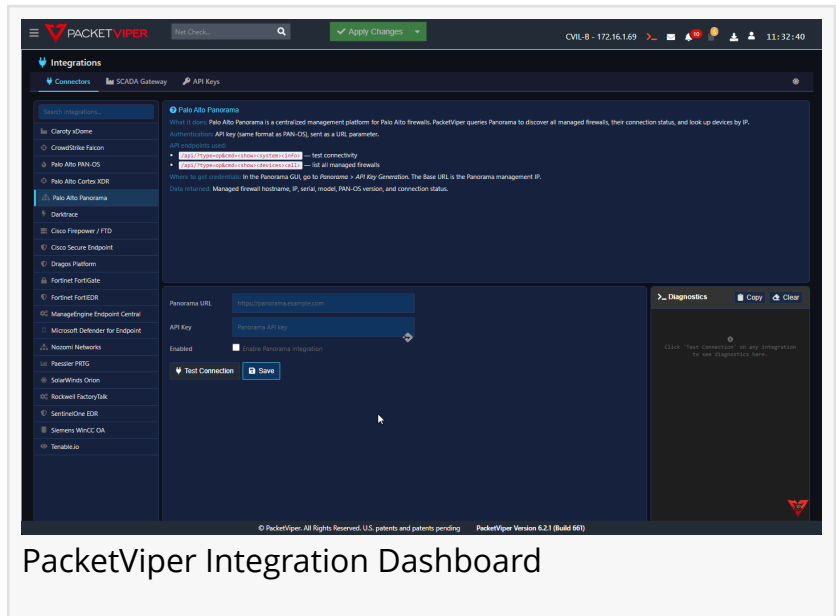


PacketViper Eliminates Swivel-Chair Security with Bidirectional Platform Integrations

PacketViper pulls data from the tools you already have -- EDR, OT, firewall, and more -- into one platform with prevention, detection, and response built in.

PITTSBURGH, PA, UNITED STATES, April 1, 2026 /EINPresswire.com/ -- PacketViper Eliminates Swivel-Chair Security with Bidirectional Integration Across Leading Security Platforms

By pulling data from the tools organizations already have, PacketViper delivers a complete picture of every threat -- from a single location, with the ability to prevent, detect, and respond.



PacketViper Integration Dashboard

Pittsburgh, PA -- April 1, 2026 -- PacketViper today announced a major expansion of its open security architecture, built around a single idea: when a threat appears, your team shouldn't have to leave the platform to understand it.

“

The swivel chair is where investigations go to die. Every tool knows something -- we built PacketViper to pull it all together and act on it.”

Francesco Trama, CEO & Founder, PacketViper

Security teams today operate across a fragmented stack. An alert fires. The analyst opens the EDR console. Then the OT platform. Then the firewall. Then the asset management tool. By the time the full picture is assembled, the window has closed.

PacketViper eliminates that workflow entirely.

ONE LOCATION. COMPLETE PICTURE.

By integrating natively with the security platforms organizations already have deployed, PacketViper pulls contextual intelligence from across the environment and surfaces it

automatically -- in the same interface where enforcement happens.

When a threat appears, PacketViper already knows what the device is from your endpoint platform, what it does from your OT or asset management system, what vulnerabilities it carries from your scanning platform, what network behavior it has shown from your detection tools, and who owns it and where it sits from your firewall and network management platforms.

No console switching. No manual correlation. No chasing data across six tools while the threat is still moving.

Native integrations include CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne, Palo Alto Networks, Fortinet, Cisco, Claroty xDome, Dragos, Nozomi Networks, Tenable.io, Siemens WinCC OA, Rockwell FactoryTalk, Darktrace, SolarWinds, ManageEngine, Paessler PRTG, and additional platforms.

PREVENTION, DETECTION, AND RESPONSE -- FROM ONE PLACE

Context without action is just a better dashboard. PacketViper combines the intelligence pulled from third-party platforms with its own inline enforcement engine -- so the complete picture doesn't just inform the analyst. It drives the response.

Identify the threat. Understand the asset. Act on it -- inline, automatically, without waiting for a ticket to clear or a playbook to run.

That is the difference between a visibility tool and a defense platform.

YOUR TOOLS CAN CONNECT BACK

PacketViper's REST API exposes 45 endpoints across nine functional areas -- giving SOAR platforms, automation workflows, and external tools direct programmatic access to PacketViper's enforcement, analytics, and intelligence capabilities.

Traffic analytics, asset data, compliance scoring, federation management, AI advisory -- all available via API. PacketViper becomes a data source and enforcement engine for the tools already running in your environment.

INCLUDED. NOT ADD-ON.

All integrations -- inbound and outbound -- are included within the PacketViper platform subscription. No per-integration licensing. No marketplace fees. No professional services required to activate.

Configure with API credentials. Available now in PacketViper version 6.

"The swivel chair is where investigations go to die. Every tool in a security stack knows something. The EDR knows the host. The OT platform knows the device. The firewall knows the policy. But none of them talk to each other -- so the analyst becomes the integration layer, bouncing between consoles trying to assemble a picture while the attacker is still moving. We built the integrations to end that. Pull it all into one place, add inline enforcement, and you're not just informed -- you're acting. That's the complete picture we set out to build."

-- Francesco Trama, CEO & Founder, PacketViper

AVAILABILITY

All integration capabilities described in this release are available now within PacketViper version 6.

ABOUT PACKETVIPER

PacketViper delivers [preemptive cyber defense](#) purpose-built for converged IT and OT environments. The platform combines inline enforcement, [automated moving target defense](#), deception technology, and high-performance analytics in a single architecture designed for critical infrastructure and enterprise networks.

For more information, visit packetviper.com.

Media Contact:

Tim Jencka
PacketViper
news@packetviper.com

Tim Jencka
PacketViper
+1 412-212-6348

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/902115961>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.