haden grey
Your Cybersecurity Services Experts

CLOUD WORKLOAD PROTECTION (CWP) SERVICES

PROTECT EVERY WORKLOAD. SECURE EVERY ENVIRONMENT. RUN WITH CONFIDENCE.

As organizations accelerate cloud adoption, workloads are increasingly distributed across virtual machines, containers, Kubernetes, and serverless platforms. These dynamic environments introduce new attack surfaces and risks that traditional security tools cannot adequately address.

Haden Grey's Cloud Workload Protection (CWP) services help organizations secure cloud workloads across their entire lifecycle, from build to runtime. We protect workloads from vulnerabilities, malware, misconfigurations, and unauthorized changes while enabling DevOps speed and scalability.

Our approach combines deep cloud security expertise, automation-first design, and practical implementation strategies to deliver strong protection without slowing innovation.

SERVICE OVERVIEW

Haden Grey delivers end-to-end Cloud Workload Protection services spanning advisory, design, implementation, and managed services. We help organizations:

- Protect workloads across multi-cloud and hybrid environments
- Reduce exposure to vulnerabilities and exploits
- Detect and stop runtime threats
- Enforce workload integrity and configuration security
- Support DevSecOps and secure CI/CD pipelines
- Maintain visibility across dynamic environments

Our services are vendor-agnostic and aligned to modern cloud-native architectures.

OUR DELIVERY METHODOLOGY

Assess

Evaluate workload exposure, configurations, and risk.

Design

Develop scalable, cloud-native protection architectures.

Implement

Deploy controls with minimal disruption to operations.

Operate & Optimize

Continuously improve workload protection.

CORE CAPABILITIES

1. Workload Visibility & Inventory

Know What Your Running

We provide comprehensive visibility into workloads across environments.

Capabilities Include:

- Automated workload discovery
- Asset inventory and classification
- Dependency mapping
- Workload telemetry collection
- Risk-based workload prioritization

Benefits:

- Improved visibility
- Reduced shadow workloads
- Better risk awareness

2. Vulnerability Management

Identitify and Reduce Exposure

We help detect and prioritize vulnerabilities across workloads.

Capabilities Include:

- VM and container vulnerability scanning
- Image scanning in CI/CD pipelines
- CVE prioritization
- Patch and remediation guidance
- Continuous vulnerability monitoring

Benefits:

- Reduced attack surface
- Faster remediation cycles
- Improved security posture

3. Runtime Protection

Stop Threats in Real Time

We implement controls that detect and prevent active threats.

Capabilities Include:

- Behavioral monitoring
- File integrity monitoring
- Process anomaly detection
- Runtime threat prevention
- Host and container protection

Benefits:

- Reduced breach impact
- Early threat detection
- Stronger runtime security

4. Container & Kubernetes Security

Secure Cloud-Native Applications

We protect containerized workloads and orchestration platforms.

Capabilities Include:

- Container image scanning
- Kubernetes configuration reviews
- Admission controller policies
- Secrets exposure detection
- Cluster hardening guidance

Benefits:

- Safer container deployments
- Reduced misconfiguration risk
- DevSecOps alignment

5. Serverless & Modern Workload Protection

Security for Ephemeral Compute

We secure serverless and short-lived workloads.

Capabilities Include:

- Function-level monitoring
- Secure configuration guidance
- Event-driven threat detection
- API and dependency protection

Benefits:

- Reduced blind spots
- Secure serverless adoption
- Better workload governance

6. Integrity Monitoring & Change Control

Detect Unauthorized Changes

We ensure workloads remain in a trusted state.

Capabilities Include:

- File and configuration integrity monitoring
- Baseline enforcement
- Drift detection
- Alerting and response workflows

Benefits:

- Reduced insider and attacker impact
- Compliance support
- Improved accountability

TECHNOLOGY ALIGNMENT

Haden Grey works across leading cloud workload protection and CNAPP ecosystems.

Common technology ecosystems include:

- Palo Alto Networks Prisma Cloud
- Wiz
- Microsoft Defender for Cloud
- CrowdStrike Falcon Cloud Security
- Trend Micro Cloud One
- SentinelOne Cloud Security

CWP ADVISORY SERVICES

- Cloud workload risk assessments
- Architecture and design reviews
- DevSecOps security strategy
- Workload security maturity assessments
- Tool evaluation and rationalization
- Multi-cloud security strategy

IMPLEMENTATION SERVICES

- CWP platform deployment and configuration
- CI/CD pipeline integration
- Policy and rule creation
- Kubernetes and container security setup
- Monitoring and alert integration
- Automation enablement

MANAGED CWP SERVICES

- Continuous monitoring and tuning
- Vulnerability management operations
- Policy optimization
- Threat detection support
- Reporting and metrics
- SLA-based support models
- Continuous improvement programs

BUSINESS OUTCOMES

Organizations partnering with Haden Grey achieve:

- Reduced workload-related risk
- Faster vulnerability remediation
- Improved runtime security
- Stronger DevSecOps alignment
- Better compliance posture
- Secure cloud-native innovation
- Greater operational visibility

WHY HADEN GREY

Clients choose Haden Grey for:

- Deep cloud and data security expertise
- Vendor-agnostic advisory
- Proven enterprise delivery
- DevSecOps-aligned approach
- White-glove client service
- Practical, outcome-driven solutions

HadenGrey.com Solutions@HadenGrey.com (303)529-0467