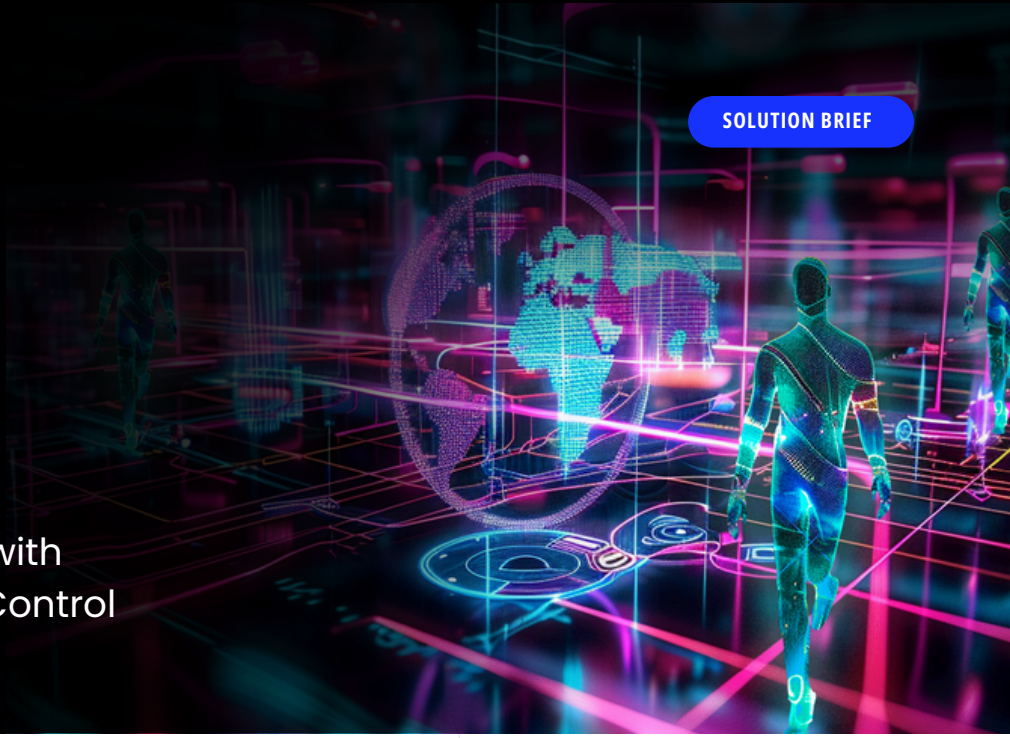
hackerone

SOLUTION BRIEF



HackerOne Gateway

Empowering Organizations with Advanced Security Testing Control

Zero-Trust Network Access, Management, and Monitoring of All Your Assets

From private financial records and sensitive patient health data to top-secret military systems, many security testing use cases require transparency and control that traditional security measures lack, leaving organizations vulnerable to hidden risks. HackerOne Gateway addresses these challenges by integrating with your existing infrastructure and delivering comprehensive security testing capabilities for your most sensitive assets through the HackerOne Platform.

Powered by Cloudflare's Zero Trust Network Access (ZTNA) technology, Gateway provides a performant, scalable, and secure zero-trust solution. It allows security researchers access to your external and internal assets while you remain in control, with features including self-service start/stop controls, traffic log access, and comprehensive coverage analytics. This ensures transparency, audibility, and regulatory compliance, making sure your security is always in the right hands.

Use Cases

Regulatory Compliance

Maintain compliance with laws like GDPR, HIPAA, or SOX through controlled access and comprehensive traffic logging for audit trails.

Secure Development and Testing Environments

Gain secure access to development environments that mimic production settings, allowing researchers to test applications safely without risking exposure to sensitive or critical data.

Internal Application Testing

Facilitate thorough testing of applications not accessible over the internet, pre-production assets, and internal network environments under zero-trust principles.

> HackerOne Gateway, backed by Cloudflare's services, helps level the playing field for defenders. With greater control and transparency around researchers and the access they have to customer environments, HackerOne can discover vulnerabilities before malicious threat actors faster than ever before.

