The bridge to possible

Introducing Cisco Hypershield

AI-native security for data centers and cloud. Ever aware, everywhere.

In the era of AI-scale data centers, managing security surpasses human capacity alone. Workloads are commonly distributed across multiple data centers and clouds, leading to fragmented policies that obscure protection coverage and delayed remediation of issues and incidents. At the same time, adversaries are exploiting any weakness ever faster, a trend which will accelerate as AI is more fully adopted. A radically new approach is needed to safeguard modern applications and dynamic compute environments.

Cisco Hypershield revolutionizes security across both on-premises and cloud environments, empowering organizations to protect modern applications more effectively. This groundbreaking product features a new distributed architecture integrating network and workload enforcement points under a unified management system. With Hypershield, businesses gain robust, scalable protection, seamlessly extending their security perimeter from traditional infrastructures to the cloud.

Benefits

- **Protects everywhere.** Implement a hyper-distributed security approach that reaches all areas of your network, tapping into a broad range of previously unreachable workload and network enforcement points.
- **Closes the exploit gap.** Our system blocks application exploits in minutes—not weeks or months. It employs surgical compensating controls that are evaluated and tested against live production traffic for optimal effectiveness.
- **Segmentation that actually works.** Achieve effective segmentation that continuously adapts and learns. Our system earns trust over time and applies highly specific controls, even down to regex filtering, ensuring tailored security.
- **Manages itself, once it earns your trust.** Get unified management across the network and workloads. Deploy software and policy updates with confidence using our dual dataplane approach, enabling safe testing on live traffic without risking your operations.

The bridge to possible

Cisco Hypershield capabilities

Making previously unimaginable outcomes a reality

Hypershield is a brand-new architecture built from the ground up to address today's realities.

Distributed exploit protection

In today's digital landscape, vulnerabilities are exploited faster than ever, sometimes within hours by AI-driven attacks. Traditional patching struggles to keep pace, often taking weeks or months to implement, which can disrupt operations and compel organizations to delay critical updates to avoid downtime.

Hypershield addresses this challenge head-on with its **Distributed Exploit Protection module,** drastically reducing the time to protect against new vulnerabilities. This module automates the entire process—from detection, prioritization, and evaluation of controls to testing and deployment—ensuring applications continue running smoothly without interruption.

Key features:

- **Accelerated response through automated workflows.** Our AI-native engine swiftly detects vulnerabilities and assists in their prioritization, directing efforts where they are most needed. It evaluates different approaches to recommend the most effective solution tailored to your environment, continuously building trust.
- **Precision with surgical compensating controls.** Tailored controls are deployed directly into a distributed mesh of workload and network enforcement points, allowing precise and effective mitigation.
- **Make updates with confidence.** All compensating controls are tested against live production traffic, ensuring their efficacy and optimal placement without risking the application.

Autonomous segmentation

Today's security challenges demand more than traditional tools can offer. With the average time to segment a single application exceeding 40 days—and rules often becoming outdated almost as soon as they are implemented—organizations face significant security gaps. These gaps allow adversaries to move laterally through networks, increasing risk exponentially.

Hypershield's **Autonomous Segmentation module** revolutionizes this process with a dynamic and intelligent segmentation model informed by a deep understanding of application behaviors and other critical inputs. This model continuously adapts based on observations and customer-defined policies, significantly reducing the time and complexity traditionally associated with segmentation.

With Hypershield's Autonomous Segmentation, protect your applications more effectively and preemptively, keeping adversaries at bay.

Key features

- **Continuous adaptation.** The network segments itself, dynamically adjusting to current realities and ensuring always-up-to-date protection.
- **Informed by comprehensive data.** Our segmentation strategy goes beyond network flows, incorporating diverse inputs like process behaviors and application updates. This holistic approach guarantees nuanced and highly effective segmentation.
- **Precision controls starting with macro-guardrails.** Beginning with broad protection parameters, the system fine-tunes its controls down to specific regex filters, ensuring precise and effective risk mitigation.

Self-qualifying updates

Traditional software upgrades to infrastructure or policy changes pose a high risk of disrupting business operations. These updates require significant time and resources to test, typically limiting them to a few times a year. This slow update cycle leaves organizations vulnerable to emerging threats with outdated defenses. Hypershield introduces a groundbreaking solution to this challenge with its **dual dataplane** technology. This innovative approach allows live production traffic to operate under current rules while simultaneously sending a copy of this traffic to a shadow dataplane. This shadow plane tests new software upgrades or policy changes without impacting the actual production environment.

With Hypershield's dual dataplane, IT and security teams can now deploy updates more frequently and with greater confidence, ensuring robust defenses against the latest threats without disrupting business processes.

Key features

- **Non-disruptive testing.** The shadow dataplane evaluates new policies and software upgrades by mirroring live traffic, ensuring that production operations remain unaffected.
- **Continuous improvement.** By testing updates in real-time, Hypershield significantly reduces the time and resources typically required for traditional updates.
- **Informed decision-making.** After testing, Hypershield generates detailed reports and provides AI-backed recommendations on whether the new updates should be deployed, enhancing confidence and operational efficiency. Additionally, operators can gain further trust through an AI assistant that helps explain the results and recommendations.

The bridge to possible

Cisco Hypershield architecture

It's not the next generation of anything. It's the first generation of something new.

By making hyperscaler technology accessible to enterprises of all sizes, Hypershield enables superior efficacy, enhanced experiences, and better economics in securing application infrastructure and systems at AI scale. **More a fabric than a fence,** Hypershield places security enforcement exactly where it's needed, seamlessly and at cloud speed, in highly distributed environments.

Here are the key components around which the solution is architected:

Tesseract Security Agent (TSA): This safe, high-performance agent operates on the workload, interfacing with processes and the operating system kernel through the extended Berkeley Packet Filter (eBPF[1]). Optimized for easy deployment in Kubernetes environments, TSA is also fully functional in non-Kubernetes settings. It offers complete visibility into workload actions, monitoring network connections, file and system calls, and kernel functions, and it alerts on anomalous activities.

Virtual machine- and container-based network enforcement points. Hypershield includes network enforcement points that operate within a virtual machine or container.

These are strategically placed close to the workload to protect specific assets more effectively, moving away from traditional centralized enforcement approaches.

Unified cloud management. Regardless of the enforcement point's form factor or location, all policies are centrally organized and managed via Hypershield's management console. New or updated policies are "compiled" and intelligently distributed to the appropriate enforcement points. This system ensures that security administrators maintain a comprehensive overview of all deployed policies, which can dynamically adapt to workloads moving from on-premises environments to public clouds or between servers.

AI-native. Designed from the ground up with AI integration, Hypershield delivers high efficacy, rapid response, and continuous protection. The system can autonomously write, test, deploy, and manage its own rules, taking advantage of the dual dataplane and extensive visibility across the network and workloads. An AI assistant is also available to explain the analysis, observed behaviors, recommendations, and more, thus earning trust through appropriate levels of autonomy and control.

To learn more, please visit: cisco.com/go/hypershield

[1] eBPF is a software framework on modern operating systems that enables programs in user space (in this case, the Tesseract agent) to safely carry out enforcement and monitoring actions via the kernel.

1337504469 04/24