UpGuard vs. Tripwire

UpGuard™

Introduction

Primarily known for its change tracking capabilities as applied to intrusion detection, Tripwire's core technology powers security, configuration management, and compliance features in its flagship offering: Tripwire Enterprise. An early pioneer of intrusion detection techniques, the company has been primarily focused on cyber threat detection and security configuration management (SCM) for medium to large enterprises. A barebones, open source version of their product is also available for free download, as well as a free Windows configuration utility called SecureCheq.

Tripwire—like many enterprise security suites—tries to cover a broad range of industry scenarios with its offering. Various add-ons and extensions are required for building a customized solution; subsequently, one should allocate significant budget to acquire various components of the solutions suite. One can certainly download the free, open source version of their product, given the requisite expertise for set up, configuration, and maintenance is available. That said, implementing a free tool based on a decades-old codebase (also used in the enterprise offering, no less) to protect one's mission-critical assets may not be for the faint of heart.

Following the company's recent acquisition by Belden, a strategic objective was made to expand Tripwire's footprint into industries such as broadcast, industrial, and manufacturing— sectors in which Belden has been entrenched in for years. This move may further isolate current and future customers as the product becomes more generalized to address these new market sectors. Furthermore, as Tripwire continues to evolve based on its large enterprise and marquee customers' wish lists, one questions whether the offering will remain viable for SMB/ mid-market and medium enterprise customers.

In contrast, UpGuard provides comprehensive, continuous security testing and monitoring with a fraction of the budgetary, personnel, and systems/network resources required by Tripwire. Application servers, cloud services, network devices, databases-- everything with a configuration state is a possible point of failure—and thus a node type supported by UpGuard. The platform provides a unified view of them all to guard against both malicious and unintentional configuration changes.

Background: **Tripwire**

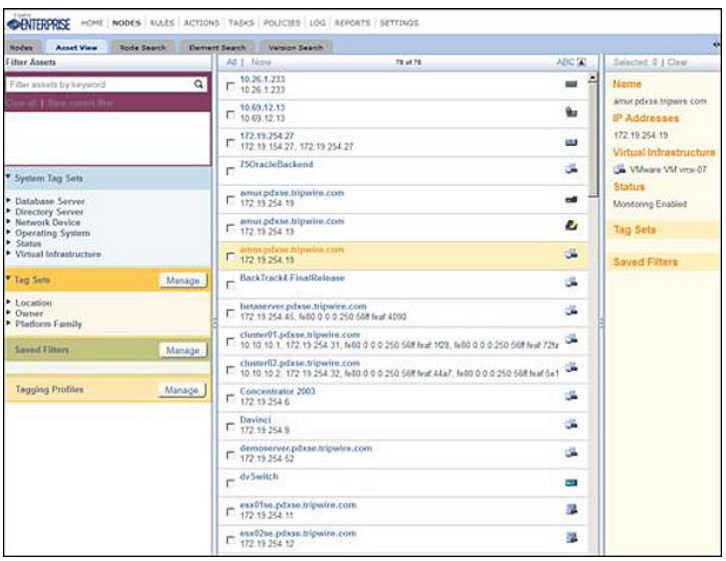
Tripwire was created in 1992 as a free, open source configuration management (CM) tool for Unix platforms. Commercial versions of the tool followed soon thereafter, with Tripwire Enterprise arriving on the scene in 2005. As the company's flagship offering for over a decade now, the solution forms the basis of a suite of interrelated products, each targeted for specific uses like vulnerability management, compliance, and log/event management.

Tripwire's Core Technology

Tripwire works by creating a baseline—a snapshot of critical files and directories in a known secure state—by calculating the hash values for the items and storing them in a database. It then compares the system's current state to the baseline continuously and reacts to any modifications changes accordingly such as triggering alerts/notifications.

A Patchwork of Acquired Solutions

Tripwire acquired information risk and security performance management solution provider nCircle in 2013. Though the merger ostensibly combines the pair's offerings to create a best-of-breed product, in reality these scenarios usually result in convoluted and complicated solutions, especially when combining solutions that weren't made to work with each other. In 2014, Tripwire was acquired by Belden, a leading manufacturer of networking and cable products. The deal was initially catalyzed by a joint venture between the two companies to create solutions for infrastructure/ cyber security in manufacturing organisations. With its parent company deeply focused and entrenched in a handful of vertical markets, it's safe to say that Tripwire Enterprise will follow suit, at least in part-- with development and feature enhancements catering to industrial and broadcast customers.



