ATLAS PLATFORM

Atlas Patch Management

Third-party software patching inside Atlas.

Known Vulnerabilities Stay Open Too Long

Most security teams already know which applications are out of date. Getting them patched takes longer.

The finding sits in one tool → *The update runs through another* → *Each handoff between security and IT adds days*

Attackers work the window between a patch's release and its install. ***Atlas Patch Management*** puts the fix next to the finding, and you approve every patch.

31%
of breaches began with vulnerability exploitation.
McKinsey, The State of AI, 2025

43 days
median time to fully patch a vulnerability.
IBM Cost of a Data Breach Report, 2026

1 in 4
CISA Known Exploited Vulnerabilities is fully remediated.
Enkrypt AI MCP Server Scan, October 2025

What Atlas Patch Management Delivers

Software Visibility

- Every installed application on every endpoint running the Atlas Sensor
- Third-party updates from WinGet, Homebrew and Linux package managers
- Needs Patching counts by software and by endpoint
- Patch history: an audit log of every request, with software, asset, version change, status and requester

Prioritization

- A priority score for each piece of software
- Ranked using public exploitation signals and VulnCheck
- For Atlas Preempt Pentesting customers, boosted when pentests prove a flaw exploitable in your environment
- Weighted by affected devices and the severity of the worst flaw

Controlled Remediation

- Your approval before every deployment
- Updates applied through each endpoint's native package manager
- Reboots left to your team, never automatic
- Version lock stops Atlas from patching software that must stay unchanged
- Atlas API ticketing for teams that patch through their own workflow

How It Works

1. **Enable**
Turn on Patch Management in the Atlas Sensor.

2. **Inventory**
The Atlas Sensor lists every installed app and finds available updates.

3. **Prioritize**
Atlas ranks updates by exploitation, device count and severity.

4. **Approve**
Your team reviews the impact and approves. The Atlas Sensor deploys.

5. **Verify**
Atlas confirms the fix and logs every action.

3 operating system families covered: Windows, macOS and Linux

100% of deployments approved by your team

Typical Patch Tooling vs Atlas Patch Management

Capability	Typical Patch Tooling	Atlas Patch Management
Inventory of installed third-party software	✓	✓
Third-party updates for Windows, macOS and Linux	✓	✓
Approval before each deployment	varies	✓
Reboots left to your team	varies	✓
Version lock for software that must stay unchanged	varies	✓
Audit log of every patch request	varies	✓
Updates ranked using public exploitation signals	varies	✓
Ticketing into your own workflow through an API	varies	✓
Ranking informed by Atlas Preempt pentest findings	—	✓
Runs on the same Atlas Sensor that powers your MDR	—	✓
Patch from the same console that surfaces the exposure	—	✓

Atlas Patch Management covers third-party applications on Windows, macOS and Linux. Operating system and kernel updates stay with your existing tools.Linux package coverage at launch: apt and dnf.

Outcomes You Can Expect

- A shorter window between patch release and patch applied
- No handoff delays between security and IT
- The vulnerabilities attackers exploit most, closed first
- Proof of remediation for auditors and leadership

Fix what Atlas finds.

See every outdated app on every endpoint, and patch it with one approval
Available as an add-on to Atlas Packages. Requires the Atlas Sensor.

LET'S TALK SECURITY →

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSentire is a leader in Controlled Autonomy SecOps, protecting thousands of organizations in 90+ countries across 35+ industries. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.