DATASHEET

Infoblox Exposure Management:
Digital Risk Protection Services (DRPS)

Preemptively stop brand abuse, fraud and data exposure before they cause harm

WHY DRPS MATTERS

Modern cyberattacks increasingly begin outside the enterprise, where attackers exploit trusted brands, identities and exposed data to defraud users and steal credentials.

Common threats include:

- Phishing and credential-harvesting sites
- Brand impersonation across social platforms, ads and messaging
- Rogue mobile apps and marketplace listings
- Executive and VIP impersonation for wire fraud
- Credential exposure and sensitive data leaks across deep and dark web sources

AI-driven automation has dramatically increased the speed and scale of these campaigns, overwhelming manual investigation and response models. Effective prevention now depends on continuous discovery, rapid validation and automated disruption.

DRPS AT A GLANCE

DRPS helps organizations reduce harm from phishing, brand impersonation, fraud and credential exposure.

These attacks exploit trusted brands, identities and exposed data before traditional security controls can respond.

By combining AI-driven external threat discovery, evidence-backed validation and large-scale takedown orchestration, DRPS enables organizations to disrupt malicious infrastructure earlier in the attack lifecycle, reducing fraud, customer harm and reputational damage.

The result: measurable risk reduction, not just alerts.

KEY BENEFITS

Identify Real External Threats Quickly
Analyzes external data to detect and validate brand abuse, fraud and data exposure. AI filters false positives so teams focus on confirmed, high-risk threats.

Disrupt Attacker Infrastructure Earlier in the Threat Lifecycle
Automated takedown orchestration generates evidence, selects the best enforcement path and removes malicious domains, content, apps and accounts at scale.

Sustain Protection with Stay-Down Monitoring
Continuous monitoring detects reappearance, infrastructure reuse and campaign evolution, preventing attackers from resurfacing with recycled assets or modified techniques.

Reduce Operational Effort Through Intelligent Automation
Automates investigation, validation and escalation, enabling up to 86% of takedowns to execute end-to-end automatically so teams can scale protection without adding headcount.

Deliver Measurable, Defensible Outcomes
Clear metrics and audit-ready evidence demonstrate real reductions in fraud, customer harm and brand risk.

Industry-Leading Performance on a Global Scale	Core Use Cases
• **<4 minute** median time to first enforcement notification • **~9 hour** median time to takedown after confirmation • **98.9%** takedown success rate • **86%** of takedowns fully automated end to end • **15-day stay-down guarantee** prevents reappearance • **40+ million URLs** analyzed daily • **1,000+ malicious assets** removed every day • **760M+ exposed cards** tracked by threat intel • **20B+ unique credentials** tracked by threat intel • **32B+ records** available for threat hunting	• Disrupt phishing and fraud campaigns across domains, ads, apps and marketplaces • Protect against brand, executive and social impersonation • Detect deep and dark web activity early • Monitor credential exposure and data leaks • Prevent account takeover and payment diversion by removing attacks early

HOW DRPS WORKS

DRPS connects external discovery, threat validation and automated disruption to reduce the exposure window:

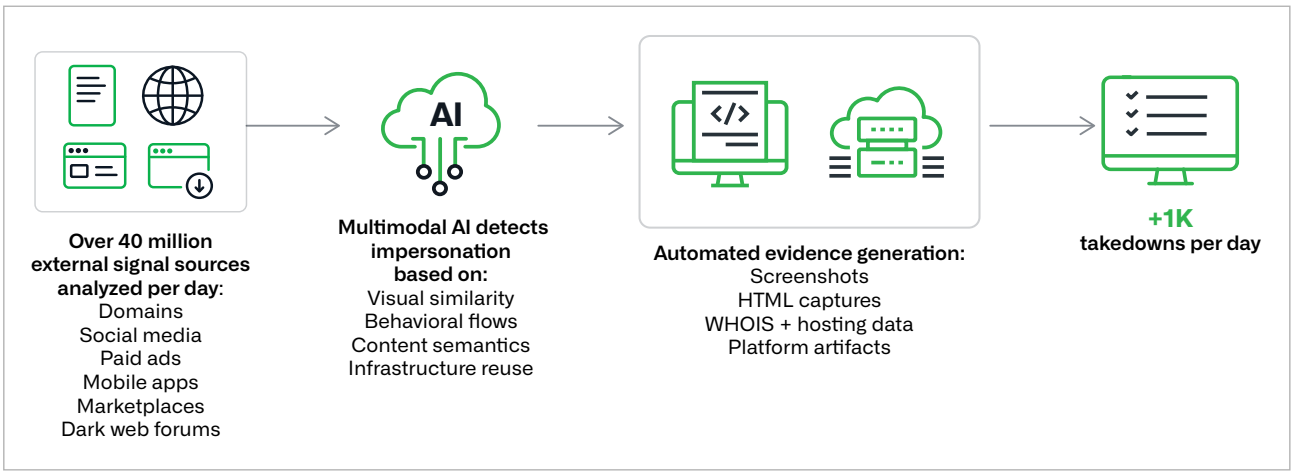

Figure 1. How DRPS leverages AI to reduce the exposure window

KEY CAPABILITIES OF THE INFOBLOX APPROACH TO EXTERNAL THREATS AND DIGITAL RISKS



External Threat Discovery

Continuously identifies phishing sites, impersonation campaigns, fraudulent ads, rogue apps and leaked credentials across web, social, ads, apps and underground sources, often before attacks are weaponized, including visual brand impersonation beyond keywords.