Tripwire Enterprise

Tripwire

Tripwire's flagship product is supported/augmented by a range of complementary and value-added solutions. The following comprise its current suite of offerings:

- Tripwire Enterprise — the company's flagship security configuration management and threat detection solution.
- Tripwire Configuration Compliance Manager (CCM) — for discovering and auditing configurations for compliance purposes.
- Tripwire Data Mart — processes and analyzes control data to drive business intelligence.
- Tripwire IP360 — vulnerability assessment for risk management and compliance.
- Tripwire WebApp 360 — web application vulnerability scanning.
- Tripwire PureCloud Enterprise — cloud-based vulnerability scanning.
- Tripwire PureCloud for PCI — cloud-based vulnerability scanning featuring PCI DSS 3.0 compliance requirements.
- Tripwire Security Intelligence Hub — customizable dashboards and automated risk reporting.
- Tripwire Log Center — provides extended log and event management capabilities.

Background: **UpGuard**

UpGuard was founded in 2012 by industry veterans to address contemporary IT needs such as continuous security testing/monitoring, configuration drift remediation, and infrastructure visibility and discovery. UpGuard was born-in-the-cloud and supports current paradigms such as DevOps, Agile, and continuous integration/delivery.

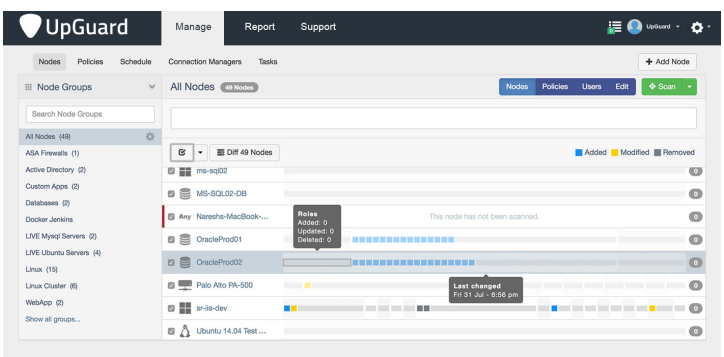
As the complexity of IT infrastructure grows, maintaining a system of record becomes both more challenging and more necessary. While older solutions struggle to adapt, UpGuard introduces a holistic platform for system state visibility.

UpGuard's Core Technology

The platform uses an agentless connection manager to retrieve and document the configuration state of every managed node. These records can be differenced against each other for diagnosing configuration errors—the root cause of 80% of outages. More importantly, UpGuard continuously tests infrastructures and environments through both user-defined policies and an OVAL-based vulnerability suite to ensure quality from development to production. And after a successful deployment, UpGuard captures infrastructure requirements from the current desired state to avoid regressions and maintain consistent baselines.

A Complementary Security Platform

Unlike legacy, monolithic solutions such as Tripwire, UpGuard plays well with other solutions, allowing one to custom tailor a security toolchain based on their organization's unique needs. Furthermore, the platform's RESTful API allows it to be extensible and easily integrated with any number of 3rd party tools available. UpGuard excels in providing vulnerability assessment and monitoring at every phase of SDLC—and can even provide validation that the security mechanisms therein are indeed optimally configured and working as expected. When integrated into an organization's security framework, UpGuard provides end-to-end security overwatch capabilities, ensuring that quality and security are baked in every step of the way.



Collaboration View in UpGuard

UpGuard

UpGuard's comprehensive solution for continuous security monitoring and testing tracks and monitors servers, network hardware, cloud services, web apps, infrastructure, and more.