Chris Draper
Product Manager at Cloudflare

Key Capabilities

Real-time Threat Insight

Immediate visibility into security researchers' attack paths for near-instant tracking of their progress.

Precision Researcher Monitoring

Consistent egress IPs reduce security alerts by distinguishing between HackerOne traffic and genuine threats.

Geo-compliant Security

Selectively admit security researchers solely from your chosen countries to ensure regulatory compliance.

Asset Expansion

Incorporate previously restricted firewalled assets without extensive setup.

One-click Control

User-friendly control panel for halting testing at any time.

Detailed Activity Logs

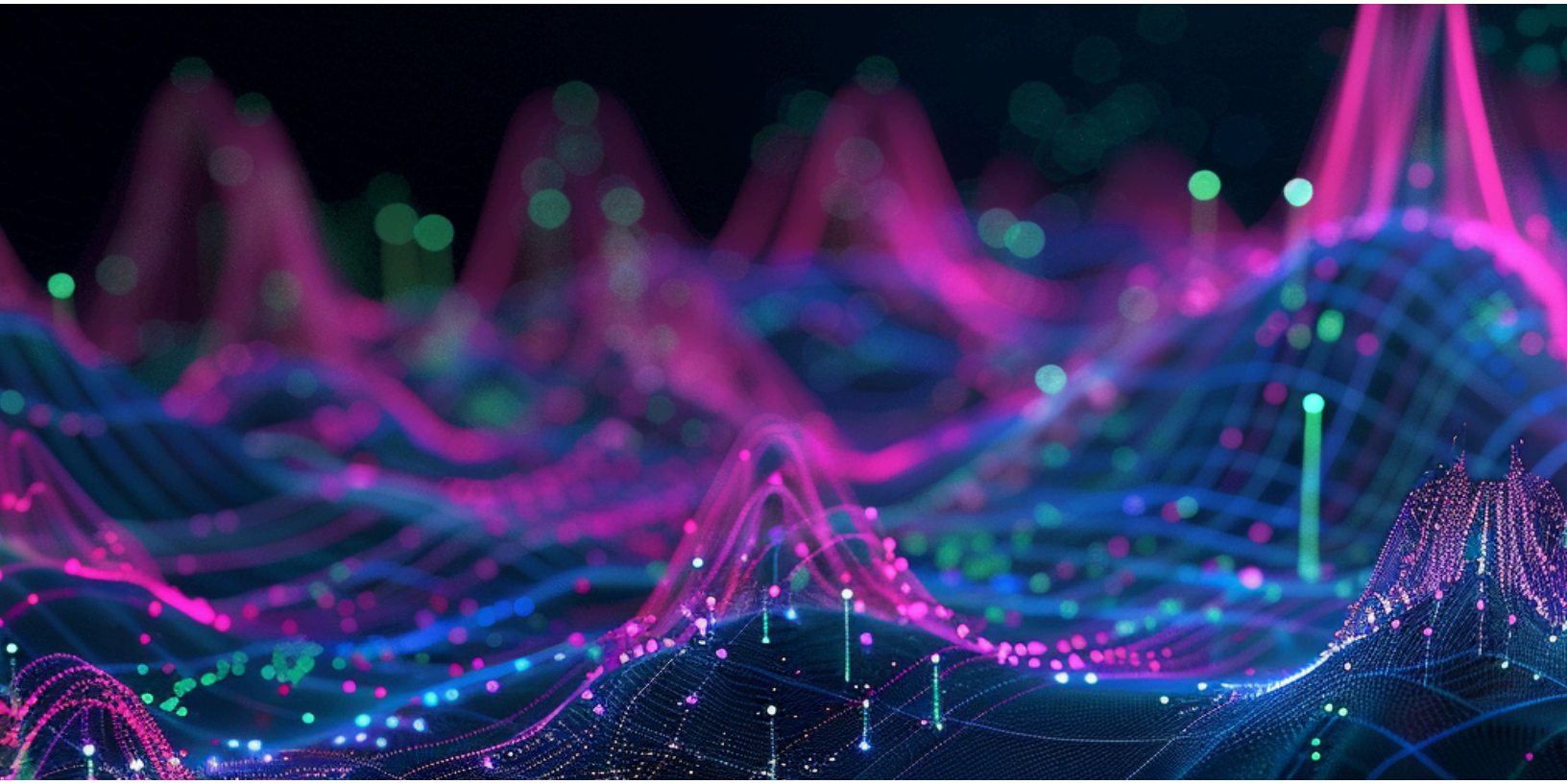
Self-serve detailed activity logs to specify assets hit on a per-researcher basis.

