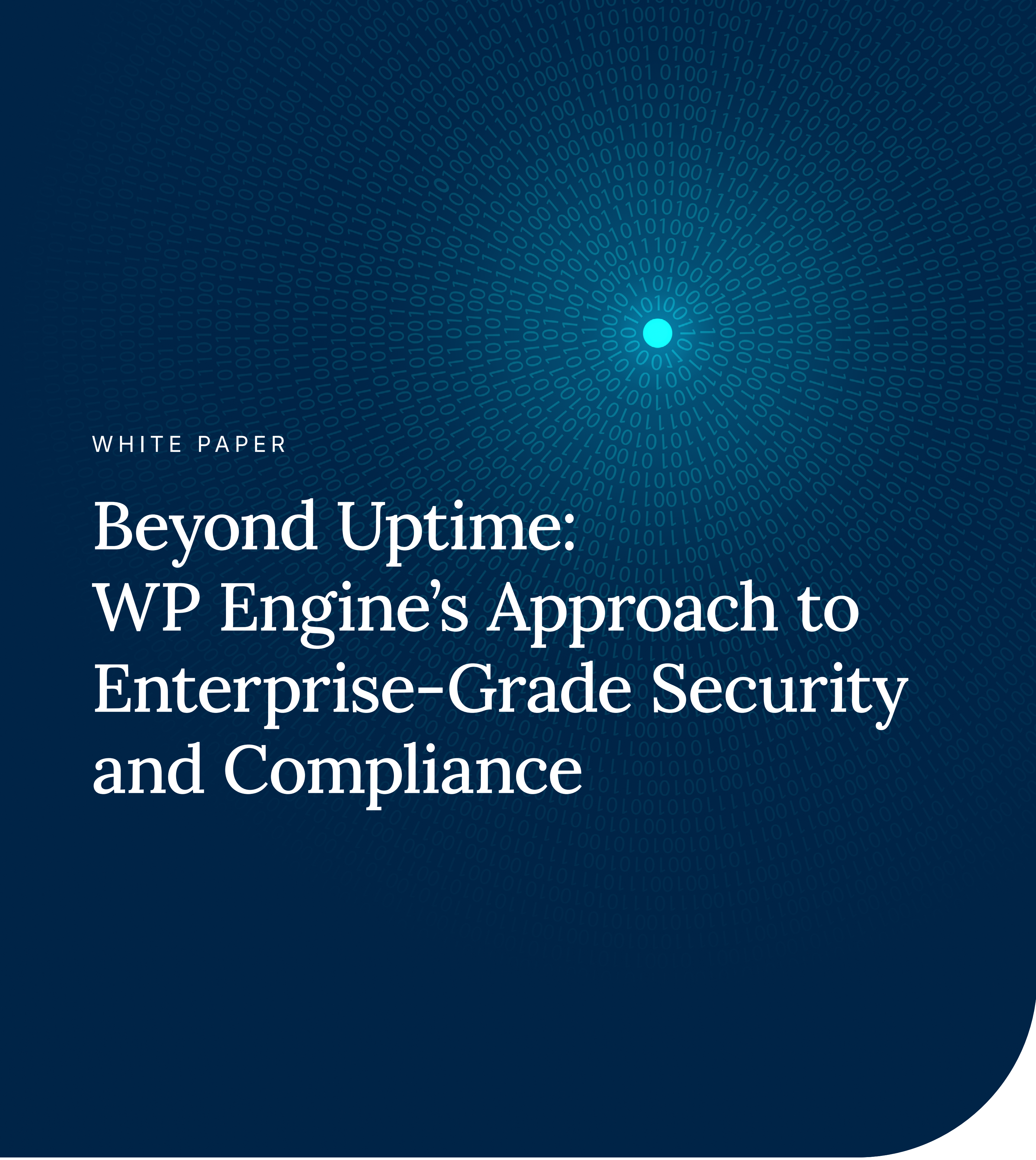
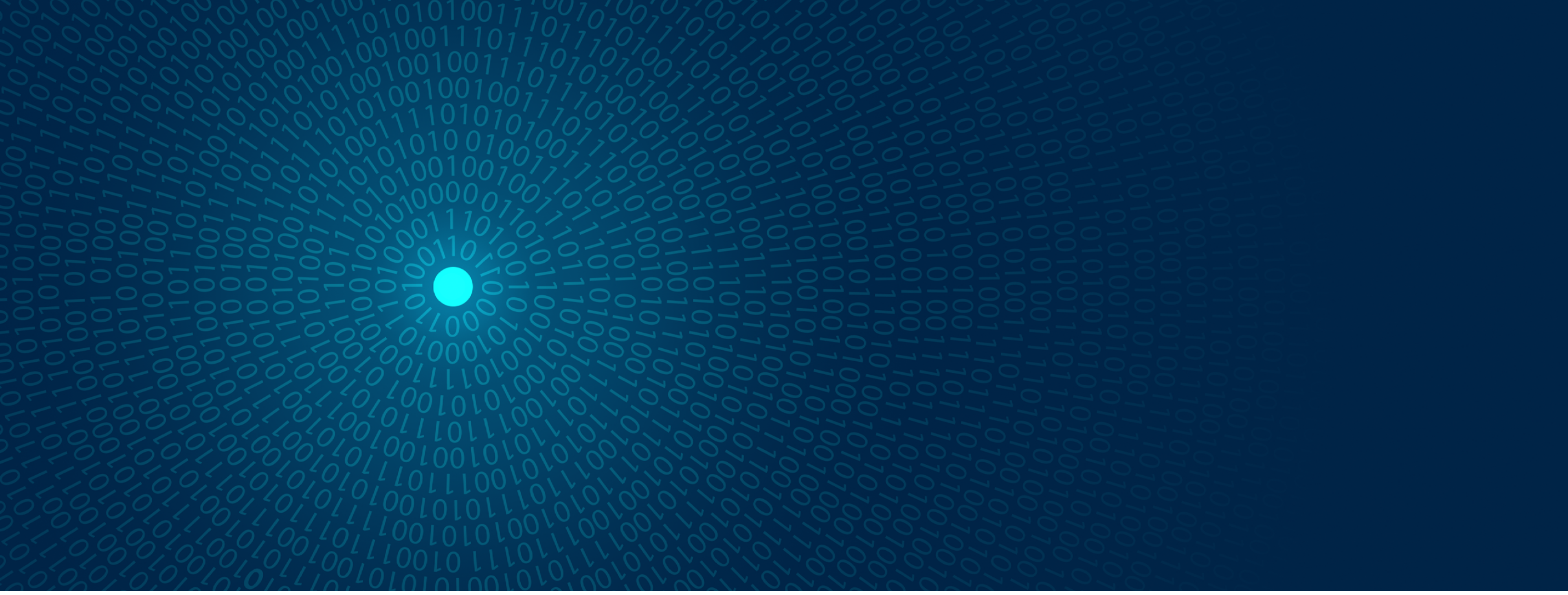