- Configuration Management
- Continuous Deployment
- Continuous Integration
- Change Management
- Infrastructure Monitoring
- Application Monitoring
- Performance Monitoring
- Software Defined Networking
- Log Analysis

Side-by-Side

	UpGuard	tripwire
List Price	Priced per node-- general pricing is available on website. $6-12 per month, per node.	Pricing not publicly available.
Ease-of-Use	Everything can be accomplished through one platform and interface. Minimal training is necessary.	Can be difficult to use; a web-based GUI for simplifying management is available. Significant expertise for tuning is required to minimize false positives and noise.
Deployment Model and Architecture	SaaS, single-tenant instance, or on-premise virtual appliance.	Saas, cloud (limited to solutions like Tripwire PureCloud Enterprise), on-premise Integrity monitoring requires extensive using the platform's agent-based architecture.
Node Types	Servers, network devices, cloud apps, websites, databases, major cloud providers (AWS, Azure) and more.	Servers, network devices, cloud apps, websites, and more.
Target Customers	SMB to large enterprises-- can be used with the simplest to most complex configurations and environments.	Mid-to-large enterprises with substantial budgets to cover software costs, support, and professional services. Customers in regulated industries are primary targets.
Time Required for Setup	Can be set up quickly to return information that is at once actionable.	Takes considerable time to configure and optimize: expect to spend 4-8 weeks for average implementations. Feature requests can take 24-30 months with extensive support.
Updates	Continuously updated (SaaS)	Per version -- current release is 8.4. Patches are also available to address issues between releases.
Language(s)	None required.	None required.
Integration/API	REST; integrates with other RESTful web services.	SOAP API
Documentation	Available online	N/A
Automatic creation/archival of current and previous security baselines	Yes	Yes
Comparison / differencing of security baselines	Yes	Yes
Comprehensive Vulnerability Assessment with OVAL	Yes	Yes/limited in Tripwire Enterprise.
Tasks Tracking and Auditing	Yes	No
Output to CM/automation solutions (Puppet, Chef, etc)	Yes	No
Documentation	Available online	User guides and manuals (PDF) available after purchase. Documentation lacks visuals like screenshots and diagrams.
Support	Free, unlimited support during regular business hours; 24-hour support also available.	Paid-for support options available.

Key Differentiations

Complexity of the Solution

Today's enterprise infrastructures are complex. No one tool can comprehensively address this complexity—instead, the most effective solutions focus on their core competencies and integrate with other solutions to fill out the security toolchain. UpGuard excels in integrating with other leading tools while focusing on state visibility the basis for a strong security posture. Furthermore, it provides the collaboration mechanisms for aiding continuous integration and configuration management—features absent in legacy tools like Tripwire. This "best of breed" approach allows for integrating the best tools from multiple leading vendors into one solution, as opposed to buying into one monolithic solution stack from the same vendor. The platform's RESTful API makes integrating with other tools a trivial affair. Tripwire uses the older, less-flexible SOAP for connecting to 3rd party packages; integrations are possible but require the assistance of professional services.

In aspiring to be a monolithic all-in-one solution, Tripwire Enterprise has instead become highly complicated and unwieldy. Its myriad of interacting components make it extremely network-resource intensive, which can be alleviated in part through the use of agents. As such, Tripwire Enterprise is primarily an agent-based platform. UpGuard uses an agentless connection manager to retrieve and document the configuration state of every managed node. Those records can be differenced against each other to diagnose configuration errors—the root cause of 80% of outages. More importantly, UpGuard continuously tests the state of your infrastructure and environments, both through user-defined policies and through an OVAL-based vulnerability suite, to ensure quality from development to production.

Baked-in product and pricing complexity is a revenue opportunity for Tripwire. Professional services comprise a significant portion of their business, and paid support is only available to customers. UpGuard support is free; furthermore, extended support for the enterprise is also available. In general, the platform's simple and intuitive interface empowers most users to get up and running on their own fairly quickly with minimal/no assistance. By supporting collaboration and an open, integrated toolset, UpGuard enables faster and more secure delivery of higher quality software.

Tripwire Enterprise's suite of offerings and respective pricing models are difficult for potential customers to traverse and comprehend. In contrast, UpGuard is straightforward: the offering consists of a single platform, and pricing is simply per node.

Effectiveness of the Solution

Tripwire has not been without its own security flaws. 2001's Symbolic Link Attack* and 2004's Format String Vulnerability** are just two examples of prominent Tripwire vulnerabilities discovered over the years.

UpGuard monitors and assesses vulnerabilities against MITRE'S OVAL— the preeminent, community-maintained repository of vulnerability definitions. This makes response and remediation an accurate, less resource-intensive affair and allows for quicker closure of security gaps. Tripwire Enterprise offers only limited support for OVAL.

