White Paper

Configuration Intelligence in the Age of Agentic IT Operations

Overview

Enterprise IT is entering a new era—agentic operations—where autonomous AI agents manage complex environments with minimal human input. This shift demands not just telemetry but deep configuration awareness. Evolven's Configuration Intelligence delivers this by providing complete, contextual, and risk-scored configuration data. It enables AI agents to act safely and intelligently, reducing risk and improving performance. As agentic IT evolves, Evolven becomes essential for enabling explainable and resilient autonomous operations at scale.

EVOLVEN

Executive Summary

Over the past five years, enterprise IT has undergone a profound transformation. The shift to cloud, the adoption of containerization, and the rise of serverless architectures have redefined how infrastructure is built and operated. Now, a new frontier is emerging—**agentic IT operations**, enabled by autonomous AI agents capable of monitoring, diagnosing, and remediating complex environments with minimal human intervention.

This marks a shift from infrastructure abstraction to **decision abstraction**. Rather than executing predefined scripts, AI agents now orchestrate workflows, evaluate telemetry, and make operational choices in real time across hybrid and multi-cloud environments. Early adopters—especially in high-complexity, high-regulation sectors—are leveraging these frameworks to scale support, reduce resolution times, and automate compliance enforcement.

Agentic systems, however, are only as effective as the data and context they consume. While they can ingest telemetry streams, ITSM records, and CI/CD pipeline outputs, they often lack a dynamic and precise understanding of the **configuration landscape** in which they operate. Key information—such as what changed, when, by whom, whether the change was expected or anomalous, and how the change correlates with outcomes—is typically fragmented across change requests, CMDBs, and deployment tools. These sources are often partial, siloed, or stale, limiting the agent's ability to make informed, reliable decisions at scale.

This is where Configuration Intelligence becomes essential.

To safely support autonomous action, agents require a continuously updated, authoritative view of configuration state-correlated, contextualized, and enriched with operational insight. This includes not only the timeline and origin of changes but also their implementation details and alignment with broader system behavior.

However, visibility alone is insufficient. Without **embedded risk assessment**, agents remain blind to the consequences of changes they observe or initiate.

- **Stability risk scoring** evaluates alignment with validated performance baselines, historical norms, and known failure patterns—identifying misconfigurations that may not violate policy but still pose real-world risk.

- **Security risk scoring** flags deviations that introduce vulnerabilities, breach compliance requirements, or create audit concerns.

Together, these capabilities transform raw configuration data into **actionable intelligence**, providing operational guardrails that support not just observation and reaction, but forward-looking, explainable decision-making.

Evolven delivers this missing layer. As the leader in Configuration Intelligence, Evolven continuously detects, analyzes, and contextualizes every meaningful granular change across infrastructure and applications: on-prem, in private clouds, and in public cloud environments. It doesn't just observe changes; it understands them.

In the emerging world of agentic IT, Evolven doesn't compete with autonomous agents, it **enables them**. By delivering continuous, risk-aware configuration awareness, Evolven empowers agents to act safely, intelligently, and transparently.

This white paper explores the evolution of agentic operations and details how Evolven's Configuration Intelligence platform plays a foundational role in enabling safe, autonomous, and accountable IT operations.

The Emerging Agentic AI Landscape in IT Operations

From Automation to Autonomy

Over the past decade, IT operations have evolved from manual administration to automated, cloud-native practices. Tools such as Infrastructure as Code, CI/CD pipelines, and observability platforms have enabled organizations to operate with greater speed, scale, and consistency. Yet, most automation remains static. It is driven by rule-based scripts reacting to predefined triggers.

Agentic IT operations represent the next stage in this evolution.

In this paradigm, AI agents with decision-making capabilities—powered by large language models, machine learning, and reasoning engines—move beyond reactive execution. They continuously monitor systems, assess context, and take proactive actions to fulfill operational objectives such as uptime, efficiency, and compliance. These agents are not bound by fixed playbooks; they interpret system state, plan remediations, and collaborate with other agents to achieve shared goals.

This marks a step-change in capability:

- Incidents are triaged autonomously, not merely escalated.
- Remediations are planned using contextual understanding, not just scripted steps.
- Multi-agent systems coordinate across domains to drive goal-oriented behavior.

