

Discover & Govern Your Digital Assets and Supply Chain

Eliminate digital blind spots across subsidiaries, suppliers, and shadow IT—Preemptive Cyber Defense from day one with zero integration.

Ask your teams, “How many domains and subdomains do we truly own?” If the answer isn't immediate, you're facing the same governance paradox as every complex enterprise. NodeZro 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.

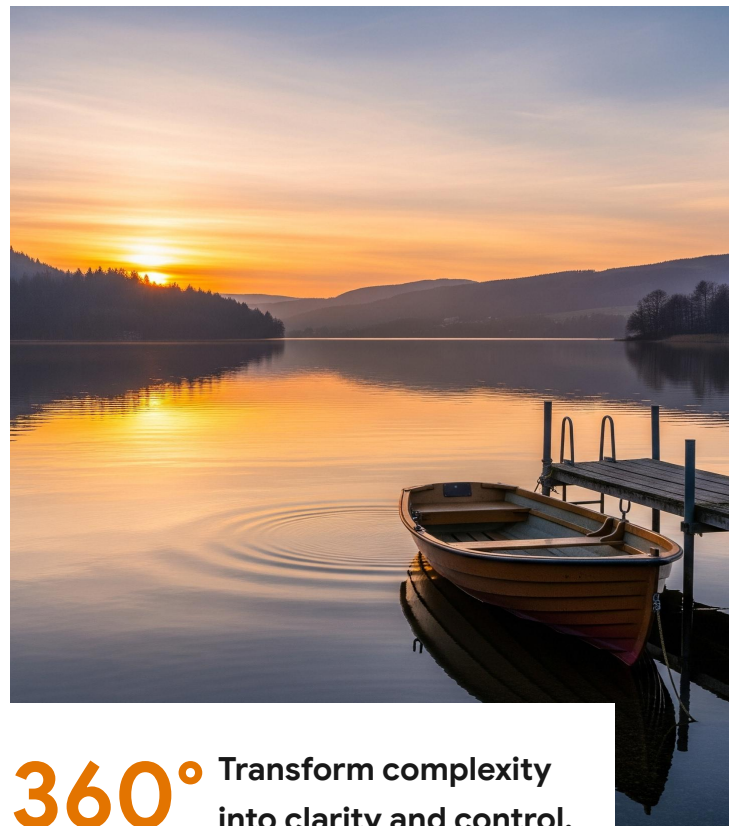
This gap is where systemic risk thrives. It's seen in unsecured email vulnerable to spoofing, unmanaged assets with expired certificates, and critical infrastructure pointing to the domains of offboarded, 'dead' suppliers. These are attacker-ready footholds, discoverable by anyone including auditors and oversight bodies).

Engineered for Global Scale and Trust on Google Cloud

NodeZro's Namespace Command Centre (NCC) 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, NCC flips this model to provide complete external visibility from day one. NodeZro tracks over 7 billion identifiers using Google's cloud and AI infrastructure.

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

This powerful technical foundation is matched by enterprise-grade assurance. Data residency options across the EU, UK, SG, and the US ensure compliance with data sovereignty regulations. Immutable, time-locked backups and audited logs provide durable proof of integrity for oversight bodies. This powerful combination 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 organizations believed they owned.

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

This isn't a failure of diligence; it's a natural consequence of enterprise complexity. By providing a complete, external view, NodeZro allows you to finally govern the attack surface you already have, but couldn't see.



Achieve Total Visibility, Instantly

NodeZro provides "x-ray vision" through your corporate structure and beyond. Mapping the complete external attack surface across your subsidiaries, partner networks, and global supply chain in hours, not months. By tracking 7 billion+ identifiers, NodeZro analyses what's relevant by leveraging AI capabilities.

The platform often discovers hundreds of unmanaged domains, dozens of unknown suppliers, and certificates spanning multiple countries where previously there were only blind spots. This gives you a continuously updated asset inventory, forming 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 weaponized for attacks. NodeZro's Supplier Intelligence and Certificates & Email Security modules neutralize this threat.

NodeZro provides continuous monitoring of the supplier lifecycle, automatically detecting expired domains, weak email security (unenforced DMARC/SPF), and unauthorized assets, allowing you to proactively prevent supply chain attacks.

Convert Evidence into Auditable Governance

NodeZro 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, NodeZro's 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 Exposure Score Trend, resolved vs. 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, NodeZro

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



Unlock Instant Governance
sales@nodezro.com