FORTRA™

WHITE PAPER (TRIPWIRE)

Tripwire Axon: Foundational Endpoint Intelligence

The Future of IT Operations, Security, and Compliance

Today's agile enterprises need to adapt quickly to business digitalization and new IT models, ensuring availability while controlling risk. What is constant is change. Organizations can control and adapt to expected changes like system virtualization, cloud deployment, IT/OT conversion and endpoint device acceptance. However, they have less control over unexpected changes that could hamper their operations that come from attacks and exploited vulnerabilities. Organizations require platforms and technologies that can adapt and provide resilience to both these expected and unexpected changes.

Digital capabilities and responding to new IT models are now a prerequisite to compete in the long term. Yet many companies seeking to go digital are still unclear about the best way to set up their IT organizations, manage digital information, and establish and maintain online services and automated processes. One technical challenge is collecting the relevant data from all parts of the enterprise. While organizations may have a large volume of data, they are still not collecting complete data, or in some cases not collecting data at all, from the many endpoints in their environment.

This paper focuses on the technology and limitations that prevent the successful utilization of endpoint intelligence in IT operations, compliance, and security and how they can be overcome with intelligent innovations. It will detail specific problems enterprises have securing their IT systems, what technology innovations Fortra's Tripwire has made in data collection and communications, and how these problems are resolved with this technology.

A current perception is that there is a data management problem: too much data. But, in reality, there is a data collection problem. Data collection can be categorized by volume and flow. An example of inappropriate volume are silos of data that are focused on a particular tool or business unit that don't allow the collaboration or integration needed to piece together a response to secure enterprises. Often multiple tools are collecting the same data from the same systems. Data collection flow is hampered by network "dark zones," where connections are intermittent, or communication is tightly controlled. Many organizations are also reluctant to install agents to every endpoint citing agent drag or performance concerns. Endpoints are also mobile, meaning they are not connected in the same manner or at the same IP as what might be expected.

Together these real problems with data collection reinforce the perception that there is too much data; there is not enough of the right data and there is too much agent management overhead.

What businesses have asked for is a common data collection and communication architecture that utilizes lightweight agents. A system that is resilient to network disruptions and can self-heal when changes or agent errors occur. A high-performance platform that is pluggable, extensible and secure. A solution that benefits IT operations, security and compliance with unparalleled visibility and cyber-resilience while reducing operational burden and improving responsiveness.

With Fortra's Tripwire Axon®, Tripwire has re-imagined what an endpoint data collection and communication platform must provide to support IT operations, security, and compliance. Simply put, the Tripwire Axon platform is a foundational agent technology and platform enabling flexible data collection and resilient communication across a broad range of devices, cloud, and virtualized assets.

The Tripwire Axon platform, a pioneering technology, addresses collection challenges utilizing an extensible and resource efficient agent, asynchronous messaging techniques, and product/platform neutral message definitions.

The Tripwire Axon platform starts from the premise that monitored data is not constant—it ebbs and flows as the computational needs of a business change. It realizes that networks are dynamic environments where connectivity is not guaranteed. An endpoint may not have the computational horsepower for heavy agents. To address these conditions, the platform introduces a new communication infrastructure to handle streams of monitored data. Tripwire products deliver the ability to derive actionable results from a stream of multi-faceted, highly detailed endpoint data.

Tripwire Axon storage requirements

- Initial storage requirements (not including spool storage) are: 135 MB for Linux systems and 330 MB for Windows systems
- The default Tripwire Axon agent spool storage maximum size is 1 GB, configurable down to 16 MB
- The lowest recommended spool maximum size is 100 MB

Tripwire Axon Components

The Tripwire Axon platform is composed of three main categories of components: the Tripwire Axon agent, Tripwire Axon platform services, and applications that utilize collected data.

Tripwire Axon Agent

The Tripwire Axon agent employs an extensible plugin design pattern where plugins run as separate processes managed by a central agent process. The combination of the central agent process with plugins is the Tripwire Axon agent. The agent uses a secure and efficient connection to the Tripwire Axon bridge—the aggregation point where load balancers may be introduced to handle individual stream redirection when loads change and networks fail. The Tripwire Axon agent initiates Transport Layer Security (TLS) connections to bridges, sending heartbeat keep-alive messages and spooling outbound messages during disconnected operations. Agent configuration is accomplished through a pre-configured bundle from Tripwire Enterprise, or through configuration files/DNS SRV records. The flexibility in configuration available helps to minimize human effort for manual installs while also providing the granular options demanded by teams who automate software deployments. The agent is responsible for maintaining a unique identity, represented using a Type 4 universally unique identifier (UUID).

The central agent process manages the Tripwire Axon agent plugin lifecycle through communications using Google protocol buffer messages over local transports. Plugins observe a strict start-up protocol through which capabilities are shared with the agent process and then announced to the bridge.