Major enterprises, particularly those seeking innovative technologies as a differentiator, for example, financial institutions, are piloting and scaling these capabilities. AI agents are resolving production support tickets, anticipating system failures, automating incident response, and optimizing cloud spend, all without explicit step-by-step human input.

Why This Matters Now

Several forces are converging to make agentic IT not just possible, but urgent:

- Operational complexity has exploded with hybrid/multi-cloud, Kubernetes, and ephemeral services.
- Customer expectations and talent shortages make 24/7 human-powered operations challenging.
- Economic pressure demands that IT do more with less, driving interest in "self-healing" and "self-optimizing" systems.
- AI maturity has reached a tipping point now that models can parse logs, interpret system states, and generate actionable decisions in real-time.
- AI capabilities are dramatically improving, with a doubling of capability every four months.

And yet, as agentic frameworks grow more powerful, some significant shortcomings remain, one of which is the lack of or insufficient change and configuration data.

The Blind Spot: Agentic AI Lacks Configuration Awareness

Agentic systems are only as effective as the context in which they operate. While AI agents can analyze log data, observe telemetry metrics, and trace transactions using APM tools, they still lack a

complete picture of the environment. Observability tells you *what* isn't working. APM highlights *where,* in the request flow, a failure or bottleneck occurs. Logs reveal *what* happened in detail. However, to understand *why* it happened and what the environment looked like at that time, you need to know *how* the system was configured and how it reached that state.

This is the core blind spot in today's agentic frameworks: they typically lack real-time awareness of configuration state and history. Without knowing what changed, when it changed, who made the change, and how it deviated from best practices or compliance policies, agents are left to guess at root causes and the safety of their own remediations.

Traditional sources like Change Management platforms, Configuration Management Databases (CMDBs), and CI/CD pipelines offer only partial answers:

- **Change Requests** defined in Change Management platforms capture what *should* change, but not what *did*. Plans and reality often diverge due to deployment issues, manual interventions, or rollback scenarios.
- **CMDBs** attempt to represent the environment but often suffer from low granularity, stale data, and reliance on manual updates. They rarely reflect the real-time or runtime state.
- **Pipelines** can show what was delivered, such as artifacts and deployment scripts, but they don't capture what those scripts actually *did* when executed. The outcome often depends on runtime conditions, external system responses, or environment-specific logic embedded in the scripts. As a result, the final configuration state may diverge from what's recorded in the pipeline, leaving critical changes untracked and invisible to agents.

Crucially, none of these systems objectively assesses the *risk profile* of a configuration change, whether it increases the chance of instability, violates a policy, introduces a security vulnerability, or deviates from established performance norms. They don't correlate changes to outcomes or enable effective proactive decision-making based on current and historical risk context.

As a result, even highly capable AI agents are effectively operating with blinders on. They may:

- Propose remediations that fail or worsen the issue
- Miss subtle but critical changes that triggered an incident
- Trigger actions that violate compliance or internal policy—without traceability
- Lack the basis to justify or explain their decisions

In short, even the smartest agent is still guessing—if it doesn't know how the system is configured and what changed.

Why Configuration Intelligence Is Foundational to the Agentic Stack

For agentic IT operations to be safe, effective, and explainable, they must operate on a continuously updated, configuration-aware foundation. This foundation must provide a trustworthy view of both the current system state and the sequence of changes that led to it. It's not enough to collect and analyze performance metrics or application logs—agentic systems must understand:

- **What are the past and current configuration states**—at the most comprehensive and detailed level.
- **What configurations changed**—across infrastructure, applications, platforms, and policies.
- **Who or what initiated the change**—including whether it was a human, an agent, or an automated policy.
- **Why the change occurred**—and whether it aligns with intent, policy, or goals.
- **How the actual change correlates** with performance trends, alerts, or incidents across the environment.

