SOLUTION BRIEF

Reducing Risk, Increasing Resilience: A Decision Maker's Guide to Puppet Core

Secure Scale for Modern Infrastructure

If you're responsible for keeping your infrastructure secure and compliant, you're likely feeling the pressure of an environment that's growing more complex by the day. You're navigating AI adoption, expanding cloud footprints, shrinking teams, and the reality that even one overlooked configuration can introduce serious risk. Manual compliance can't keep pace, and every gap creates exposure that threatens uptime, audits, and the trust your business depends on.

You shouldn't have to worry that a single missed update or unexpected drift could disrupt operations or put your organization at risk.

You deserve tools that help you stay ahead of threats, strengthen resilience, and protect the systems your business runs on.

Running mission-critical environments on Open Source Puppet still carries the burden of patching vulnerabilities, maintaining compliance, and protecting complex estates at scale. Even well-run open source environments face real exposure when a critical CVE appears without a fast, supported fix, putting operational continuity and business resilience at risk.

Puppet Core eliminates that risk by providing **vendor-backed software** with **hardened binaries**, and **guaranteed SLAs** for critical and high severity CVEs. **Certified builds** let you avoid the overhead of building, maintaining, and certifying Open Source Puppet. **Security Compliance Enforcement** capabilities continuously align infrastructure with widely-adopted security standards. And, to ensure you get started quickly, training engagements with **certified Puppet Engineers** are included.

It shifts accountability from internal teams to a trusted, enterprise-grade platform; ensuring consistent, compliant, and secure infrastructure across hybrid and multi-cloud environments.

Why Organizations Choose Puppet Core

When you're managing complex, fast-growing infrastructure, you need more than tools, you need confidence.

With Puppet Core you are implementing a vendor-backed solution, so you can automate with certainty, govern with clarity, and protect your environments without constantly worrying about what you might have missed.

With consistent desired-state enforcement, you can reduce configuration drift, cut provisioning time, and maintain stable environments across hybrid and multi-cloud infrastructures.

And when issues arise, Puppet Core has guaranteed SLAs and vendor backing to ensure rapid remediation, reducing the risk of downtime and protecting business continuity.

Get Started Off Right

With Puppet Core, you get peace of mind knowing you have access to the latest updates and are using a stable, vendor-backed solution to keep your critical systems running smoothly.

To ensure you get started off right, Puppet Core includes a **training engagement** where you'll spend up to 4 hours with a Certified Puppet Engineer.

In addition, you will have access to a private support portal, where you can submit tickets for product defects and vulnerability patch requests for the software and 3rd party libraries. Any CVE with a CVSS score of 7 or higher has a guaranteed SLA. You can also access free online documentation, resources, and modules.

The Bottom Line: Which Puppet Solution Your Organization Should Choose

Choose Open Source Puppet if:

- You have minimal compliance or regulatory requirements
- Your team prefers to move fast without formal SLAs or vendor accountability
- Your infrastructure is relatively simple and not spread across hybrid/cloud environments
- You don't require oversight of network devices and edge systems

Choose Puppet Core if:

- Your organization operates regulated, audit-sensitive, or risk-intolerant environments
- You need tested releases with secure, signed binaries
- You need guaranteed SLAs for critical and high severity CVEs
- You value a trusted, established vendor partner with documented security controls and testing standards

Category	Open Source Puppet (OSP)	Puppet Core
Security	No guaranteed CVE remediation: fixes depend on community availability	**Guaranteed CVE SLAs**, vendor-backed remediation, hardened & signed binaries
Risk Posture	Risk is fully owned by the internal team	**Risk transferred to vendor**, reducing exposure and liability
Compliance	Manual policy definition for CIS Benchmarks and DISA STIGs	**Built-in enforcement** of CIS Benchmarks & DISA STIGs. **Automated drift correction** through continuous desired state enforcement
Operational Continuity	Operational continuity relies on internal processes for assessing and addressing risk	**Enterprise-grade stability** supported by predictable updates and vendor accountability
Support	No official defect or vulnerability support: issues handled in-house or via community	**24/7, ticket-based support** (follow the sun) for product defects and vulnerability patches
Scalability	Scales effectively, with scale outcomes owned by internal teams	**Optimized for large, complex estates** with vendor-backed reliability and predictability
Maintenance Burden	Teams must build, maintain, patch, test, and secure all components, and 3rd party libraries.	**Vendor-managed testing and maintenance**, reducing overhead and firefighting
Release Cadence	Depends on community contributions	**Predictable, SLA-aligned release cycle** with urgent patches as needed
Time-to-Value	Depends on internal prioritization, testing, and deployment timelines	**Reduce delays and uncertainty** with predictable releases and defect support
Ideal For	Teams with low compliance requirements and greater risk tolerance	Organizations running **critical, large-scale, compliance-centric environments**

Puppet Edge: Take Automation Even Further

As infrastructure becomes more distributed across data centers, cloud environments, remote sites, and edge locations, maintaining consistent visibility and governance context becomes increasingly difficult. These environments are often managed separately, leading to fragmented oversight, inconsistent understanding of risk, and limited insight into how standards are applied. The result is increased uncertainty, a broader attack surface, and greater exposure during audits.

What if you could extend the same governance context and operational visibility you rely on in core environments to every endpoint across your estate?

With a Puppet Core commercial license, you can add Puppet Edge as a premium capability that extends the governance model of Puppet Core to network and edge infrastructure. Rather than treating these systems as isolated environments, Puppet Edge brings them into a unified view, enabling consistent visibility, shared standards, and centralized insight across locations that are traditionally difficult to observe.

When paired with Puppet Core, Puppet Edge helps organizations better understand configuration state and risk exposure across distributed environments. This unified, policy-aware visibility supports governance initiatives, improves confidence during audits, and enables teams to make informed decisions as infrastructure continues to expand beyond the data center.

Why Puppet?

Modern IT environments demand intelligent, automated governance that scales. Puppet delivers the reliability, stability, security, and compliance your organization needs to confidently keep pace with rapid technology change.

Take the next step:

Talk to an Expert ▶

puppet.com/contact

About Perforce

The best-run DevOps teams in the world choose Perforce. Powered by advanced technology, including powerful AI that takes you from AI ambition to real results, the Perforce suite is purpose-built to handle complexity, maintain speed without compromise, and ensure end-to-end integrity across your DevOps toolchain. With a global footprint spanning more than 80 countries and including over 75% of the Fortune 100, Perforce is the trusted partner for innovation. Harness the power of AI and accelerate your technology delivery without shortcuts. Build, scale, and innovate with Perforce—where efficiency meets intelligence.