WHITE PAPER

Beyond Uptime: WP Engine’s Approach to Enterprise-Grade Security and Compliance



Taking steps to prevent cyber attacks is the *best* course of action in today's growing landscape of evolving threats.

For IT and development professionals, the reality of WordPress® security extends far beyond installing a simple firewall.[1] It is a relentless operational burden defined by the reactive, endless cycle of patching, the complexity of maintaining compliance across fragmented systems, and the underlying anxiety that a single, unmitigated zero-day exploit could cause catastrophic downtime. This constant focus on threat mitigation stifles innovation and consumes valuable engineering hours that should be spent on growth initiatives.

In this paper, we shift the conversation from generalized "best practices" to a concrete, enterprise-grade security framework. Achieving robust security is not a checklist of individual features. It starts with your organization committing to processes and procedures that mitigate data threats and seamlessly integrates a multi-layered security approach.

In the following chapters, we will detail a modern security framework built on three pillars:

- **Defense in depth at the architectural level**
- **Compliance as a strategic asset**
- **The true cost of in-house security**

This strategic approach is designed to eliminate the operational overhead of self-managed infrastructure security, empowering you and your team to shift focus from constant defense to confident digital acceleration. In other words, less time spent on maintenance, and more time spent on innovation.

[1] WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation. Uses of the WordPress® trademarks in this ebook are for identification purposes only and do not imply an endorsement by WordPress Foundation. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation.

Multi-layered security framework: Defense in depth

In enterprise-grade architecture, security is not a single point solution. It is a continuously monitored, coordinated strategy known as "Defense in Depth". This framework implements multiple, independent layers of security controls, so that if a threat actor bypasses one control, they are immediately met by the next.

For web applications, this framework is critical for insulating the valuable origin infrastructure from external threats. WP Engine's security framework operates across three distinct layers: the network Edge, the Application layer (WordPress core), and the underlying Platform.