Compliance Details

Maintain compliance and provide evidence of testing through access to traffic logs.

Analytics

View, analyze, and download data to inform strategy adjustments and prove program ROI.



Enhanced Internal Network Testing and Pentesting with Gateway

Gateway Internal Network Testing (INT) provides secure and efficient internal network testing by routing all security program traffic through Cloudflare's superior ZTNA. This offers the traceability required in regulated industries, enabling external security researchers to conduct thorough testing of pre-production or internal assets. By simplifying restricted access to internal networks for pentesting and security assessments, Gateway INT ensures easy access to virtual desktops and VDI/VM environments, leading to higher-quality pentest results.

Key supporting technologies include:

Cloudflare Tunnel (Cloudflared)

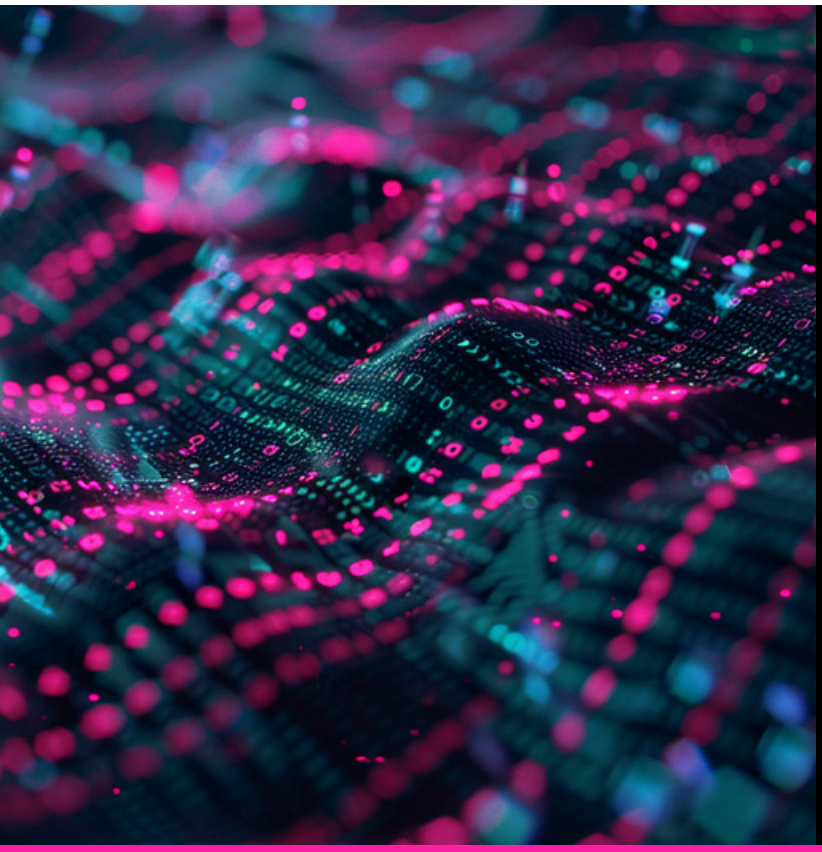
provides secure access to internal applications without internet exposure, routing all security testing traffic through a secure ZTNA infrastructure.

Cloudflare's WARP technology

establishes a Zero-Trust tunnel connecting security researchers to target assets without needing multiple IP addresses, simplifying access control and enhancing productivity.

IPsec

adds an extra layer of encryption and security to traffic between internal networks and security researchers, safeguarding sensitive data and ensuring continuous proof of testing.



> The sensitive nature of our assets and researcher participation requirements makes HackerOne's vetting capabilities a critical component of our program's success.

Reina Staley
Former Chief of Staff, Digital Defense Service

Contact our experts to discover how you can maximize your internal and external security testing results with HackerOne Gateway's advanced control and transparency over your programs.