The architecture has to work after authentication

Continuous authorization depends on several parts of the security stack doing different jobs but responding to the same context.

The identity provider establishes who a user or workload claims to be. A Policy Decision Point evaluates what that identity should be allowed to do under the current conditions. The Policy Enforcement Point then applies that decision at the application, network, cloud service, data, or Application Programming Interface (API) layer.

That separation is important because proving an identity and deciding what it can do are not the same problem.

Consider what that means in a normal working day. An employee signs in successfully at 09:00 and receives an access token. At 09:15, the device becomes compromised. If that token remains trusted for hours, the security architecture is effectively relying on a decision made before the risk changed.

Short-lived tokens reduce this exposure by requiring the policy engine to reassess access more often. Event-driven controls can go further because they do not need to wait for a token renewal. A meaningful change in endpoint health, location, privilege use, or behavior can trigger a new access decision immediately.

It creates a closed loop between identity and security operations. Endpoint and identity signals influence access, while actions such as a blocked request, privilege reduction, or forced reauthentication become new evidence for the Security Operations Center (SOC).

The technology pieces already exist in many enterprises. Connecting them is the harder job.

What you do after login may matter more

Once a user has authenticated, credentials gradually become less useful as evidence that the legitimate person is still behind the session. What the identity does next can reveal much more.

A token appearing from another browser fingerprint, device, network, or location deserves attention. So does a session that appears in Mumbai and then in Eastern Europe 40 minutes later. An employee who suddenly starts accessing unfamiliar systems, calling administrative APIs, or moving large volumes of data may also be behaving outside the account's normal pattern.

The important word here is combination. One unusual event does not necessarily mean that an account has been compromised. People travel. Networks change. Employees take on new projects. Legitimate users sometimes behave in ways that look unusual to a security system.

But a new network combined with unfamiliar privilege use and a bulk data transfer tells a different story. New MFA device registration followed by unusual token refresh activity, an unexpected password reset, or lateral movement can add still more context.

Privilege use can be especially revealing. An employee may have possessed elevated permissions for months without using them.

> "Effective Zero Trust requires identity signals from IAM, device posture, endpoint telemetry, workloads and threat intelligence to be unified through a central policy engine that scores them into a single, real-time risk decision at the point of access.

VINEET MORONEY,
Chief Transformation Officer,
Xoriant