Layer 1: Network edge security

The most effective security is filtering malicious traffic before it ever consumes resources on the origin server. This approach is fundamental to mitigating high-volume attacks like DDoS and common application-layer vulnerabilities, many of which map directly to the OWASP Top 10.

Advanced DDoS protection: Mitigation at layers 3 & 4

Distributed Denial-of-Service (DDoS) attacks attempt to overwhelm infrastructure capacity. WP Engine's proactive defense framework utilizes a vast, globally distributed network to absorb and mitigate these volumetric threats. Mitigation occurs at the network and transport layers (OSI Layers 3 and 4) to ensure that malicious traffic is dropped immediately, protecting the core infrastructure and maintaining site availability.

Managed web application firewall (WAF)

The WAF is your critical layer of application-level defense, positioned at the network edge to inspect and filter HTTP/S traffic before it reaches your WordPress application.

- **Zero-day filtering:** WP Engine's WAF is managed and automatically updated by a dedicated team. It uses shared threat intelligence gathered across millions of sites to identify emerging attack patterns and instantly deploy new rulesets, often mitigating zero-day threats before they can be exploited.
- **OWASP Top 10 defense:** The WAF provides specific protection against common web application vulnerabilities, including SQL injection and Cross-Site Scripting (XSS), by inspecting payloads and blocking suspicious requests at the edge.

SSL/TLS encryption enforcement

End-to-end encryption is a non-negotiable standard. We enforce strong SSL/TLS configuration, ensuring all data transmitted between the user, the edge, and the origin is secured, acting as a direct countermeasure against Adversary-in-the-Middle (AiTM) attacks.

Layer 2: Application-level security (WordPress core assurance)

This layer provides tools that extend security deep into the application, giving control back to the IT team without compromising the framework's integrity.

- **Smart Plugin Manager:** Recognizing that plugin vulnerabilities account for a significant portion of security incidents, WP Engine's Smart Plugin Manager automates plugin updates on a scheduled interval. Critically, it uses visual regression testing (VRT) powered by machine learning to confirm that updates pass without visually breaking the site, reducing update risk and eliminating a major manual burden for developers.
- **Plugin Vulnerability Scanning:** Daily plugin vulnerability scans notify customers by email and in the User Portal for continuous security awareness.

Layer 3: Platform-level protection (Automated maintenance & monitoring)

Security management is defined by consistency. This layer eliminates the engineering overhead of perpetual patching and scanning by automating maintenance and providing continuous, non-stop monitoring of the hosting environment.

- **Automated maintenance and upgrades:** WP Engine automatically manages platform updates, PHP upgrades, and security-focused WordPress core updates. This ensures your infrastructure stack remains current, eliminating one of the most common sources of exploitation: ***outdated dependencies.***
- **Proactive threat detection:** The platform is continuously monitored for malicious activity, allowing traffic to be instantly blocked and flagged. We leverage advanced scanning techniques to identify malware and privilege escalation attempts within the hosting environment.
- **Encrypted data backups:** Critical to disaster recovery and compliance, the platform performs automatic daily backups. All backup data is encrypted both in transit and at rest, providing a final, secure contingency against data corruption or loss.
- **Proprietary Firewall:** WP Engine's proprietary firewall automatically detects and mitigates malicious traffic.

The imperative of trust: Compliance & certifications

For any business dealing with sensitive customer data, compliance is a mandatory pillar of risk mitigation and a prerequisite for establishing vendor trust. Leveraging a secure platform minimizes exposure to regulatory risk and provides concrete, auditable proof of control efficacy.

SOC 2 Type II: The non-negotiable standard

The Service Organization Control 2 (SOC 2) Type II examination is the gold standard audit for any organization that stores customer data. It goes beyond merely having policies in place; the Type II designation confirms that the platform's security controls are not only designed correctly but have been operating effectively over a sustained period of time (typically six to twelve months).

For WP Engine, the SOC 2 Type II report specifically covers the Security and Availability trust services categories. This means a comprehensive, independent audit has verified two critical assurances for our customers:

- **Security:** Controls are in place to protect against unauthorized access (logical and physical), unauthorized disclosure of information, and other system abuse.
- **Availability:** Controls are in place to ensure the system is operational and available for use as committed or agreed, a direct guarantee of business continuity.

