haden grey
Your Cybersecurity Services Experts

NETWORK SEGMANTATION & MICRO-SEGMENTATION SERVICES

CONTAIN THREATS. LIMIT EXPOSURE. STRENGTHEN NETWORK SECURITY.

Flat networks increase risk. When attackers gain access, they can often move laterally with little resistance, escalating privileges and reaching critical systems. Traditional perimeter defenses alone are no longer enough.

Haden Grey's Network Segmentation & Microsegmentation services help organizations reduce attack surfaces and contain threats by enforcing granular, policy-driven network controls. We design and implement segmentation strategies that limit lateral movement, protect critical assets, and align with Zero Trust principles.

Our approach combines deep network and cloud security expertise with practical, scalable architectures that support both security and operational efficiency.

SERVICE OVERVIEW

Haden Grey delivers end-to-end segmentation services spanning advisory, architecture, implementation, and managed services. We help organizations:

- Reduce lateral movement risk
- Protect high-value assets and sensitive data
- Enforce least-privilege network access
- Improve visibility into traffic flows
- Support Zero Trust and compliance initiatives
- Simplify network security management

Our services are vendor-agnostic and tailored to your environment, risk profile, and operational needs.

OUR DELIVERY METHODOLOGY

Assess

Evaluate current network design, traffic flows, and risk exposure.

Design

Develop scalable segmentation architectures and policy models.

Implement

Deploy segmentation with minimal operational disruption.

Operate & Optimize

Continuously improve segmentation effectiveness.

CORE CAPABILITIES

1. Segmentation Strategy & Architecture

Design Security Into the Network

We develop segmentation strategies aligned to business and security goals.

Capabilities Include:

- Segmentation strategy development
- Zone and trust boundary design
- Critical asset identification
- Data flow mapping
- Zero Trust-aligned architecture
- Multi-site and hybrid design planning

Benefits:

- Clear segmentation roadmap
- Reduced attack surface
- Scalable architecture

2. Network Segmentation (Macro-Segmentation)

Establishing Strong Security Zones

We design and implement network-level segmentation.

Capabilities Include:

- VLAN and subnet segmentation
- Firewall-based segmentation
- DMZ design
- Environment separation (prod/dev/test)
- Regulatory segmentation models (e.g., PCI zones)

Benefits:

- Improved isolation
- Reduced blast radius
- Compliance support

3. Micro-Segmentation

Granular, Workload-Level Protection

We implement fine-grained segmentation controls at the workload or application level.

Capabilities Include:

- Identity-based segmentation
- Host-based segmentation
- Application-level policy enforcement
- Software-defined segmentation
- East-west traffic control

Benefits:

- Strong lateral movement prevention
- Precise access control
- Adaptive security

4. Application Dependency Mapping

Understand Traffic Before Enforcing Policy

We map application flows to avoid disruption.

Capabilities Include:

- Traffic flow analysis
- Dependency visualization
- Baseline policy modeling
- Simulation and testing
- Policy validation

Benefits:

- Reduced deployment risk
- Minimal business disruption
- Better policy accuracy

5. Policy Design & Enforcement

Least Privilege by Default

We design policies that enforce least-privilege communication.

Capabilities Include:

- Allowlist policy models
- Role-based communication rules
- Dynamic policy enforcement
- Policy lifecycle management
- Change management integration

Benefits:

- Reduced rule sprawl
- Stronger control
- Easier governance

6. Continuous Monitoring & Optimization

Keep Segmentation Effective

We ensure segmentation remains aligned to change.

Capabilities Include:

- Policy review and tuning
- Drift detection
- Traffic monitoring
- Reporting and analytics
- Compliance validation

Benefits:

- Sustained protection
- Improved visibility
- Ongoing alignment

TECHNOLOGY ALIGNMENT

Haden Grey maintains expertise across leading segmentation and microsegmentation platforms.

Common segmentation platforms include:

- Illumio
- Akamai Guardicore Segmentation
- VMware NSX
- Cisco Secure Workload (Tetration)
- Palo Alto Networks (VM-Series / segmentation capabilities)
- Check Point segmentation solutions
- Fortinet FortiGate segmentation
- Zscaler workload segmentation capabilities

SEGMENTATION ADVISORY SERVICES

- Segmentation maturity assessments
- Architecture and design reviews
- Zero Trust network alignment
- Regulatory segmentation planning
- Tool evaluation and rationalization
- M&A network integration strategy

IMPLEMENTATION SERVICES

- Segmentation platform deployment
- Policy creation and rollout
- Firewall and host control integration
- Phased deployment strategies
- Validation and testing
- Automation enablement

MANAGED SEGMENTATION SERVICES

- Policy management and updates
- Continuous monitoring
- Incident support
- Reporting and metrics
- SLA-based support models
- Continuous improvement programs

BUSINESS OUTCOMES

Organizations partnering with Haden Grey achieve:

- Reduced lateral movement risk
- Smaller breach impact radius
- Stronger Zero Trust posture
- Improved compliance alignment
- Better visibility into network flows
- Simplified security operations
- Scalable network security architecture

WHY HADEN GREY

Clients choose Haden Grey for:

- Deep network and cloud security expertise
- Vendor-agnostic advisory
- Proven Zero Trust and segmentation delivery
- Security-first architecture approach
- White-glove client service
- Practical, outcome-driven solutions

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