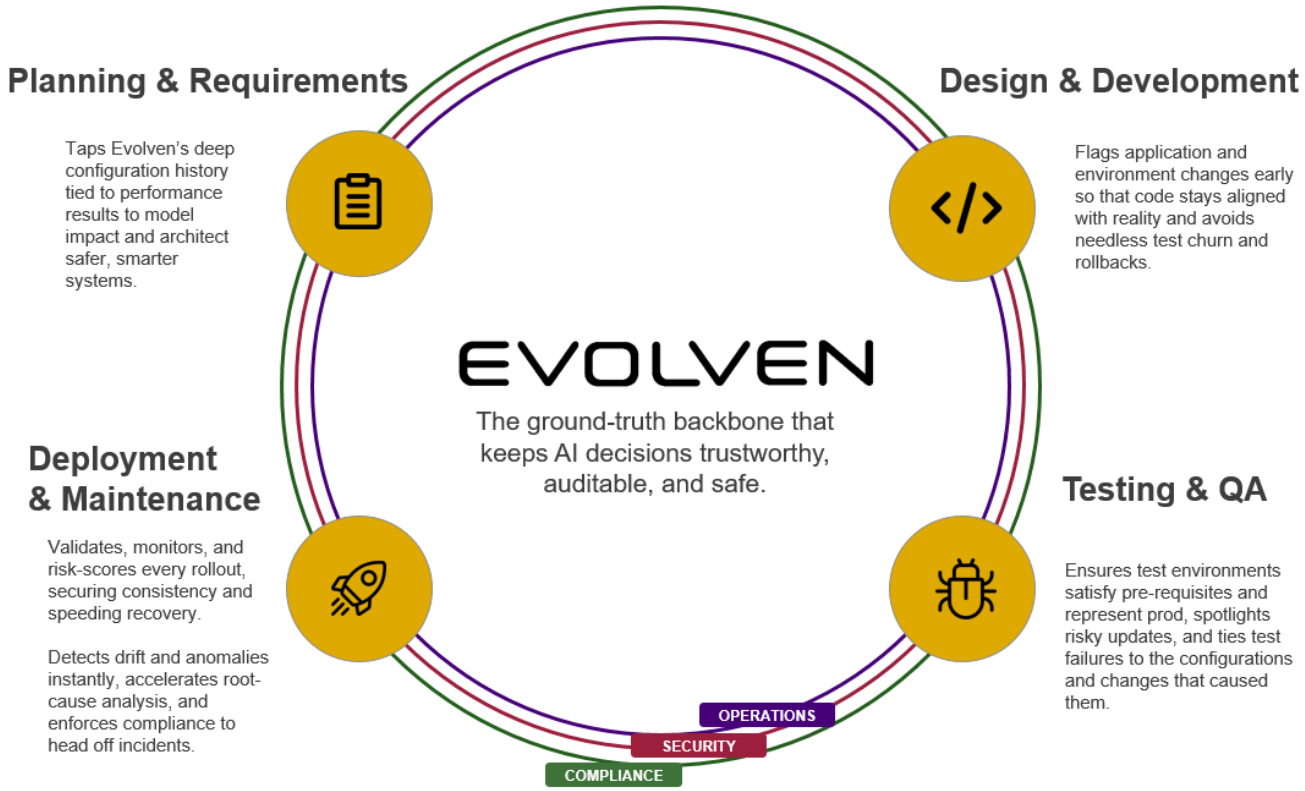
This depth of insight is not available from traditional observability, configuration, or change management tools, including cloud native ones. It requires a dedicated layer of Configuration Intelligence—one that consolidates, correlates, and risk-scores all changes in real time.

Even in environments where AI agents autonomously manage and deploy changes, Configuration Intelligence remains critical. The concept of "unauthorized change" may evolve into **"unjustified or illegitimate change intent"**, for example, a policy violation disguised as an optimization goal, or a flawed prompt that triggers an agent to deploy insecure parameters. In these scenarios, the agent's actions may be technically valid but contextually risky or noncompliant.

Agentic drift introduces a new category of operational risk. Unlike traditional drift, typically caused by manual deployments, hotfixes, or out-of-band changes, agentic drift emerges from the autonomous decisions made by AI agents themselves, like entropy in thermodynamic systems. These systems may execute a series of changes that are locally rational and technically valid, yet over time, collectively move the system away from intended baselines, compliance policies, or performance norms. Without continuous configuration awareness, even well-intentioned agents can drift from organizational goals, taking a series of locally rational actions that, in aggregate, lead the system into unstable or noncompliant territory. This kind of recursive deviation, where the agent effectively follows its own logic down a rabbit hole, underscores the need for an independent control layer to detect and correct course before risk accumulates.

That's why it's essential to separate the function that governs change from the function that executes it.