Assurance for the Customer: For your IT or development team, relying on a SOC 2 Type II compliant partner like WP Engine significantly offloads a major portion of vendor risk management. The audit report serves as verifiable evidence that the controls related to system protection and incident handling are robust, allowing internal teams to accelerate procurement and confidently satisfy their own regulatory and audit requirements without needing to perform deep, proprietary investigations into the infrastructure layer.

Adhering to global standards

Beyond the SOC 2 commitment, a robust security framework must integrate with other global standards that define best practices for security management and data protection.

The ISO/IEC 27001:2022 certification is an internationally recognized standard that outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system. This certification confirms that WP Engine operates security processes that are globally recognized, systematic, and follow a mature, risk-based approach to managing sensitive information.

By adhering to these rigorous standards, the platform is designed to assist with broader regulatory mandates, including general data protection regulations (like GDPR) and sector-specific requirements (such as protecting customer data for financial services). By providing encryption at rest, established data recovery protocols, and formalized access control procedures, the hosting platform provides the proven, foundational security layer necessary for clients to meet their own complex compliance obligations.

WP Engine's Audited Assurance: Eliminating Vendor Risk

A proven platform that guarantees security, availability, and performance

CERTIFIED ISO/IEC 27001:2022 CERTIFIED

Global Security Management

Confirms a systematic, risk-based approach to managing the Information Security Management System (ISMS), aligning with international best practices.

SOC 2 COMPLIANT TYPE II

Operating Effectiveness Guaranteed

Independent audit verifies the design and ***operating effectiveness*** of controls related to ***Security and Availability*** over a sustained period of time.

SOC 3 REPORT

Public Trust Report

A general-use, non-confidential report summarizing the full SOC 2 examination, ideal for quick vendor review and immediate assurance for procurement teams.

The true cost of in-house security

The true cost of digital risk is rarely defined by the final settlement of a breach. Instead, the real cost is embedded in the daily expenditure of high-value engineering time. For IT leadership, managing a self-hosted infrastructure means absorbing the perpetual, non-scaling operational costs of vulnerability management, patching cycles, and constant manual scanning. These hidden costs deplete budgets and, more critically, impose an opportunity cost on the entire development roadmap. The central financial question is not if you will spend money on security, but where you will spend it: on reactive, manual labor or on a comprehensive, automated platform.

Quantifying the labor burden: The security cost calculator

To move beyond anecdotal estimates, IT risk management requires quantifying the actual labor hours diverted from innovation toward maintenance. We offer a tool to help estimate the annual financial drain of self-managed security. This calculator provides a realistic, data-driven view of resource allocation by analyzing three core inputs against industry benchmarks for downtime risk:

- **Inputs:** Estimated hours per month spent on security patches, estimated hours per month spent on vulnerability scanning, and average developer/ security analyst salary.
- **Outputs:** The estimated annual cost of in-house security labor and the projected annual cost of downtime risk (using industry benchmarks for a mid-market site).

