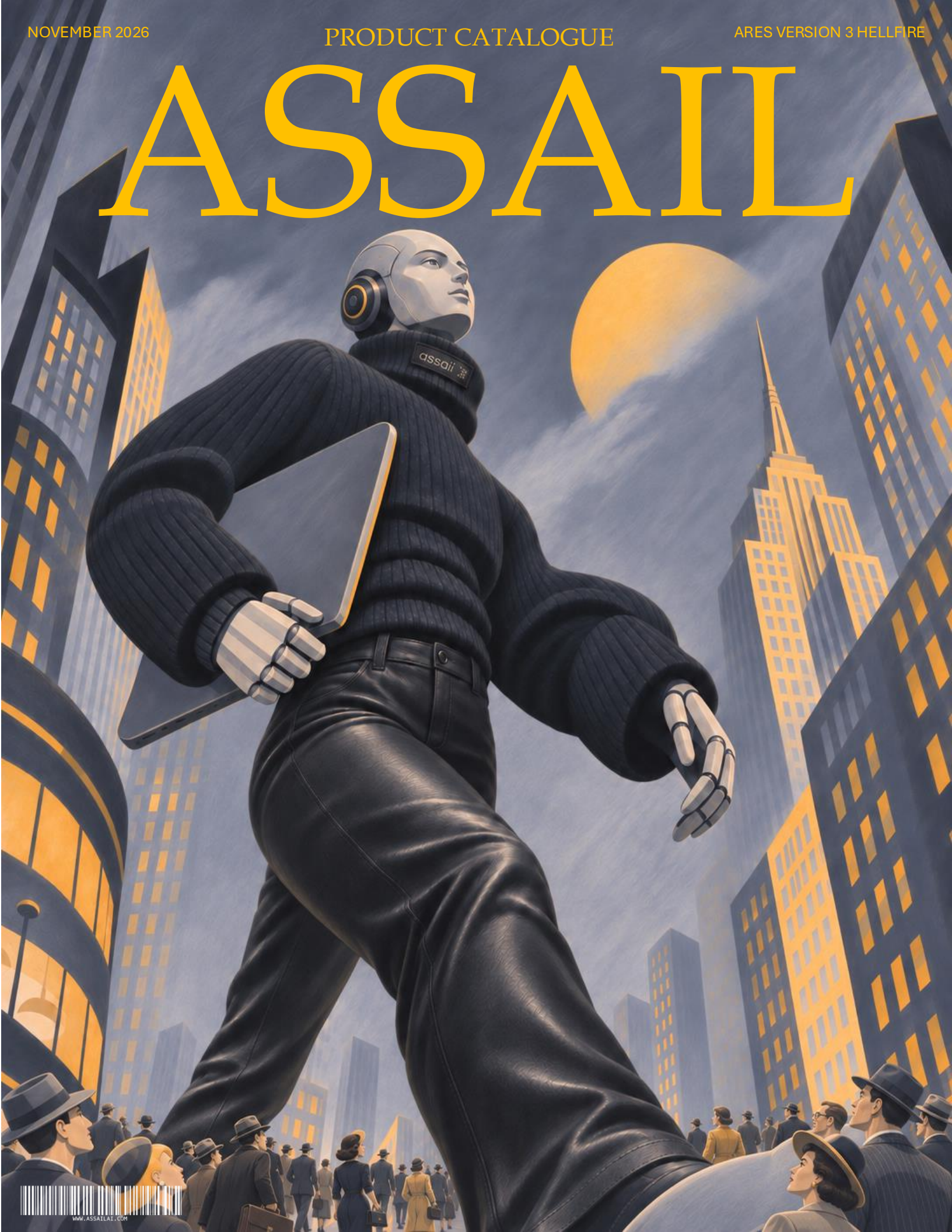
NOVEMBER 2026

PRODUCT CATALOGUE

ARES VERSION 3 HELLFIRE

ASSAIL



WWW.ASSAILAI.COM

Contents



Letter from the CEO 02
A personal welcome from Alissa Knight

Meet Assail 03
Our Mission and Approach

Ares 04
Adversarial Exposure Validation for the Enterprise

Ares Cloud 05
Offensive pressure in our SaaS cloud

Ares Edge 06
Offensive pressure under your control on your own terms

Halo 07
Federated management of your Ares Edge fleet

Key Facts 08
Spec Sheet

What Makes Us Different



"Confidence begins with evidence."