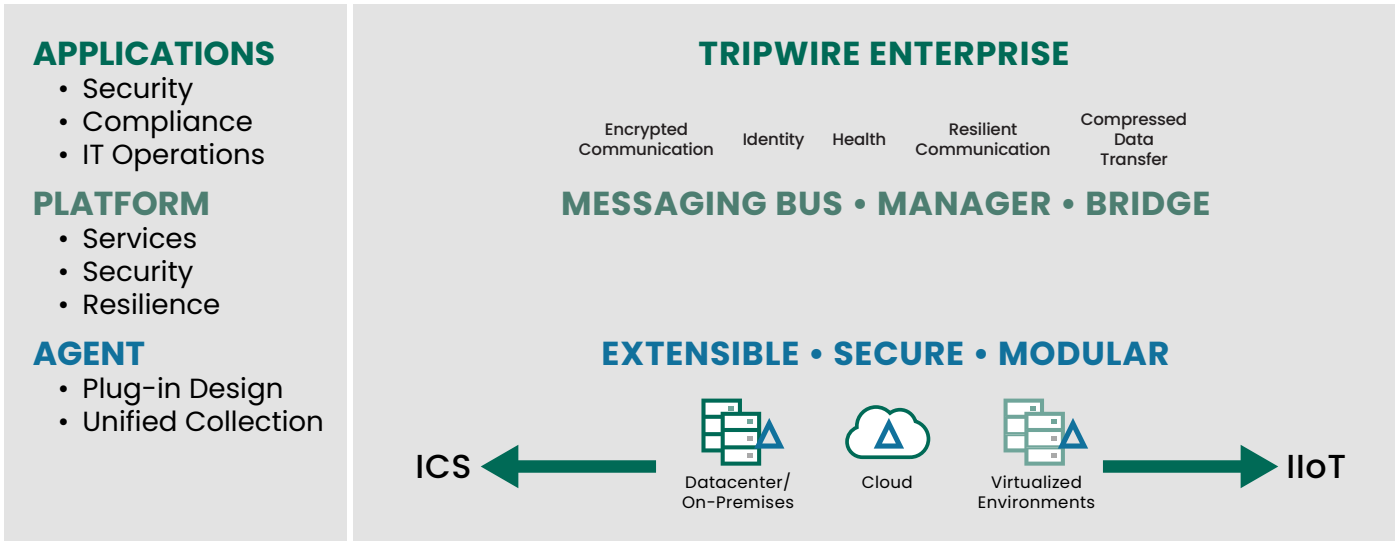
Optimized for minimal overall system resource utilization and network bandwidth, the Tripwire Axon agent and its plugins are designed to operate efficiently. The complete set of agent binaries is implemented in C++ to minimize footprint and maximize performance for their specific data collection objectives. The agent is packaged and deployed using native OS installers for AIX, Linux, and Windows.

Tripwire Axon Bridge

The bridge is the Tripwire Axon platform process which securely bridges communications from Tripwire Axon agents to consuming products such as the Tripwire® Enterprise Console through the broker. The agent and bridge use the Transport Layer Security (TLS) protocol and X.509 certificates to secure each connection. Tripwire Enterprise installations include the bridge. The communication payload between the agent and the bridge is batched, compressed, and serialized using Google protocol buffers to minimize message overhead and maximize network bandwidth efficiency. Communications between the Tripwire Axon agent and bridge support customer provided SOCKS5 proxies and Layer 4 load balancers.

Tripwire Axon Broker

The broker is a Tripwire Axon platform process implemented using Apache ActiveMQ, an enterprise-class open-source message broker. The broker serves as the messaging fabric



Tripwire Axon platform architecture

for communication and provides persistence for messages. This ensures that messages are delivered and recovered if either the console or agents are unavailable. The broker also supports cross-language clients. Each Tripwire Enterprise installation includes a broker.

Tripwire Axon Agent Manager

The Agent Manager is the Tripwire Axon platform process that manages Tripwire Axon agent sessions. It tracks agent availability, so Tripwire applications don't have to. The Agent Manager announces newly discovered Tripwire Axon agents and their associated capabilities, which allows products to dynamically discover Tripwire Axon agents and proceed with agent configuration. Each Tripwire Enterprise installation includes the Agent Manager.

Tripwire Axon Messaging and Capabilities

The Tripwire Axon agent messaging platform introduces a new powerful messaging abstraction called Capabilities. Implemented through Google's Interface Definition Language (IDL), Capabilities allow for the introduction of new platform collection features e.g., new plugins or completely new agents. The discovery and utilization of newly introduced Capabilities by Tripwire applications can occur as they are deployed. Conversely, new or existing products can be made aware of previously deployed Capabilities through content or product upgrades.

