hadengrey
Your Cybersecurity Services Experts

NEXT-GENERATION ANTIVIRUS (NGAV) & MALWARE PREVENTION SERVICES

STOP MODERN MALWARE. STRENGTHEN ENDPOINT DEFENSE. STAY AHEAD OF THREATS.

Traditional signature-based antivirus tools can no longer keep pace with modern threats. Today's attackers use fileless malware, living-off-the-land techniques, ransomware, and zero-day exploits to bypass legacy defenses.

Haden Grey's Next-Generation Antivirus (NGAV) & Malware Prevention services help organizations proactively prevent, detect, and block advanced threats before they impact the business. We design and optimize modern endpoint protection strategies that leverage behavioral analysis, AI-driven detection, and threat intelligence.

Our approach combines deep threat defense expertise, practical architecture strategies, and white-glove advisory to deliver strong protection with minimal user disruption.

SERVICE OVERVIEW

Haden Grey delivers end-to-end NGAV and malware prevention services spanning advisory, architecture, deployment guidance, and optimization. We help organizations:

- Prevent malware and ransomware infections
- Replace or modernize legacy antivirus tools
- Reduce endpoint attack surfaces
- Improve threat detection accuracy
- Strengthen endpoint resilience
- Align malware defense to Zero Trust strategies

Our services are vendor-agnostic and tailored to your environment, workforce model, and risk tolerance.

OUR DELIVERY METHODOLOGY

Assess

Evaluate current malware defenses, gaps, and risks.

Design

Develop scalable, layered malware prevention architectures.

Implement
(Guide & Validate)

Support deployment with security-by-design principles.

Optimize

Continuously refine detection and prevention.

CORE CAPABILITIES

1. NGAV Strategy & Roadmap Development

Modern Protection for Modern Threats

We define a strategic approach to next-gen malware defense.

Capabilities Include:

- NGAV roadmap development
- Legacy AV replacement planning
- Risk-based protection strategies
- Control rationalization
- Investment prioritization

Benefits:

- Clear modernization path
- Reduced risk exposure
- Stronger protection posture

2. Advanced Malware Prevention Architecture

Security by Design

We design scalable NGAV architectures aligned to business needs.

Capabilities Include:

- AI/ML-based detection strategy
- Behavioral analysis integration
- Cloud-delivered protection design
- Policy architecture design
- Multi-layered defense models

Benefits:

- Stronger detection coverage
- Reduced false positives
- Scalable protection

3. Ransomware Prevention Strategy

Stop Ransomware Before it Executes

We help organizations build proactive ransomware defenses.

Capabilities Include:

- Anti-ransomware policy design
- Behavior-based blocking
- Exploit prevention strategies
- Rollback and recovery alignment
- Attack surface reduction guidance

Benefits:

- Lower ransomware risk
- Faster containment
- Reduced business impact

4. Fileless & Script-Based Attack Protection

Defend Against Evasive Techniques

We protect against advanced attack methods.

Capabilities Include:

- Memory-based attack detection
- Script control strategies
- Living-off-the-land detection
- PowerShell and macro protections
- Exploit guard alignment

Benefits:

- Reduced evasion success
- Stronger prevention
- Better detection coverage

5. Threat Intelligence & Analytics Integration

Stay Ahead of Threat Actors

We integrate intelligence-driven defenses.

Capabilities Include:

- Global threat intelligence integration
- IOC and behavioral indicator tuning
- Threat trend analysis
- Proactive defense alignment

Benefits:

- Faster detection
- Adaptive protection
- Improved threat awareness

6. Policy Optimization & Tuning

Security Without Disruption

We ensure protection is effective and usable.

Capabilities Include:

- Policy tuning and baselining
- False-positive reduction
- User impact analysis
- Performance optimization

Benefits:

- Better user experience
- Higher operational efficiency
- Stronger adoption

TECHNOLOGY ALIGNMENT

Haden Grey works across leading NGAV and endpoint protection platforms to design interoperable solutions.

Common NGAV platforms include:

- Microsoft Defender Antivirus / Defender for Endpoint
- CrowdStrike Falcon Prevent
- SentinelOne Singularity
- VMware Carbon Black
- Sophos Intercept X
- Trellix (McAfee) Endpoint Security
- Trend Micro Apex One
- Palo Alto Networks Cortex XDR Prevent
- Cisco Secure Endpoint

NGAV ADVISORY SERVICES

- Malware defense maturity assessment
- Architecture and design reviews
- Tool evaluation and rationalization
- Ransomware readiness assessments
- Zero Trust endpoint alignment
- Mergers and acquisitions endpoint security integration planning

IMPLEMENTATION SERVICES

- NGAV platform deployment guidance
- Policy configuration design
- Integration with EDR/XDR and SIEM
- Secure baseline development
- Automation enablement

ONGOING OPTIMIZATION SUPPORT

- Policy refinement
- Protection tuning
- Threat trend reviews
- Control optimization
- Roadmap updates

BUSINESS OUTCOMES

Organizations partnering with Haden Grey achieve:

- Reduced malware and ransomware risk
- Stronger endpoint resilience
- Lower infection rates
- Improved detection accuracy
- Reduced operational disruptions
- Scalable malware defense programs
- Greater confidence in cyber readiness

WHY HADEN GREY

Clients choose Haden Grey for:

- Deep endpoint and threat defense expertise
- Vendor-agnostic advisory
- Proven enterprise security architecture experience
- Security-first, business-aligned approach
- White-glove client service
- Practical, outcome-driven strategies

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