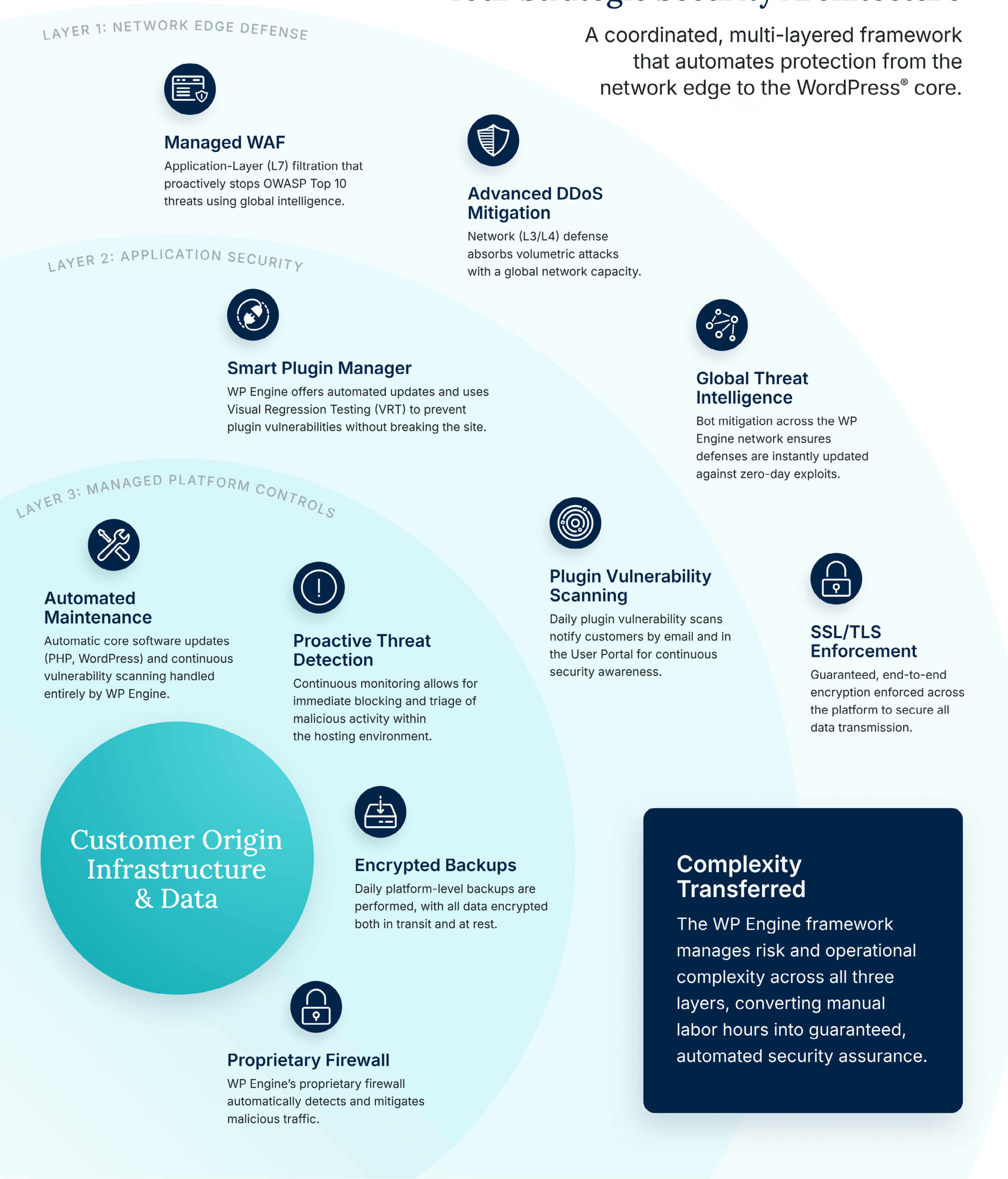
You can check out the calculator for yourself here.

The opportunity cost of manual maintenance

The single most significant drain on a technology organization is the forced reallocation of highly paid talent to low-leverage security tasks. Every hour a developer or engineer spends validating WordPress plugin updates, performing manual vulnerability scans, or triaging false-positive alerts is an hour taken away from core product development and revenue-generating feature work. By offloading the entire infrastructure security and compliance layer to a managed framework, your team can convert fixed, unpredictable operational spending into a scalable platform investment. This transfer of risk and responsibility frees up engineering capacity, allowing high-value personnel to focus on strategic initiatives rather than reactive maintenance.

WP Engine's Defense in Depth: Your Strategic Security Architecture

A coordinated, multi-layered framework that automates protection from the network edge to the WordPress® core.



LAYER 1: NETWORK EDGE DEFENSE

Managed WAF

Application-Layer (L7) filtration that proactively stops OWASP Top 10 threats using global intelligence.

Advanced DDoS Mitigation

Network (L3/L4) defense absorbs volumetric attacks with a global network capacity.

LAYER 2: APPLICATION SECURITY

Smart Plugin Manager

WP Engine offers automated updates and uses Visual Regression Testing (VRT) to prevent plugin vulnerabilities without breaking the site.

Global Threat Intelligence

Bot mitigation across the WP Engine network ensures defenses are instantly updated against zero-day exploits.

LAYER 3: MANAGED PLATFORM CONTROLS

Plugin Vulnerability Scanning

Daily plugin vulnerability scans notify customers by email and in the User Portal for continuous security awareness.

Automated Maintenance

Automatic core software updates (PHP, WordPress) and continuous vulnerability scanning handled entirely by WP Engine.

Proactive Threat Detection

Continuous monitoring allows for immediate blocking and triage of malicious activity within the hosting environment.

SSL/TLS Enforcement

Guaranteed, end-to-end encryption enforced across the platform to secure all data transmission.

Customer Origin Infrastructure & Data

Encrypted Backups

Daily platform-level backups are performed, with all data encrypted both in transit and at rest.

Proprietary Firewall

WP Engine’s proprietary firewall automatically detects and mitigates malicious traffic.