Dear Reader,

After more than 26 years in offensive security, I have learned that the hardest question is often the simplest: could someone actually, use this weakness to hurt our organization?

I founded Assail to help you answer that question with evidence you can act on. We build autonomous offensive security platforms that test your applications, APIs, mobile apps, and AI systems, helping your team find exploitable weaknesses before someone else does.

In a market described as adversarial exposure validation, or AEV, my focus is practical: what can an attacker reach, what can they do, and what should you fix first? Our approach brings together threat modeling, autonomous testing, and evidence of what happened. Testing across different user identities helps expose failures that can let one person access another person's data or perform actions they should never be allowed to take.

For your organization, the value is clarity. Your security team gets evidence to assess risk. Your developers get findings they can reproduce and use to guide repairs. Your leaders get a clearer view of what those weaknesses could mean for the business. As your systems change, repeat testing helps you check whether fixes worked and uncover new problems.

I also believe security should fit the way you operate. Whether you need cloud delivery, deployment in your own environment, or testing in a disconnected setting, our platforms are built for those different realities.

Our mission is to make rigorous offensive security a continuous capability, giving your people more time to solve the problems that matter and greater confidence in the systems your organization depends on.

Thank you for taking the time to get to know Assail. I look forward to helping you protect what you are building.

Warm regards,

Alissa Knight

CEO, ASSAIL, INC.

Meet Assail

Built to ask harder questions.



Who we are

Assail builds autonomous offensive security platforms powered by AI. We help organizations test their applications, APIs, mobile apps, and AI systems, uncover exploitable weaknesses, and give teams the evidence they need to act.

Our why

We believe every organization deserves confidence in the technology it depends on. We exist to help people pursue what's possible without fear of what's vulnerable.

Our mission

Make rigorous offensive security a continuous capability for every organization we serve. We connect threat modeling with autonomous testing to help you understand what is at risk, prioritize repairs, and check that fixes hold. Through cloud and customer-controlled deployment options, we bring that capability to the environments where your work happens.

Ares



A clearer view of risk

Ares is Assail's autonomous offensive security platform for applications, APIs, mobile apps, and AI systems. It helps your team discover exploitable weaknesses and understand what an attacker could do with them.

Start with the systems you are authorized to test. Ares brings threat modeling and security testing together, helping you turn questions about risk into practical tests.

Beyond the first finding

Real attacks depend on context: who is signed in, what they can access, and how different parts of a system interact. Ares tests across user identities to uncover weaknesses in access controls and business logic.

The result is evidence your security team can assess and findings your developers can reproduce, giving both teams a clearer path from discovery to repair.

Built for ongoing change

New releases and integrations can create new ways into your systems. Repeat testing helps your team check that repairs worked and discover weaknesses introduced by change.

Choose the deployment that fits your organization. Ares Cloud and Ares Edge bring the platform to different operating environments, with dedicated pages later in this catalogue.

Ares Cloud

Offensive Security, delivered from the cloud

Ares, without the hardware

Ares Cloud brings Assail's autonomous offensive security platform to your team through a cloud-delivered service. Test authorized applications, APIs, mobile apps, and AI systems without operating dedicated testing hardware.into practical tests.

Focus on what needs fixing

Bring your targets and the questions you need answered. Ares connects threat modeling with autonomous testing to help your team investigate exploitable weaknesses and understand their consequences.

Testing across different user identities helps expose access-control failures and business-logic weaknesses. Findings your developers can reproduce give your team a practical starting point for repair.



Keep pace with change

As your applications evolve, repeat testing helps you check that fixes worked and find weaknesses introduced by new releases and integrations.

Choose the right fit

Ares Cloud is the cloud-delivered option in the Ares family. For environments that call for deployment closer to your systems, explore Ares Edge on the following page.

Ares Edge

Offensive Security, delivered from the cloud

Bring autonomous security testing inside your environment.



Your environment. Your deployment.

Ares Edge is the on-premises version of Assail's autonomous offensive security platform. Deploy it within your own environment to test authorized applications, APIs, mobile apps, and AI systems closer to where they run.

It brings the Ares approach to organizations that need local deployment, access to private systems, or greater control over how security testing fits into their operations.

Reach the systems behind the perimeter

Some of your most important applications are available only inside your network. Ares Edge lets you place testing within that environment, so your team can assess internal systems without making them publicly accessible for the assessment.

Define the approved targets, provide the access needed for testing, and investigate weaknesses in the context of your own systems.

