sonet.io

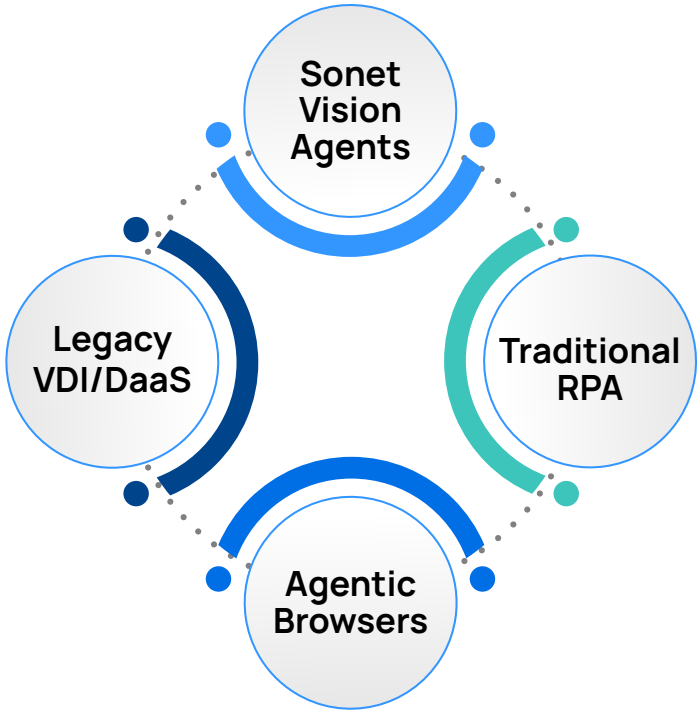
Governed Enterprise Automation: A Comparison Guide

As enterprises expand AI-driven automation, the challenge is no longer just making agents work. It is making them work inside a model that security, compliance, and IT can govern in production.

Legacy VDI and DaaS can contain applications, but they bring infrastructure and operational overhead. Traditional RPA can automate structured workflows, but often depends on authored logic, runners, and ongoing maintenance. Agentic browsers can navigate the web autonomously, but they are typically built for open-web interaction rather than enterprise control.

Sonet Vision Agents take a different approach: governed automation inside a controlled browser workspace with centralized policy, session isolation, and audit-ready visibility.

Comparing Four Approaches



Architecture and Control

	Legacy VDI / DaaS	Traditional RPA	Agentic Browsers	Sonet Vision Agents
Execution model	Delivers centralized desktops or remote apps for users; not purpose-built for native agent execution	Executes authored automations through bots, runners, and orchestrators	Designed primarily for single-user, human-in-the-loop web browsing and task execution	Run inside a secure, Sonet-controlled browser workspace and can execute many Vision Agents in parallel
Control boundary	Contained in a remote desktop or app session, with policy shaped by the VDI/DaaS stack	Governed through the bot runtime, orchestration layer, and target-system permissions	Operate outside enterprise app delivery, often with user credentials and browser-native context	Fully contained within the enterprise workspace, with identity, access, and policy enforced centrally
Integration approach	Accesses apps through hosted desktops/apps, but often still depends on image, connector, and environment setup	Uses UI automation, selectors, scripts, APIs, and platform integrations depending on the workflow	Typically requires open internet access to interpret, navigate, and act on websites	Operate directly on applications inside the workspace with no API or MCP access required
Ease of creation	Higher setup burden; not designed for fast business-user automation creation	Higher barrier; automations usually require workflow design, testing, and ongoing upkeep	Lower barrier for individual browsing tasks, but limited for governed enterprise automation	Workflows can be created by recording an expert completing the task once, reducing prompt-heavy setup and lowering adoption barriers

Security and Isolation

	Legacy VDI / DaaS	Traditional RPA	Agentic Browsers	Sonet Vision Agents
Isolation level	Strong remote-session isolation, though enforcement varies by platform, client, and policy configuration	Depends on where bots run; isolation is not inherent to the model	Limited isolation; activity occurs in a browser exposed to prompt injection, session hijacking, and token reuse risks	Full session isolation within the Sonet workspace; no data touches the endpoint
Data protection	Can support strong controls, but often requires layered configuration for watermarking, clipboard, file transfer, and redirection	Protection depends on bot environment, vaulting, and surrounding platform controls	No enterprise-grade DLP or session controls; activity on live internet pages can expose sensitive data	Built-in DLP, watermarking, and clipboard controls applied to all agent sessions
Credential handling	Credentials are often managed through enterprise identity and remote-session controls, but still tied to desktop delivery architecture	Usually handled through vaults, service accounts, and orchestrator-managed credentials	Commonly relies on direct sign-in to external services with user-held credentials	Credentials stay within the controlled workspace and inherit enterprise access policy rather than being exposed through local browser execution
Support beyond the browser	Yes	Yes	No	Yes