Agents may build and apply changes, but they should be continuously validated by an independent layer that understands configuration context, assesses risk, and enforces organizational guardrails. Configuration Intelligence performs this role not by dictating policy, but by capturing and analyzing every change in context: its rationale, trajectory, and impact. It enables enforcement by providing the insight needed for agents and teams to act in alignment with policy and intent.



Configuration Intelligence provides the historical trail and up-to-date understanding needed to:

- Detect emerging patterns of risk or drift
- Flag deviations from organizational goals or policies
- Enable agents to refine decisions through feedback loops
- Support audits and compliance with full contextual traceability

In short, Configuration Intelligence is not just a support tool for agentic IT, instead it is a foundational control plane for the change and configuration of IT environments managed by agentic frameworks. And Evolven delivers this missing layer, enabling agentic systems to act with clarity, safety, and accountability.

Why Evolven Is Critical in the Agentic Future

Evolven: The Configuration Intelligence Layer That Makes Agentic IT Trustworthy

In the emerging world of autonomous IT operations, Evolven is not only compatible with agentic architectures, it is foundational to them.

Where AI agents bring the ability to reason, plan, and act, Evolven brings the continuous, trusted environmental awareness that allows those agents to operate safely and intelligently. Evolven does this by continuously delivering Configuration Intelligence: a stream of high-fidelity insights about actual detailed configurations and changes—initiated by the systems or users—across infrastructure, applications, services, data centers, and public cloud environments.

How Evolven Enables Safe, Autonomous IT Operations

1. **Serving as the Source of Environmental Truth**

In an agentic IT landscape, decision quality is entirely dependent on the quality of the context. Evolven acts as the definitive source of environmental truth, capturing the full lifecycle of configuration changes across infrastructure, applications, and services in near real time. It reconciles what was deployed with what exists in the environment now, capturing both traditional drift caused by post-deployment edits and emerging forms of agentic drift resulting from recursive, autonomous changes. This provides a comprehensive and accurate view of both the current state and the path taken to achieve it.

Unlike traditional CMDBs, which rely on periodic updates, manual inputs, and brittle integrations, Evolven continuously ingests, reconciles, and correlates configuration data across the full operational stack. It captures parameters, deployment artifacts, runtime state, environmental variables, and policy-driven changes—whether introduced manually, via automation, or through autonomous agents. Every change is time-aligned and cross-referenced with logs, incidents, alerts, and performance data, creating a living, contextualized record of the environment.

Rather than evolving into a next-gen CMDB, Evolven redefines what a system of record for operational state must be. In agentic IT, the role traditionally played by CMDBs—holding a trusted view of the environment—is no longer viable in static form. Evolven replaces this with a dynamic, continuously validated data and control layers that serve the same foundational purpose, but in a way aligned with autonomous, real-time, and policy-driven operations.

This persistent, unified configuration awareness allows AI agents to base decisions not on inferred assumptions or noisy telemetry, but on verified ground truth. Agents can determine whether a recent

regression is due to a misaligned deployment, confirm that an environment matches baseline expectations before executing a fix, or reject an action that would violate stability constraints. Evolven provides the factual layer needed for agents to act safely, confidently, and effectively.

Evolven provides a continuous, unified record of all configurations including infrastructure modifications, deployment outcomes, and policy adjustments. This enables AI agents to reason over actual system state, not just symptoms. Agents can validate proposed actions, correlate changes to incidents, and make safer, context-aware decisions.

2. **Acting as a Specialized Agent for Risk and Drift Intelligence Within Multi-Agent Architectures**

In dynamic, cloud-native environments, configuration changes happen continuously. Changes are driven by CI/CD pipelines, infrastructure-as-code deployments, container orchestration, and, increasingly, by autonomous AI agents. Within this complex ecosystem Evolven operates as a specialized configuration intelligence agent, continuously assessing the risk associated with change and monitoring for signs of drift, even in ephemeral and rapidly scaling environments like Kubernetes clusters or serverless platforms.

Unlike legacy tools that rely on static inventories, infrequent scans or manually updated baselines, Evolven is purpose built for fluid, continuously evolving systems. It distinguishes between intended automation and unintended divergence, identifying subtle and often overlooked mismatches such as misaligned Kubernetes manifest between staging and production, residual drift from overlapping IaC executions, or parameter inconsistencies introduced by multiple agents acting concurrently.