Look beyond individual weaknesses

A weakness becomes more meaningful when you understand what someone could do with it. Ares combines threat modeling with autonomous testing to examine attack scenarios and gather evidence of what happened. Testing across different user identities helps reveal access-control and business-logic failures, including situations where one user can reach another user's data or perform an action beyond their permissions.

Give developers a path to repair

Your team needs findings it can investigate and reproduce. Ares provides evidence that helps security teams assess risk and developers understand the behavior they need to correct. Repeat testing helps you check whether repairs worked and identify weaknesses introduced by subsequent changes.

Designed for operational control

On-premises deployment gives your organization control over where the platform runs and how it connects to approved targets. Plan the installation around your network boundaries, access policies, and infrastructure requirements.

For disconnected or air-gapped environments, work with Assail to define the appropriate deployment and operating model.

Make testing part of the routine

Use Ares Edge to bring repeatable offensive security testing into your own environment as applications and integrations evolve.

The goal is practical: clearer evidence, better-informed priorities, and greater confidence in the systems your people depend on.



Halo

One fleet. One place to manage it.

Bring your Ares deployments together without losing sight of where each one operates.

The server behind the fleet

Halo is Assail's federated server for managing multiple Ares deployments. It gives your team a common place to manage the fleet as Ares expands across your organization.

An Ares deployment provides offensive security testing within its operating environment. Halo brings those deployments into a shared management structure, helping your team work across the fleet.

A clearer way to manage scale

A single deployment is one thing. A growing fleet across offices, business units, or customer environments creates a different operational challenge.

Halo is built for that broader view. Organize your approach around the deployments you operate, while keeping each deployment's environment and purpose in context.

Central management. Distributed testing.

Your organization may need testing close to different applications and networks. With Halo, fleet management can sit above those distributed Ares deployments.

That distinction matters: the testing happens through Ares, while Halo gives your team a place to manage the deployments that deliver it.

Built around your organization

Whether you are coordinating deployments for one enterprise or managing a fleet across multiple environments, Halo provides the federated management layer.

Work with Assail to plan the server, connected deployments, and network access around your operating requirements. The objective is simple: make a larger Ares estate easier for your people to manage.

Your deployments, working as a fleet.

Key Facts

Version 3 Hellfire

Release Date: SEP 30, 2026

01 / SUPPORTED TARGETS

Target	Support
APIs	Supported
Web Apps	Supported
Mobile Apps	Supported*
AI systems	Supported

02 / CURRENT MODULES

Module
Red Team module
Attack Surface Management module
Asset Management module
Cassandra AI Assistant Module

03 / PLATFORM & MODEL

Item	Specification
Deployment	Ares Cloud; Ares Edge (on-premises)
Fleet management	Halo federated server
Model size	31 billion parameters
CPU architectures	x86_64 (AMD64); ARM64 (AArch64)
Reference precision	BF16: RTX configuration; FP8: GB10
Configured context	32k: 1 GPU; 128k: 2 GPUs; 64k: GB10

04 / x86 ON-PREMISES LAB

Component	Reference specification
Topology	Separate model and application hosts
CPU	32 cores per host
System RAM	256 GB per host
Storage	1 TB NVMe per host
Network	10 GbE per host
Recommended GPU	NVIDIA RTX PRO 6000 Blackwell
GPU memory	96 GB GDDR7 ECC per card
GPU count	1 minimum; 2 recommended
Application host GPU	Not required

05 / ARM / GRACE BLACKWELL

Component	Reference specification
Platform	NVIDIA GB10 Grace Blackwell
Example system	DGX Spark / GB10 OEM desktop
CPU	20-core Arm
Unified memory	128 GB shared CPU/GPU
Validated OS	Ubuntu 24.04 ARM64
Free disk for install	90 GB in GB10 install guide
Model precision	FP8
Intended use	Evaluation; lower throughput than RTX pair

Lab configurations are evaluation references, not universal production minimums. Production sizing depends on workload, concurrency, context and release. GB10 requires a different configuration from discrete-GPU hosts.

Installation: 64-bit Linux; architecture-specific bundle; container runtime; NVIDIA driver for model serving; TPM 2.0. Secure Boot enabled for standard installation posture.

***Mobile Apps:** static binary analysis runs locally; live mobile runtime testing currently uses a cloud device farm.

Source basis: Assail deployment guides and NVIDIA hardware specifications.