

Discover and govern your digital assets and supply chain

Eliminate digital blind spots across subsidiaries, suppliers, and shadow IT.
Pre-emptive cyber defence from day 1, with zero integration.

Ask your teams, ‘How many domains and subdomains do we truly own?’ If the answer isn’t immediate, you are facing the same governance paradox as every complex enterprise.

Klarvantage® provides an external, passive view, so you can govern what is already public, closing the gap between your perceived attack surface and its sprawling, actual reality.

This gap is where systemic risk thrives. It shows up as unsecured email vulnerable to spoofing, unmanaged assets with expired certificates, and critical infrastructure still pointing to the domains of offboarded, ‘dead’ suppliers. These are attacker-ready footholds, discoverable by anyone, including auditors and oversight bodies.

Built for global scale and trust on Google Cloud

Klarvantage’s Namespace Command platform eliminates this visibility paradox. Its core promises are zero integration, AI-first capabilities, passive discovery, SSO access, and external-first visibility. Unlike traditional tools that require months of integration and can only see known assets, Namespace Command delivers complete external visibility from day 1. Klarvantage tracks over 7 billion identifiers using Google’s cloud and AI infrastructure.

The discovery engine is engineered on Google Cloud to meet extreme demands for scale and security. It uses Google’s secure-by-design infrastructure to protect sensitive organisational intelligence during processing, and operates within a private network environment, shielded from external web attacks and other malicious threats. Klarvantage is secure by design.

This foundation is matched by enterprise-grade assurance. Data residency options across the EU, UK, and the US ensure compliance with data sovereignty regulations. Immutable, time-locked backups and audited logs provide durable proof of integrity for oversight bodies. Together, this gives enterprises and governments the confidence to manage governance, risk, and compliance at global scale.



360°

*Transform complexity into clarity
and control.*

*More digital assets and suppliers are
typically discovered than
organisations believed they owned.*

Klarvantage’s initial discovery frequently reveals hundreds of forgotten subdomains, dozens of unknown suppliers, and certificates spanning multiple countries where there were previously only blind spots. Klarvantage’s proprietary approach and AI capabilities make this level of insight possible.

This isn’t a failure of diligence; it is a natural consequence of enterprise complexity. By providing a complete, external view, Klarvantage lets you finally govern the attack surface you already have, but couldn’t see.

WHAT KLARVANT DELIVERS

CAPABILITIES	PLATFORM	OUTCOMES
✓ Automated discovery of your entire digital footprint ✓ Continuous monitoring for supply chain and brand risk ✓ Actionable intelligence to close governance gaps	✓ Enterprise-grade security and threat protection ✓ Global scale and high-performance infrastructure ✓ Built-in compliance and data residency controls	✓ Complete visibility across your entire namespace ✓ Proactive reduction of brand and supplier risk ✓ Auditable proof of governance and control

Achieve total visibility, from day 1

Klarvant provides ‘x-ray vision’ through your corporate structure and beyond, mapping the complete external attack surface across your subsidiaries, collaborator networks, and global supply chain from day 1, not months. By tracking more than 7 billion identifiers, Klarvant analyses what is relevant using AI capabilities. The platform often discovers hundreds of unmanaged domains, dozens of unknown suppliers, and certificates spanning multiple countries where there were previously only blind spots. This gives you a continuously updated asset inventory: the definitive basis for enterprise-wide governance.

Secure the blind spot: your digital supply chain

Your biggest unknown risk is often your third-party ecosystem. As a global company might discover, an abandoned supplier domain can be weaponised for attacks. Klarvant’s Supplier Intelligence and Certificates & Email Security modules neutralise this threat. Klarvant provides continuous monitoring of the supplier lifecycle, automatically detecting expired domains, weak email security (unenforced DMARC and SPF), and unauthorised assets, so you can proactively prevent supply chain attacks.

Convert evidence into auditable governance

Klarvant turns data into action, powered by its Automated Analysts. This AI-driven engine sifts through your most complex data to surface the critical insights that matter most, delivering them how your team wants them: through audio briefings, text presentations, APIs, or direct to automated agents. From there, the Gap Management module converts every AI-surfaced finding into an auditable campaign with clear ownership and SLAs. The KPI Dashboard translates this work into metrics the board understands: a real-time Posture Rating trend, resolved versus active vulnerabilities, and time to remediate.

‘Once you experience this level of visibility, you can’t unsee it, and you won’t want to operate without it.’

LUIS NOVELLA · CEO, KLARVANT

Unlock instant governance

Hidden risks are your greatest liability, and because they are public, anyone can discover your gaps before you do. Klarvant Namespace Command on Google Cloud replaces uncertainty with auditable control. Provide your primary domains, and Namespace Command returns a live namespace map and posture rating baseline within days.

REQUEST YOUR NAMESPACE MAP

sales@klarvant.com