Threat Validation and Prioritization

Enriches findings with content analysis and DNS infrastructure context, correlates external abuse indicators with DNS telemetry to map related attacker infrastructure and prioritizes threats based on real-world risk and business impact.



Evidence Collection and Takedown Orchestration

Validates abuse, gathers defensible evidence and coordinates takedowns across registrars, hosting providers, social platforms, ad networks, app stores and marketplaces with minimal manual effort.



Continuous Monitoring and Stay-Down Enforcement

Post-takedown monitoring detects reappearance or infrastructure reuse, ensuring attacks remain neutralized over time.



Cross-Team Visibility and Reporting

Shared dashboards and outcome reporting support security, legal, fraud and brand teams with clear status tracking and leadership-ready metrics.

BETTER TOGETHER: DRPS AND PROTECTIVE DNS

When DRPS is used alongside Protective DNS, part of Infoblox Threat Defense™, organizations gain preemptive containment during active investigations and takedowns by preventing access to confirmed malicious destinations.

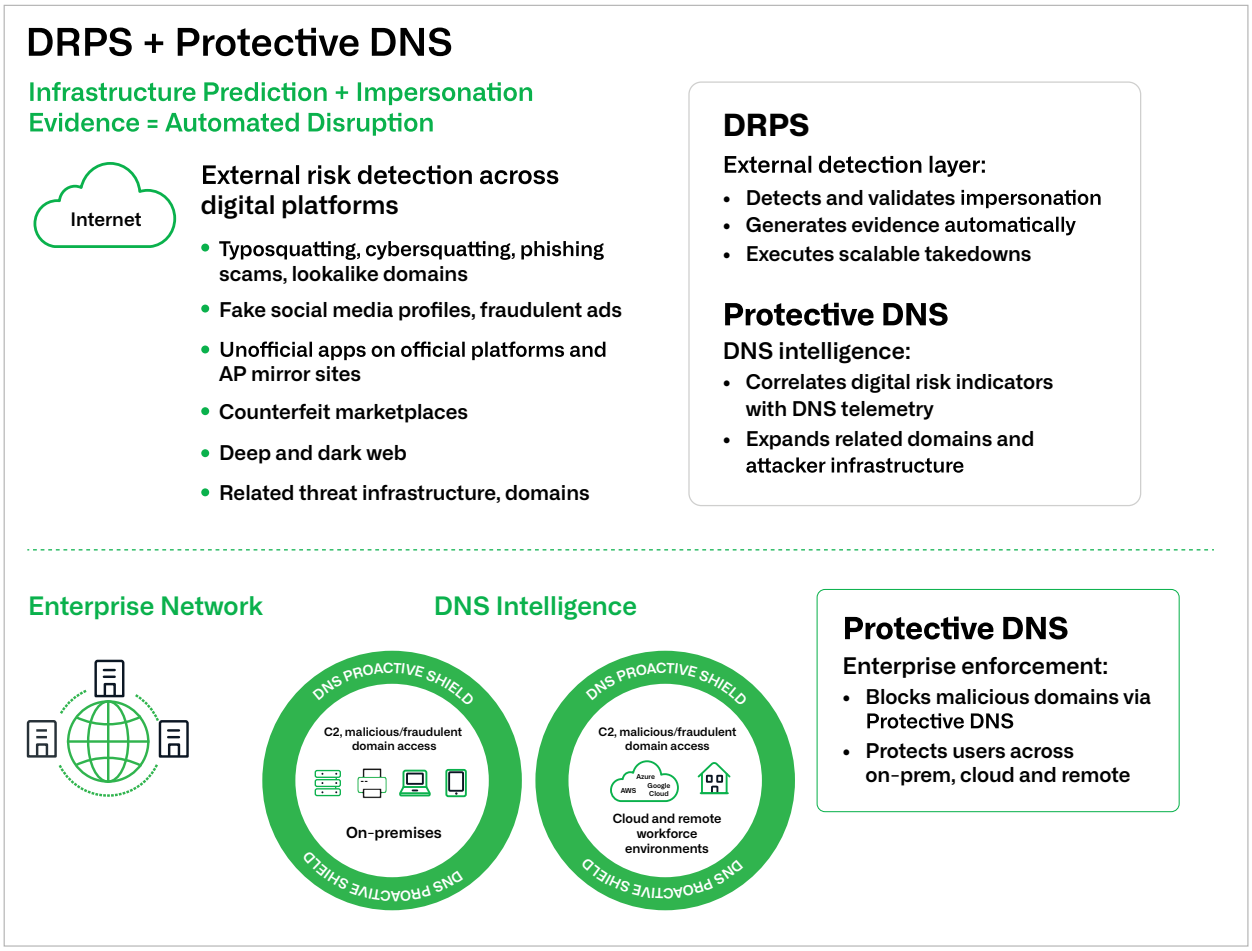

Figure 2. How DRPS works with Protective DNS to deliver preemptive protection

Together these capabilities help organizations:

- Reduce exposure during the most critical early-stage window of an attack
- Protect users and brand trust while attacks are actively dismantled
- Strengthen defense-in-depth without slowing takedown or response efforts

Ready to reduce external threats, brand abuse and fraud? Talk to an Infoblox expert to see how DRPS, part of Infoblox Exposure Management, can help protect your brand, customers and revenue.

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2026 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20260501v1