Tripwire Axon Security

The security of data streams is a core design element of the Tripwire Axon platform. The Tripwire Axon agent and the Tripwire Axon platform components employ standard 509.x certificates to achieve mutual authentications for all exposed network connections. An agent's encryption algorithms are always FIPs 140-2 compliant and cannot be downgraded through commands or configuration. The agent is strict about establishing trust as it builds a connection to its bridges. It both validates the bridge's certificate chain of trust and verifies the validity dates of all certificates in that chain before finalizing its connection. Tripwire Axon agent plugins and their associated shared libraries are cryptographically signed. Plugin signatures are verified upon agent startup; plugins failing validation are immediately terminated.

Tripwire Axon

- Unified modular platform to support the Tripwire portfolio, giving deep insight and flexibility
- Efficient and fast collection and access architecture for rich and broad data capture and aggregation
- Resilient and secure design for offline and connected data collection and transmission
- Extensible and scalable for emerging devices, services, and applications
- Lean and agile, consumes fewer resources while delivering vital functionality

Data Silos and Agent Infrastructure

Many believe that they have collected all the data from the critical assets and are only concerned about how to glean the actionable insights needed to respond to the latest threat or improve operational efficiency. However, the vast volume of data they have is segregated and redundant from the numerous tools often collecting the same data from the same systems. Gartner refers to this as "agent bloat," where each tool has its own collection architecture and collection agents.

These data silos are also expressed in data islands, where, due to business transformations, individual lines of business maintain their own IT. They get some tools from a central service bureau but often run unique IT operations and security tools. These tools do not share data easily with the rest of the business.

There is a tremendous variety in today's devices. Endpoints vary substantially in size and have different monitoring needs. The Tripwire Axon agent modular plugin design loads only the necessary plugins for the specific monitoring requirements of each system keeping endpoint memory and CPU footprint low. Plugins are loaded on demand and unloaded when they have no work.

The Tripwire Axon agent plugins may be written in any language appropriate for accessing required security data. Using Google protocol buffer messages between the central agent process and the plugin processes allows for this language-neutrality. The usage of protocol buffers in combination with the agent capability pattern provides boundary interfaces between agents, agent plugins, and Tripwire applications, upon which Tripwire will gain access to new sources and consumers of security data.

Network Dark Zones

Enterprise networks are more diverse and sophisticated than ever, often utilizing secure zones with strict communication requirements. Endpoints are highly distributed and may use lower bandwidth or unstable network connections. We refer to these network connection challenges as "dark zones" where data collection is not always consistent. For example, today's data centers have satellite sites, dynamic endpoint lifecycles and systems that may operate disconnected from the network or move around within the network for periods of time. Point of sale (POS) and other devices are often in remote sites with frail networks. Dark zone challenges include both connected and disconnected operations, providing robust and resilient data capture infrastructure that easily handles network outages, dramatic activity spikes, server maintenance windows, and even online/offline devices that operate with periodic network connectivity.

The Tripwire Axon agent's design allows for access into dark zones through efficient network utilization by batching and compressing messages, locally spooling them until they can be reliably delivered to the bridge. The Tripwire Axon agent, bridge and broker control data flow from end to end and can slow or halt message flow based on consumption rate. To increase message delivery reliability, when interruptions in the data stream are detected, the agent allows applications to request re-sending data from the agent spool.

When a device is disconnected or when a Tripwire Enterprise Console is down for maintenance, plugins continue to monitor and collect data, and data continues to spool. When a connection is reestablished, the spool system picks up where it left off and message delivery resumes. When an agent is disconnected for an extended period, the spool can become full by reaching its configured maximum. At this time, the agent orchestrates the shutdown of any running plugins, and agent activity is paused. When connection is reestablished and the spool begins to drain, plugins are reloaded and resumed. The agent interaction with the plugin allows it to record its state and resume the plugin from where it left off. The size of the spool is configurable to support hours, days, or weeks (or even longer) of disconnected operation.

The Tripwire Axon agent supports monitoring the following, real-time events from Windows and Linux kernels:

- File system changes
- Windows registry changes
- Updates to the contents of files
- Both streaming and differential
- User information
- Windows event logs
- Ability to capture the output of whitelisted commands

Because of the Tripwire Axon agent's modular plug-in design pattern, this list is easily expanded.

Endpoint Blind Spots

The costs of managing and maintaining agent-based systems sometimes overshadow the benefits and features these systems provide. For example, agents that are unable to self-heal from common disruptions, require constant monitoring, do not survive system upgrades, and consume valuable security and IT resources. IT departments are forced to choose between having to manage multiple agents or not getting the security visibility they need to protect their organization. Endpoints that are not covered due to software performance or host limitations represent "blind spots." These include embedded OSes and systems with lower computational power (like POS or ATMs)—critical assets that provide the least amount of endpoint intelligence.

