britive

Britive + Crowdstrike:
JIT Local Admin Elevation

Zero Standing Privilege, All the Way to the Endpoint

Least privilege was never meant to stop at the laptop. Teams have driven standing privilege out of cloud, SaaS, and the data center, but local admin on the endpoint is the holdout. Britive extends its zero-standingprivilege engine to the endpoint using the CrowdStrike Falcon sensor you already have. No new agent. No second policy engine.

THE CHALLENGE

Every Endpoint Admin Option is a Tradeoff

- Always-on local admin. Low friction, but a permanent grant of the single most valuable foothold for ransomware and malware.
- Secondary “-a” accounts. Standing privilege isn’t removed, just moved to a second account that’s privileged by design and watched less by habit. High user friction.
- Legacy EPM. Genuinely reduces standing admin, but adds another agent on every machine, a separate policy engine, and ongoing operational cost, a parallel access-control plane.

THE SOLUTION

A native integration delivering policy-controlled, temporary local admin elevation on endpoints. Britive elevates the user, not an account — dynamically adding them to the local Administrators group for a defined window, then auto-revoking. It’s the same platform that already governs just-in-time, zero-standing-privilege access for human, non-human, and agentic identities across cloud, SaaS, hybrid, and on-prem.

HOW IT WORKS

1. Request. User signs in to Britive via SSO, selects the “Desktop Admin Access” profile, and checks out.
2. Policy decision. Britive evaluates the request — MFA, justification, network location, approval routing, and device posture. Fail any check and elevation is denied, regardless of who’s asking.
4. Resolve device. Britive resolves the user’s hostname to its Falcon device ID.
5. Elevate. Britive invokes Falcon Real Time Response (RTR) to add the user to the local Administrators group for a policy-defined window (typically 15–60 minutes).
5. Work under watch. The user does the task while Falcon keeps monitoring. SSF risk signals can block or terminate the session mid-flight.
6. Auto-revoke & audit. On expiry or check-in, a second RTR command removes the user. The host returns to zero standing privilege — and both platforms log who elevated, on what device, why, and for how long.

WHY IT MATTERS

Attackers aren’t hacking in, they’re logging in. A standing local admin account is exactly the credential they’re after: high privilege, alays available, sitting in the open.

39%

of breaches involve credential abuse; the single most pervasive technique

Verizon 2026 DBIR

32%

rise in identity-based attacks in H1 2025. ~97% are simple password attacks.

Microsoft Digital Defense Report 2025

~2x

the price stolen admin accounts fetch on criminal markets to skip privilege escalation

SpyCloud, on the 2026 DBIR

73%

of ransomware victims had a prior infostealer infection or credential leak

SpyCloud, on the 2026 DBIR

Why It's Different from Legacy EPM

Legacy EPM bolts a separate endpoint tool onto your stack. Britive governs the endpoint with the same zero standing privilege engine that already exists in your cloud, SaaS, hybrid, and on-prem environments. Britive only elevates on a device that's healthy at the moment of request.

CAPABILITY	LEGACY EPM	BRITIVE + CROWDSTRIKE
Dedicated EPM Agent	Required	Not needed — uses Falcon sensor
Separate policy engine	Required	Not needed — one Britive engine
Privilege scope	Endpoint only	Cloud, SaaS, hybrid, on-prem + endpoint
True JIT elevation	Rule-based	Native JIT
Zero standing privilege	Partial	Full ZSP
Live device-posture gating	No	Yes — via CrowdStrike SSF
Uses existing EDR	No	Yes — Falcon RTR
Time to Value	Weeks - Months	Days

HOW IT WORKS

No Additional Agent
Leverage the Falcon sensor already deployed; zero incremental endpoint footprint

Genuinely Zero Standing Privilege
No permanent admin account, no -a identity, no persistent evaluation artifact left behind.

Posture-Aware Elevation
A compromised or out-of-compliance device can't check out admin permissions, and active sessions can be cut off on risk detection.

One Policy Engine Across Every Environment
Cloud, SaaS, hybrid, on-prem, and endpoint all operate under a single Britive model.

Unified, Compliance-Ready Audit Trail
Full elevation lifecycle correlated across Britive + Falcon; SIEM-ready evidence for PCI-DSS, SOX, HIPAA, ISO 27001.

Fast Time to Value
An RTR script plus a Britive profile is all you need, not an EPM rollout, which can be completed in days, not months.

SECURING ACCESS FOR INDUSTRY LEADERS

fiserv. TOYOTA Forbes ThermoFisher SCIENTIFIC GAP