely on black box solutions, which eventually become obsolete as attacker techniques evolve. What it does is help better control the full stack of security operations that includes managing technologies and monitoring the environment for compliance. In addition, UES enriches the data used for correlating activities between endpoints and other data sources, such as application logs or network events.

UES is a continuous approach to security management and must align with common frameworks, such as the NIST Cybersecurity Framework. UES starts with identifying endpoint assets, then building a complete attack surface inventory. A UES solution must also link critical endpoint security activities in order to identify and remediate security gaps, such as software vulnerabilities. It also serves to protect the endpoint through required controls, including antivirus or disk encryption. Finally, UES facilitates the detection, response, and recovery from threats in the environment.

Identify
Discover unmanaged assets, vulnerabilities and misconfigurations

Protect
Deploy security controls to fortify against attack

UES
Unified Endpoint Security

Detect
Detect threat actors and hunt for indicators of attack

Recover
Actively remediate threats and enforce configuration policies

Respond
Investigate and scope the incident with detail

[1]Forrester. (2019). Strained Relationships Between Security And IT Ops Teams Leave Businesses At Risk.

Tanium for UES: Security in one place.

Providing unparalleled speed, visibility, and control, Tanium is a unified endpoint management and security platform built for the world's most technically demanding organizations and IT teams. Unlike the plethora of endpoint security point solutions currently available, Tanium's approach to UES prioritizes solving the underlying conditions that contribute to organizational risk, beginning with a solid foundation based on full endpoint visibility and control.

Tanium starts with a modern, patented architecture. Built to provide full endpoint management at any scale, the architecture provides a powerful foundation for endpoint security. It effortlessly supports millions of endpoints and maintains optimal performance, without the need for ongoing investment in costly hardware. Tanium is also well-suited to withstand the effects of today's dynamic environments, in which machines constantly move on- and offline and infrastructure as a service (IaaS) virtual machines come and go by the hundreds or thousands.

As a result, Tanium covers critical requirements of security and risk management and a breadth of endpoint types, supporting security operations, engineering, and analyst teams through:

- **A single view** of all end-user, server, and cloud endpoints.
- **Real-time data** that informs immediate business decisions.
- **One endpoint agent** for integrated management and security to fortify endpoints against threats
- **An extensible and flexible platform** that adapts easily to new threats and vulnerabilities.
- **A bridge from SecOps to operations** that aligns teams around a single set of data.

Execute on all pillars of the UES lifecycle with one platform and console.

- **Asset Discovery & Inventory:** Discover managed and unmanaged assets as well as multi-tier application services to provide a complete inventory instantly.
- **Endpoint Detection & Response:** Detect, react, and recover quickly from attacks and resulting business disruptions.
- **Vulnerability & Configuration Management:** Identify and measure risks with immediate and comprehensive vulnerability and configuration assessments.
- **Data & Risk Privacy:** Identify and manage sensitive data at rest across every endpoint.

Realize game-changing security benefits with Tanium for UES.

- **Improve Asset Inventory:** Many organizations discover 10 to 20 percent more endpoints other operations tools failed to identify.
- **Ask Any Question:** Move more quickly and comprehensively to scope an issue or incident through natural language queries to understand what's going on with your endpoints right that minute.
- **Reduce the Attack Surface:** Improve first-pass "zero-day" patching efficacy from 60 to 99+ percent.
- **Improve Recovery Time:** Speed things up from weeks or even months to hours by deploying recovery actions, patches, or other software updates to remediate at any scale.
- **Eliminate Many Point Tools:** Consolidate multiple endpoint security functions with one, flexible agent designed to continually keep up with the security measures and threats of tomorrow.

UES Unified Endpoint Security

- Vulnerability & Configuration Management
- Endpoint Detection & Response
- Data Risk & Privacy
- Asset Discovery & Inventory

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