SOLUTION BRIEF

Endace Always-on Hybrid Cloud Packet Capture Enhances Your Tines Stories For Rapid Incident Response

The Problem

The most serious threats require hard evidence that exposes exactly what's happening before, during, and after any security alert so you can confidently respond, remediate, and report. Logs and events can be wiped or manipulated and often lack the detail to show you exactly what's transpiring, leaving you to guess or assume the worst case.

The hard evidence exists in the network packets. Always-on network packet capture gives you a tamper-proof record of all activity across your environment, allowing you to understand and respond to any threat. Leveraging PCAP insights in your automation and workflow stories makes packet-level evidence easily accessible to your entire SoC team. It is essential for elevating security, and achieving stringent compliance and reporting requirements.

Organizations need a solution that:

- Provides always-on packet capture to record every incident reliably.
- Can be deployed on all the organization's infrastructure – including on-premise, private and public cloud.
- Is easy-to-use and fast to implement.
- Is cost-effective and scalable.
- Integrates with existing security solutions and workflows
- Has the flexibility to change easily to meet evolving needs.

Benefits

- Always-on recording to capture all traffic.
- Store weeks or months of full packet capture data for a complete record of network activity.
- Rapid search and data-mining.
- Full visibility across complex networks including Hybrid and Multi Cloud, including visibility into encrypted traffic.
- Deliver accurate, reliable, tamper-resistant forensic data to your security tools and teams.
- Give frontline teams automation superpowers.
- Break down barriers across systems with fewer duplicate efforts, unnecessary alerts, and information silos.
- Increase efficiency, mitigate risk, and protect revenue.
- Easy to deploy, integrates with existing infrastructure. Open architecture to work in multiple environments.
- Can be deployed in secure, air-gapped environments. Compliant with FIPS 140-3 and NIAP NDcPP 2.2E.

The Solution

Endace Packet Capture Workflows for Tines automates the search, archive, and download of critical network evidence (PCAP) related to any threat activity. Endace always-on packet capture records weeks or months of network traffic, including zero days, APTs, and insider threats.

Tines Workflows for Endace automates packet data mining for threat hunting, incident response, and compliance reporting.

Packet capture (PCAP) holds vital information that will help you resolve security incidents.

Couple this workflow with other actions, such as:

- Reconstructing file content from packet data
- Checking if a zero day threat was exploited in your environment.
- Analyzing lateral movement from infected hosts.
- Reconstructing historical activity from insider threats.
- Determining the root cause of a security brea.
- Monitoring and auditing network traffic in zero trust environments.

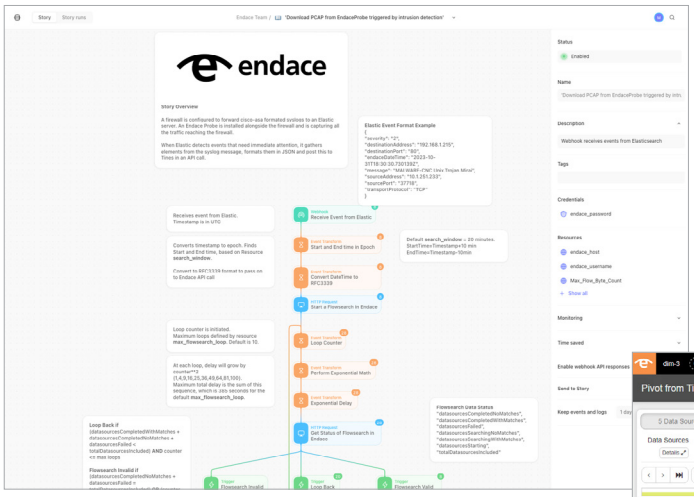
By combining Tines automation platform with Endace's always-on packet capture, organizations can bring the ultimate network forensic evidence - full packet capture data - into their investigation and threat hunting processes easily.

Multiple EndaceProbes can be connected to provide a unified, hybrid cloud packet capture recording fabric. This fabric enables rapid, centralized search, data-mining and analysis of packet data, and integrates directly with many security tools including Cisco, Palo Alto Networks, Splunk, IBM, etc. Automated investigations with Tines enables faster, more efficient investigation and resolution of network security and performance issues.

Conclusion

Tines and Endace have implemented proven solutions for government agencies and enterprise customers globally that simplify workflows, deliver unparalleled visibility into network activity and enable fast, accurate investigation and response. This joint solution simplifies repetitive tasks and programmatically preserves key forensic evidence, mitigating risk for your organization and empowering operations teams to be smarter and more efficient.

How it works



Efficient, Automated Workflows

- Tines stories automate finding and extracting the full packet data related to detected threats.
- Analysts are notified via email or alerts containing a direct link to analyze the related traffic in InvestigationManager.
- They can apply filters or views to examine traffic related to the alert, zero in on packets-of-interest and view decoded packets in Wireshark without downloading pcap files.

Solution Components

- Tines™
- EndaceProbe™ Always-On Packet Capture for On-Premise and Cloud
- Turnkey integrations with popular SIEM, NGFW, NDR, and NPM Solutions