Governance and Policy Control

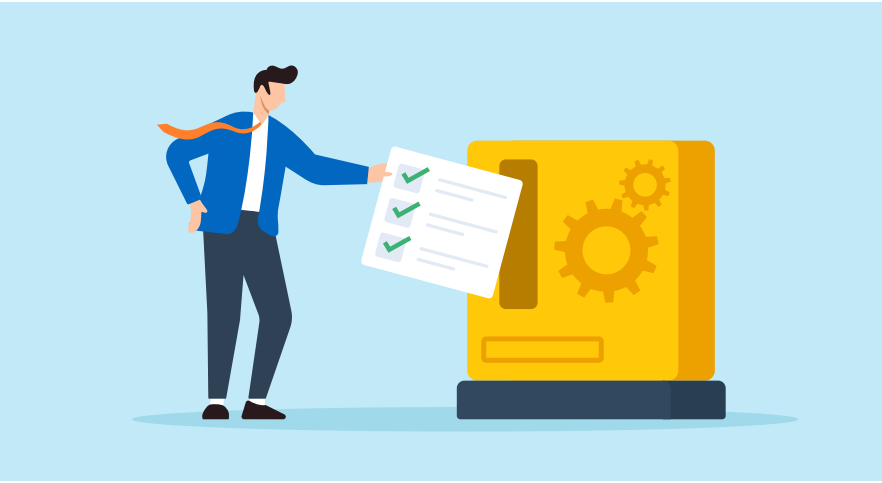
	Legacy VDI / DaaS	Traditional RPA	Agentic Browsers	Sonet Vision Agents
Administrative oversight	Centralized admin control for desktops, apps, and session policies, but tied to infrastructure operations	Strong governance through orchestrators, RBAC, approvals, queues, and credential controls	Minimal policy support; often managed through user settings or limited vendor controls	Centralized control through enterprise policy; admins define what apps and actions each Vision Agent can access
Identity and access	Usually integrated with enterprise IdPs and access policies	Can integrate with enterprise identity, but often through separate setup and role design	Limited or no SSO integration; users often authenticate directly to external services	Integrated with corporate IdPs such as Okta and Entra ID; agents inherit least-privilege policies
Compliance alignment	Can align to regulated environments, but proof, controls, and retention often depend on platform-specific configuration	Can support audit and control requirements, but usually through a heavier operating model	Limited or no built-in compliance support for controlled, evidence-based operation	Designed for regulated environments where actions must be logged, recorded, and approved inside a private stack

Observability and Auditability

	Legacy VDI / DaaS	Traditional RPA	Agentic Browsers	Sonet Vision Agents
Session recording	Available in some platforms, but often varies by vendor and may require added components or services	Audit logs are common, but full replay or recording varies by platform	No integrated session recording or replay capability	Every session is recorded with event-level detail, including a step-by-step activity trail, screenshots, and logical steps for audit and playback
Event visibility	Good admin and control-plane visibility; session-level visibility varies across stacks	Strong process-level logging through the orchestration layer	No standardized telemetry or audit events; visibility depends on vendor access	Centralized dashboard for all event logs and sessions, exportable to SIEM for full traceability
Incident response	Admins can terminate sessions and revoke access, but response is tied to the desktop/ session stack	Response happens through the RPA control plane and operator workflows	No enterprise kill switch or live session control	Admins can terminate agent sessions instantly

Enterprise Readiness

	Legacy VDI / DaaS	Traditional RPA	Agentic Browsers	Sonet Vision Agents
Deployment	Requires standing up and maintaining desktop/ app delivery environments, policies, and supporting infrastructure	Requires platform deployment, runners, credential setup, and automation lifecycle management	Requires installing and managing an alternative browser	SaaS-based; no endpoint software or extensions required
Scalability	Can scale, but capacity planning, image management, and cost control remain ongoing concerns	Scales through bots and orchestrators, but with meaningful operational overhead	Lacks centralized management and version control for large deployments	Scales securely across thousands of AI agents with centralized policies
Use cases	Secure access to desktops, Windows apps, and some legacy environments	Highly structured, repeatable business processes across systems	Consumer research and general web exploration	Secure automation across Windows, web, and legacy apps
Maturity	Established enterprise category, but infrastructure-heavy and operationally complex	Mature enterprise automation category, but maintenance-heavy for changing workflows	Early-stage technology with unresolved security and governance challenges	Enterprise-ready with zero trust controls, compliance, and audit



The Modern Alternative

For IT and security leaders evaluating AI-assisted automation, Sonet Vision Agents provide a more practical path forward.

Legacy VDI/DaaS can provide control, but with too much infrastructure. Traditional RPA can automate workflows, but often with too much design and maintenance overhead. Agentic browsers can move quickly, but without the governance, containment, and auditability enterprise teams need.

Sonet Vision Agents are built differently. They operate entirely inside a controlled browser workspace with full session isolation, centralized policy enforcement, and complete observability. They work across legacy and modern applications alike, while maintaining the same zero trust and compliance standards enterprises already require for human access.

Everything you need, nothing you don't.

- **Secure automation across all applications**
- **Centralized policy and audit visibility**
- **No APIs, no extensions, no new attack surface**

Schedule a Demo:
To see Sonet.io in action.

Talk to Our Team

sonet.io

Secure Workspaces for Humans and AI

sales@sonet.io

Find us online at **sonet.io**

3031 Tisch Way, 110 Plaza West
San Jose, CA 95128