This is where Evolven plays a critical role in countering agentic drift. Without oversight, autonomous agents can take a series of contextually valid actions that, over time, diverge from operational baselines, leading the system into instability or noncompliance. Evolven acts as a real-time stabilizer, recognizing when agents begin to follow their own logic “down a rabbit hole” and surfacing these recursive deviations before risk accumulates.

As a specialized agent, Evolven autonomously classifies detected changes by severity, scope, and impact, distinguishing low-risk noise from critical misconfigurations. It can recognize drift that's acceptable in one environment but problematic in another, such as a memory limit increase that's safe in dev but unsustainable in production. This nuanced risk awareness allows Evolven to prioritize alerts, trigger automated policy enforcement, or escalate only when thresholds for instability, non-compliance, or performance degradation are met. In this role, Evolven acts as a continuous, context-aware filter, keeping agentic systems agile without letting them become chaotic.

3. **Enabling Explainability and Auditability in AI-Driven Ops**

As AI agents begin to make autonomous changes, enterprises need not just observability but explainability. Evolven provides the forensic timeline that underpins this capability, logging every configuration change along with its origin, context, and risk profile. Whether triggered by a human, an agent, or an automated pipeline, each change is recorded with metadata that includes when, how, and why it occurred.

This data enables backward traceability. If a performance issue emerges, Evolven can correlate it with configuration events that occurred in the minutes, hours, or days before—highlighting risky or unexpected changes and enabling fast, accurate root cause analysis. If a compliance audit requires justification for why a policy was violated or when a sensitive setting changed, Evolven can provide a comprehensive change narrative including the actor, intent, and impact.

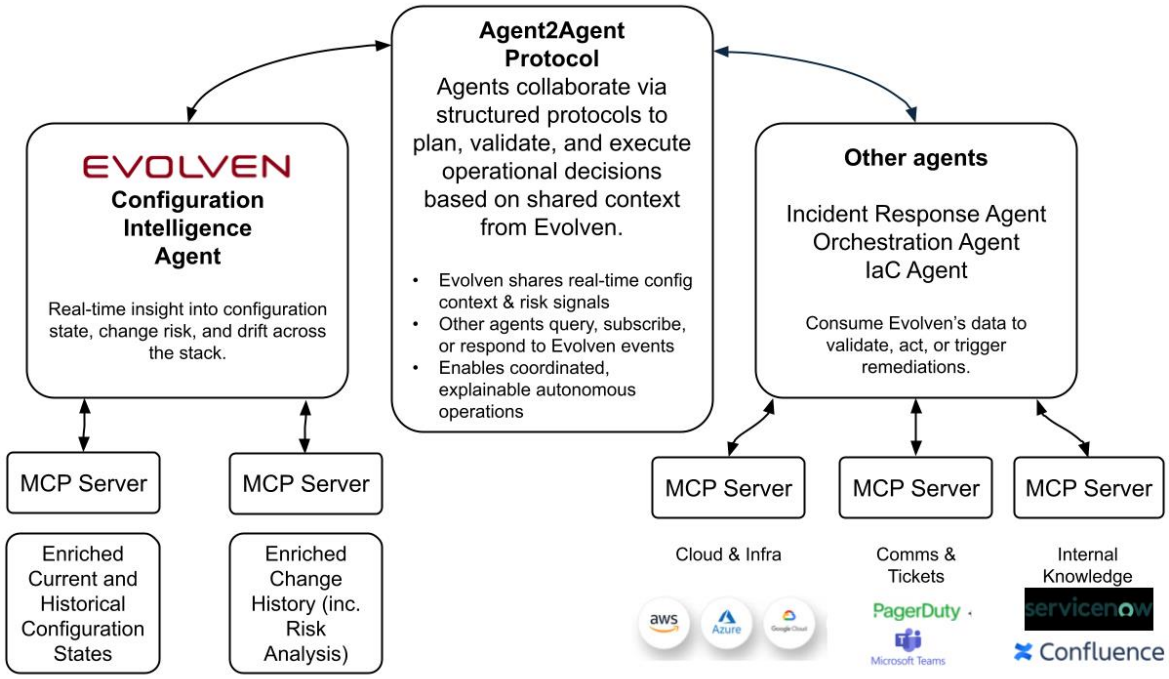
Beyond reactive forensics, this historical awareness also supports learning and governance. Organizations can train agents not just on what worked, but on what *should* have happened based on policies and previous outcomes. Evolven enables continuous refinement of agent behavior through transparent records and actionable insights, ensuring that autonomous operations remain safe, aligned, and accountable.

