SOLUTION BRIEF

Armis enterprise workflow automation, in partnership with Torq.

The challenge

Today's modern enterprises are struggling to keep up with the unprecedented growth in the number of digital assets, and asset types, that are being adopted to support the business. This explosion of assets is being driven by digital transformation and the need to innovate by introducing new technologies. However, most of these new assets and technologies are unmanaged, or "unmanageable." In fact, today over 70% of enterprise assets are unmanaged.

This has created a complex security problem and a growing operational headache. The fact that a vast number of assets are unmanaged means that users don't have the visibility and control they need in order to secure their operations. It creates an extended cyber-attack surface that is difficult to manage and protect. Attempting to resolve this with manual processes is almost a lost battle as new assets are being added on a daily basis, often more rapidly than assets are being decommissioned.

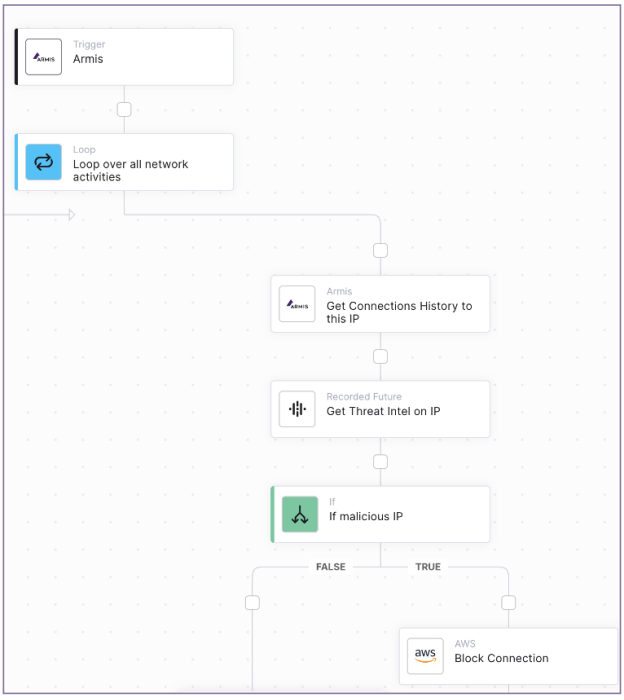
To effectively manage and control this attack surface, a new approach is needed. One that combines unprecedented visibility into assets, contextual intelligence into the vulnerabilities and threats that put these assets and operations at risk, and automated workflows that can orchestrate the response to detected threats.

Enter the power of Armis & Torq

The Armis Asset Intelligence Platform enables enterprises the ability to see and control their full cyber asset attack surface. By providing complete asset discovery, real time cyber vulnerability and threat intelligence, and highlighting critical assets that should be prioritized, Armis enables enterprises to quickly hone in on the assets that put their operations at risk, prioritize mitigation efforts to better manage their attack surface, and improve their overall risk posture.

Armis Enterprise Workflow Automation (EWA), powered by Torq, provides the security team with a seamless experience to build extremely powerful workflows, and to replace manual processes with an orchestrated response to events. The Torq solution enables security teams to automate any remediation or workflow, involving literally any IT, cyber or communications tool, without requiring any professional services or scripting.

A rich library of templates allows any security professional to quickly deploy event-triggered workflows, no matter how simple or complex the process, and no matter how many tools are involved. Consequently, all of the underlying asset intelligence and threat prioritization can be fully realized, and put into action without the complexity of coding and testing new integrations.



Use cases examples:

Automated vulnerability management

Effectively triaging and remediating vulnerabilities is critical to keeping your devices safe from threats. Together, Armis and Torq reduce attack surface by ensuring rapid CVE response. When Armis detects a new CVE for a device, Torq can kick off automated remediation workflows, or retrieve details, perform quarantine actions, and route alerts for immediate follow-up. Open CVEs can be regularly polled and escalated if not resolved within a set timeframe.

Accelerated threat response

The speed of threat response can be the difference between containing a breach, or being left exposed to ongoing risk. Connecting an automated Torq workflow to Armis' real-time threat detection ensures rapid response to keep threats contained. When a new threat is detected by Armis, Torq can enrich the alert before sending it to the responsible teams. Devices can be isolated or moved to quarantine, and device users suspended in IAM systems. Where remediation can be applied automatically, Torq workflows can also perform these actions - with humans in the approval cycle as necessary.

Enforce device compliance automatically

Keeping IT and OT assets protected at scale requires constant vigilance. Endpoint protection must be regularly updated, new assets must be brought into a protected state, and regular compliance must be proven to both internal and external audits. Armis' complete visibility into assets, with orchestrated Torq workflows across any system, turn this tedious manual work into automatic processes – freeing up valuable time for security teams. When Armis detects an endpoint with a missing or out-of-date agent, a Torq workflow can automatically install an updated version, or open a ticket for manual installation. Devices left out of policy over a set period of time can be quarantined, with alerts escalated as needed.

Key Benefits

- Maximize your investment in existing IT and security tools.
- Eliminate tedious manual work with automated workflows.
- Create complex workflows without scripting.
- Run automations across any tool, with no need for content packs or building new integrations.
- Respond faster to threats and operational events, and deliver better protection.

Why Security Teams Choose Armis Enterprise Workflow Automation?

Armis EWA is the easiest way for security teams to maximize their existing investments, respond faster to threats, and deliver better protection to their organizations:

- **Easily automate any security process:** ease of use leads to widespread adoption. The average customer automates 17 processes in the first two weeks. A leading EV manufacturer automated 44 distinct security processes in their first 30 days with the platform.
- **Respond to threats at machine speed:** Automated response leads to significant reduction in MTTR. For example, Lemonade, a leading Insurance Company in the United States, reduced their MTTR by 70x by using Torq automated workflows.
- **Focus on prevention, instead of reaction:** by eliminating manual toil when responding to alerts, triaging false positives, or following up on threats, the security team can focus on threat prevention. A leading global payments company reduced manual work in their SOC by 75% by creating automated workflows.

About Torq

At Torq, we understand the challenges facing front line security teams, who are often overwhelmed as the number of security events continues to rise within increasingly complex environments. Our platform helps front line teams and CISOs by delivering lightweight, modern security automation that is easily integrated with their existing tools set, and flexible enough to seamlessly scale as organizations' needs change

torq.io

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | armis.com

20220425-1

ARMIS. torq