A security platform is ineffective if it generates so many false notifications that operators become accustomed to ignoring them. As a complex, difficult-to-manage solution, Tripwire becomes burdensome to work with and leaves users less inclined to track down suspicious changes when notified.

Key Differentiations

Long-Term Visibility

Tripwire is a legacy IDS product, augmented and updated over the span of its existence to address contemporary issues in security and accommodate new IT service delivery models like the cloud. UpGuard was born-in-the-cloud and built with contemporary design patterns, methodologies, and paradigms such as DevOps, Agile, and continuous software delivery. Furthermore, UpGuard's agentless model significantly reduces maintenance overhead and network noise, in contrast to Tripwire Enterprise's noisy, difficult-to-manage agent-based architecture.

Tripwire's prior acquisition of nCircle—coupled with its recent acquisition by Belden— may result in an increasingly complicated and difficult-to-use product. A strategic drive to address the needs and concerns of the parent company's target verticals may lead to overspecialization of the offering.

Integration capabilities are critical to customers for getting the most out of their software investments. UpGuard includes integrations with its platform at no cost; in contrast, Tripwire Enterprise integrations are paid-for services engagements that are cost prohibitive to most customers.

Pricing and Implementation Cost

Tripwire's licensing can get expensive, as pricing is per component. For example, the management console license must be purchased as a separate component. Implementation can take weeks and feature requests are for the most part unavailable to average customers. UpGuard requires very little to start, with benefits realized almost immediately. A proof of value deployment takes a few hours over one week to complete and on average 3 months to recuperate initial investments.

Tripwire's overall cost of ownership is extremely high, especially after additional products and extensions, training, support, and professional services are accounted for. UpGuard uses a straightforward pricing model that makes costing easier and more accurate. Furthermore, everything required to run UpGuard comes standard, out-of-the-box.

Even after initial pricing has been determined, unforeseen future licensing costs for additional features can again make costing a complicated affair. For example, an additional fee is required for the appropriate solution to implement PCI compliance monitoring. Even items that one would think come standard (e.g., the management console GUI) must be purchased individually. With UpGuard, all required parts comes standard with the SaaS or on-premise virtual appliance.

Conclusion

Tripwire utilizes legacy core technologies to combat new security vulnerabilities, and is costly and complex to acquire, configure, and manage. And though a competent and mature SCM tool, the Tripwire offering has had its own share of critical vulnerabilities. On the other hand, UpGuard can scan for and identify problems like vulnerabilities, open ports, configuration changes, and drift quickly and cost-effectively— with minimal baked-in cost and complexity.

In short, there's no doubt that in the past Tripwire has been a competent solution for SCM and enterprise threat protection. However, yesterday's methodology for effective cyber security is history; today's threat landscape requires an integrated and dynamic best-of-breed approach that combines ongoing monitoring for vulnerabilities with collaborative remediation. To this end, UpGuard provides lightweight security testing and monitoring for bolstering enterprise security postures against current and future threat landscapes.

Source(s)

* Symbolic Link Attack
On Linux/Unix, Tripwire opens insecure temporary files with predictable names in publicly-writable directories. Using a symbolic link attack, a local intruder may overwrite or create arbitrary files on machines running tripwire.

** Format String Vulnerability
When an e-mail report is created, a local user can execute arbitrary code that runs with the same rights as the user running the file check (usually root or sysadmin).

http://www.scmagazine.com/tripwire-enterprise/review/3498/

http://www.linux-magazine.com/Issues/2014/163/Tripwire-IDS

http://www.slideshare.net/LOGONSoftware/tlc-overview-26263051

https://www.sics.se/~amir/files/download/slides/ids.pdf

http://www.riskmanageworks.com/Tripwire-Log-Center.asp

http://linux.about.com/cs/linux101/g/tripwire.htm

http://searchsecurity.techtarget.com/magazineContent/Intrusion-Detection-Tripwires-Enterprise-50

http://www.pcworld.com/article/2030489/tripwire-acquires-ncircle-to-form-new-security-giant.html

http://www.iiisci.org/Journal/CV$/sci/pdfs/P101422.pdf

http://www.slideshare.net/dhananjay5315/tripwire-44629995

548 Market Street #38076
San Francisco, CA 94104
+1 888 882 3223
hello@UpGuard.com
UpGuard.com