4. **Providing a Secure, Interoperable Data Layer for Agent Consumption**

Evolven is built to plug directly into the agentic and automation ecosystems that are redefining IT operations. It exposes its intelligence through modern, secure interfaces including RESTful APIs, event-driven feeds, and native integrations. Crucially, it supports agentic protocols, such as the Model Context Protocol (MCP), and Agent-to-Agent communication layers, allowing Evolven to participate fully in orchestrated workflows.

This interoperability enables Evolven to serve as a context provider for various AI agents and platforms. Observability agents can query configuration changes before raising alerts, remediation agents can validate rollback candidates, and compliance agents can subscribe to policy violation events. Evolven's insights aren't locked in a dashboard—they're live, machine-readable, effectively supporting decisions made by IT agentic framework.

By being composable and integration-ready, Evolven doesn't force organizations to adopt a single vendor's vision of automation. Instead, it enhances whatever tooling and architecture they already have—acting as a modular brain that injects configuration awareness into every layer of AI-driven operations. This flexibility makes it ideal for enterprises transitioning gradually into agentic operations, as well as those scaling to full autonomy.



To illustrate the role of Evolven and its integration into an agentic framework, let's consider the following example. Soon after a recent application deployment, an AI observability agent detects a spike in transaction latency. It communicates the spike to the AI remediation agent. The obvious decision would be to roll back the deployment. However, before initiating rollback, the agent queries Evolven for recent configuration changes. Evolven identifies a memory limit increase in the payments microservice—introduced outside the deployment flow by another agent reacting to workload conditions—and flags it as high-risk. Since this change is not part of the deployed artifact, rollback wouldn't revert it and might destabilize the environment. The agent escalates the issue with full context, and logs justification. Evolven's continuous configuration intelligence enables agents to differentiate between helpful intent and risky impact, ensuring safe, explainable operations.

Strategic Benefits & Next Steps

Evolven Enables AI Autonomy Without Losing Control

As enterprises embrace agentic IT operations, the challenge shifts from whether AI agents can act autonomously to whether they can do so safely, transparently, and in alignment with enterprise policy. Evolven turns that challenge into an advantage. By anchoring autonomous decisions in continuously updated configuration intelligence, it transforms AI operations from opaque and brittle into explainable and resilient.

Organizations that integrate Evolven into their agentic frameworks gain the ability to:

- Minimize mean time to resolution (MTTR) through immediate root cause correlation
- Prevent cascading failures by flagging risky or unstable changes before they propagate
- Enforce continuous compliance through full traceability of all configuration activity
- Build trust in autonomous systems through audit-ready transparency and explainability

Strategic Benefits at a Glance

- **Faster, Safer Decisions: Agents validate actions against current configuration data.**
- **Lower MTTR: Direct correlation between change and incident accelerates resolution.**
- **Continuous Compliance: Risk scoring and policy alignment out of the box.**
- **Explainable Autonomy: Full forensic history of every change and agent action.**
- **Cross-Platform Resilience: Works seamlessly across cloud, hybrid, and legacy infrastructure.**

Positioning Evolven in Your Agentic Stack

Evolven is not just another monitoring or analytics tool. It is a specialized configuration intelligence agent and a foundational component of your autonomous architecture. Evolven provides both the data and operational capabilities needed to track, assess, and respond to change, thereby serving as the system of record, context engine, and risk interpreter. It validates decisions, enforces policy boundaries, explains outcomes, and ensures every action taken by an agent is grounded in current, trusted configuration insight. In this role, Evolven balances autonomy with control, empowering agentic systems to act faster, safer, and with accountability.

Next Steps: Preparing Your Environment for Agentic IT

As you evaluate or scale your investment in agentic operations, ask:

- Do your agents have up-to-date visibility into detailed configuration state and actual granular changes?
- Can your team explain and audit every decision made by an autonomous system?
- Are your AI and automation strategies built on a trusted, context-rich foundation?

If the answer to any of these is "no," Evolven should be a strategic cornerstone of your roadmap.

📧 **For more information, visit www.evolven.com , or contact us at info@evolven.com .

EVOLVEN