Tripwire has considered the system's resources utilization to help minimize and rationalize its resource usage in the design and implementation of the Tripwire Axon agent. For example, the Tripwire Axon agent has facilities to load and unload plugins on demand, only consuming resources when there is a need for data collection, then returning CPU and memory resources back to the system for its primary mission. For those systems where disk storage is severely limited, the spool can be reduced to 16 MB.

The Tripwire Axon agent is packaged to handle server updates seamlessly to provide constant monitoring in the face of updates required to minimize system vulnerabilities. For example, when a system's Linux kernel is updated, the agent automatically selects the appropriate driver (using the kernel version) from a wide array of pre-packaged drivers. Alternatively, the agent can also adapt by utilizing Dynamic Kernel Module Support (DKMS) features.

The agent's automatic flow control feature provides dramatic capacity for peak loads and extreme spikes in monitoring activity. Consuming applications run at their own pace without having to be concerned about losing data during extreme loads. If data collection outpaces server processing capacity, the capture layer pushes back on agents to spool more data locally on the endpoints. When processing capacity is available and backpressure is reduced, data flow returns to normal—with no data loss.

Moving and Transient Endpoints

The unit of computation modularity is (and has been) shrinking rapidly, from multi-purpose bare-metal servers to single-purpose VMs, to single-process containers. Coupled with this trend of miniaturization is an increase in transience: VMs are cloned, automatically moved from one data center to the next, while containers are extended, initialized, and halted with incredible ease. Even the desktop has been replaced with a highly mobile laptop system. Increased miniaturization and transience are a real headache when attempting to "follow" an endpoint asset and monitor its operations.

To address just this challenge, every Tripwire Axon agent generates a unique identity, which enables discovery of new agents and their inventory of Capabilities, as well as re-linking previously collected security data to the re-establish stream. The Agent Identity, based on a generated Universally Unique Identifier (UUID), is independent of IP address or hostnames, allowing systems to move from one network to another without interruption in the monitored stream of data. This provides exceptional asset tracking data for even the most dynamic asset lifecycles.

When cloned, VMs typically change their MAC addresses. Also, restored VM images often have a completely new set of MAC addresses. The Tripwire Axon agent handles such cases by paying close attention to network adapter MAC addresses. When all the MAC addresses change a new UUID is generated to distinguish the new asset.

The agent is designed to automatically discover the route back to the server without user intervention or complex deployment time configuration. Agents can automatically query DNS SRV records for the list of available bridge hosts. For environments for which DNS changes are not feasible, agents can be statically configured through configuration files.

> For customers with an existing public key infrastructure (PKI) for certificate management, the Tripwire Axon agent accommodates them with an option to utilize those certificates.

Added Tripwire Axon Value

For organizations that who have enjoyed the benefits of Tripwire Enterprise agents, transitioning to the new Tripwire Axon platform has been made seamless through an automatic linkage of previous endpoint history (e.g., Tripwire Enterprise Elements and Versions) to freshly harvested Tripwire Axon data.

Tripwire applications such as Tripwire Enterprise communicate with the Axon platform components using the Tripwire Axon broker. Implementing asynchronous one-way messaging initiated by the endpoint, Tripwire applications minimize potentially slow or intermittent communications. Through dynamic pub/sub message patterns they are dynamic in the way they discover and configure Tripwire Axon agents.

The Tripwire Axon platform has features for attaching business relevant metadata in the form of "tags" at the point of collection, aiding the challenge of managing and maintaining the volumes of security as it flows from agents. It does this through the ability to add tags at each deployed agent, using a simple YAML formatted file. Tagged data surfaces as Asset View tags in Tripwire Enterprise, enabling automatic policy and rule scoping. Integrated with security results, this tag metadata enhances drill-down in security reports by focusing on endpoint mission relevance. Finally, tag metadata can indicate the importance of collected security data and can be used to implement security data storage policies.

> In a 2023 analysis of Tripwire ExpertOps℠ customers, over 98% of monitored systems were using the Tripwire Axon platform.

Conclusion

Tripwire has set a new standard in how IT operations, security and compliance can work together and integrate around a single source of endpoint intelligence. The Tripwire Axon platform is the bridging technology that efficiently gathers endpoint intelligence across an organization. Tripwire Axon removes the barriers of data silos, network dark zones, endpoint

blind spots, and transient devices through its innovative best practices for data collection and communication.

Tripwire Enterprise, Tripwire's flagship security configuration management (SCM) product, is the first of many applications to be built on the Tripwire Axon platform. The commitment to resolving real customer problems is clear. Tripwire Axon is the future of IT operations, security and compliance.

Request a Demo

Let us take you through a demo of Tripwire Axon and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to your specific IT security and compliance needs. Visit www.tripwire.com/demo.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.