Complexity Transferred

The WP Engine framework manages risk and operational complexity across all three layers, converting manual labor hours into guaranteed, automated security assurance.

The unfair advantage: A dedicated security team

WP Engine maintains a full-time, dedicated Security and Compliance team—an internal advantage that translates directly into a massive operational relief for our customers. This team is focused entirely on the platform security layer, allowing our clients to fully offload the non-core, high-risk work associated with continuous platform governance.

In effect, this team functions as a risk management division, handling complex, ongoing security needs that typically consume internal IT resources:

- **Continuous threat landscape monitoring:** The team constantly scans the global security environment, legal mandates, and compliance standards, ensuring the platform remains protected against emerging vulnerabilities and evolving regulations.
- **Legal and compliance review:** They manage the exhaustive process of ongoing security reviews, audit preparation, and maintenance of certifications like SOC 2 and ISO 27001—eliminating the need for the client's internal legal or compliance officers to handle infrastructure-level validation.
- **Proactive incident response:** Should an event occur, this dedicated, expert team manages the full scope of triage, containment, and remediation, providing 24/7 coverage that few individual IT departments can afford to staff.

By transferring the responsibility for security governance, vulnerability management, and audit maintenance to WP Engine's specialized team, your IT and dev teams gain more than just features; they get their time back. This allows high-value engineers to shift their attention entirely to application development, feature innovation, and strategic business growth.

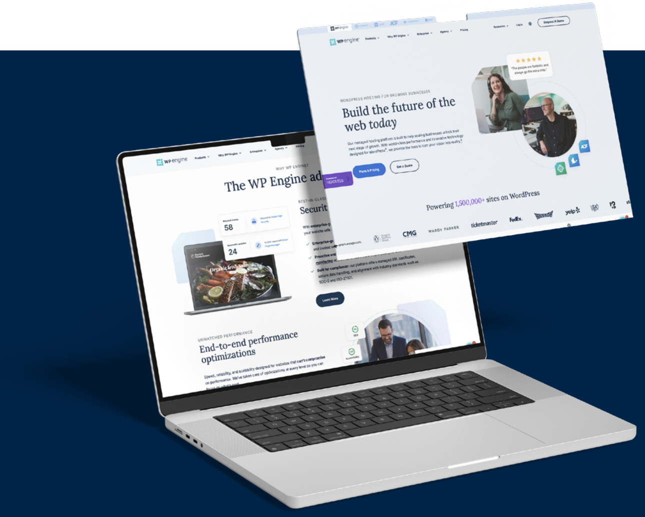
Conclusion:
Prevention is a framework, not a fix

The demands placed upon modern IT and development teams have made reactive, self-managed security infrastructure financially unsustainable and strategically obsolete. The true path to digital resilience is moving away from the costly, never-ending cycle of patching and manual risk mitigation.

The WP Engine security framework provides a proven solution by fully integrating the three pillars essential for enterprise assurance:

- **Defense in Depth:** Protecting the application via coordinated layers of edge, platform, and application-level controls, including Managed WAF and advanced DDoS mitigation.
- **Compliance as a Strategic Asset:** Providing auditable, third-party assurance through non-negotiable standards like SOC 2 Type II and ISO 27001:2022..
- **Cost Efficiency:** Quantifying and eliminating the labor drain associated with manual security tasks, allowing the IT budget to be reallocated toward innovation.

By partnering with a provider that treats security as an automated, continuous, and highly specialized operational service, you free your internal teams to stop focusing on defense and start focusing on digital acceleration.


Build the future of the web today
Powering 1,500,000+ sites on WordPress
The WP Engine ad
End-to-end performance optimizations

How does your CMS investment compare?

Get a personalized TCO assessment with WP Engine and uncover key cost-saving opportunities, security enhancements, and performance optimizations tailored to your business. Future-proof your digital presence.

Start your assessment today

WP engine®

WP Engine empowers companies and agencies of all sizes to build, power, manage, and optimize their WordPress websites and applications with confidence.

Serving 1.5 million customers across 150+ countries, the global technology company provides premium, enterprise-grade solutions, tools, and services, including specialized platforms for WordPress, industry-tailored eCommerce and agency solution suites, and developer-centric tools like Local, Advanced Custom Fields, and more. WP Engine's innovative technology and industry-leading expertise are why 8% of the web visits a WP Engine-powered site daily. Learn more at wpengine.com.