

Brand and Digital Risk Protection

Preemptive Protection against Brand Impersonation, Fraud and External Threats

IMPACT SUMMARY



Prevent Brand Impersonation and Fraud

Stop phishing, impersonation, fraudulent ads, rogue apps and lookalike domains before they impact customers or employees.



Disrupt Attacker Infrastructure at Scale

Automate validation and removal of malicious assets across web, social, ads, apps and online marketplaces, delivering fast takedowns and sustained protection against recurring attacks.



Protect Users Immediately

Block access to confirmed threats within minutes using network-level enforcement and browser warnings, protecting employees and customers during investigations before infrastructure is removed.



Reduce Business Risk, Not Just Alerts

Deliver measurable reductions in fraud, customer harm and operational effort by prioritizing validated threats, automated disruption and outcomes that demonstrate real-world risk reduction.

Sub-4-minute

median time to notification after detection

9-hour

median time to confirmed takedown across platforms

15-day stay-down

guarantee to prevent recurrence

86%

fully automated takedowns with no human intervention

INTRODUCTION

Brand impersonation has evolved far beyond spoofed domains. Modern attackers exploit trusted brands across websites, social platforms, paid ads, app stores and messaging channels, often launching campaigns and reaching victims within hours. These attacks enable phishing, account takeovers, payment fraud, credential theft and executive impersonation before security teams are even aware they exist.

CHALLENGE

Brand impersonation, phishing and fraud attacks now originate entirely outside the enterprise and move at machine speed. Attackers abuse trusted brands across domains, websites, social platforms, paid ads, app stores and messaging channels, often reaching customers within hours of launch (Figure 1). Fragmented visibility, manual validation and slow takedown workflows force organizations into reactive mode after customer harm, revenue loss and reputational damage have already occurred.

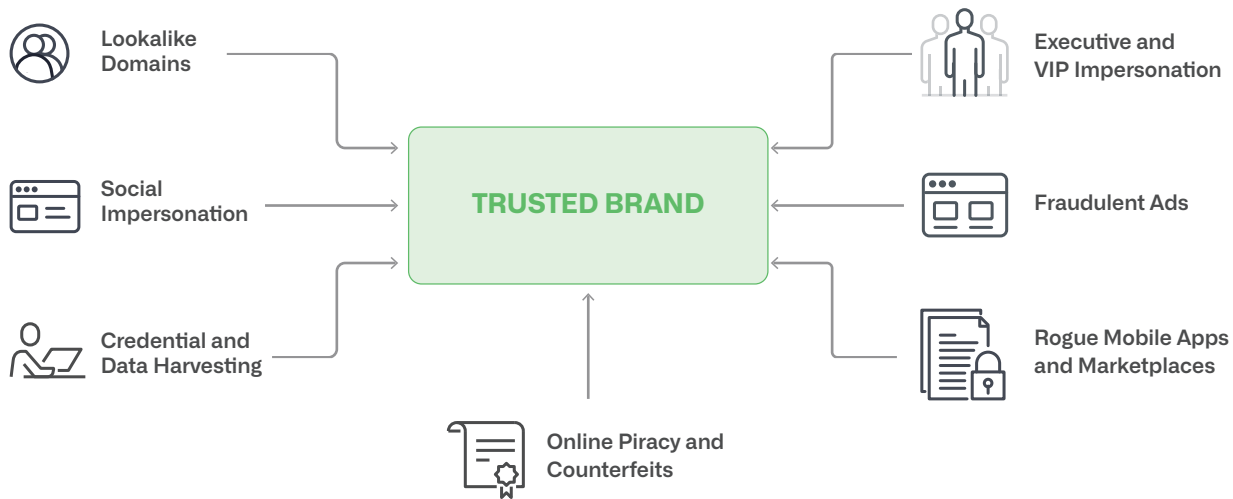


Figure 1. Brand abuse can span multiple platforms

Brand Abuse Now Operates at Machine Speed

Attackers increasingly use AI to generate convincing impersonation assets, localize lures, rotate infrastructure and relaunch campaigns in minutes. Brand abuse now scales faster than human-driven detection and response models can keep up. Many campaigns move from setup to customer impact within hours, leaving little room for slow investigation or manual escalation.

Fragmented Visibility across Digital Channels

Organizations operate across dozens of domains, cloud services, advertising platforms, social networks and app marketplaces. Traditional brand monitoring tools provide only partial coverage and often lack the context needed to distinguish real threats from noise. Without unified visibility across all external channels where brands appear, impersonation and fraud can persist unnoticed until customers report harm.

Manual Validation and Slow Takedowns

Most brand protection workflows still rely on analysts to manually validate abuse, gather evidence and coordinate takedowns with third-party providers. That process introduces delays at exactly the moment speed matters most. While investigations are underway, malicious sites, ads and profiles remain live, actively stealing credentials, diverting payments and damaging trust.

Recurring Attacks and Limited Proof of Impact

Even after takedowns occur, attackers frequently relaunch using new domains, ads or accounts. Without continuous monitoring and stay-down assurance, organizations are forced into repeated response cycles. At the same time, security and brand teams struggle to demonstrate measurable impact: what was prevented, what was removed and whether risk was meaningfully reduced.

SOLUTION

Infoblox addresses modern brand abuse by intervening earlier in the attack lifecycle and operating at the speed today's attackers demand. Rather than relying on fragmented monitoring or manual escalation, the solution combines continuous external discovery, high-confidence validation, immediate containment and automated disruption into a single, outcome-driven workflow (Figure 2). This enables organizations to prevent customer harm, revenue loss and reputational damage before attacks can scale.

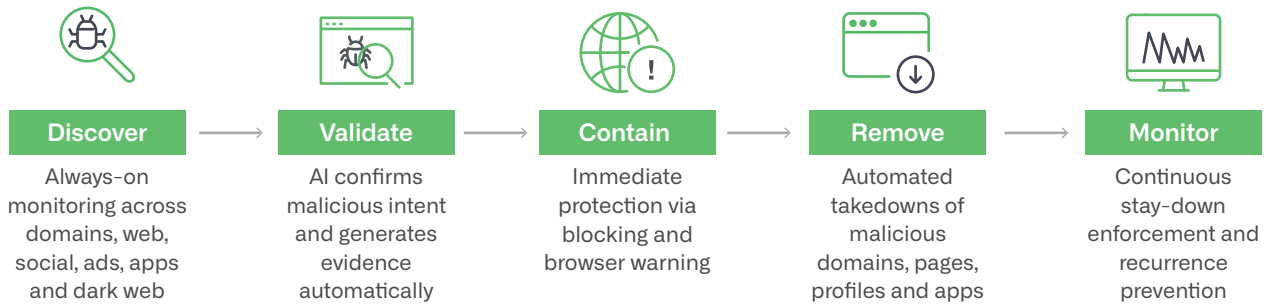


Figure 2. Brand attacks must be stopped at every phase of the attack lifecycle

Unified External Visibility and Early Intervention

Before

Brand impersonation monitoring is fragmented across domains, social platforms, advertising channels and app stores. Discovery often depends on customer complaints, periodic searches or isolated alerts that lack context. As a result, teams struggle to determine what represents real risk, delaying action while attacks continue to operate.

After

Infoblox provides continuous visibility across the external channels attackers use to impersonate brands. Advanced validation confirms which findings represent real, active abuse, allowing teams to prioritize threats earlier and intervene before campaigns reach customers or employees.

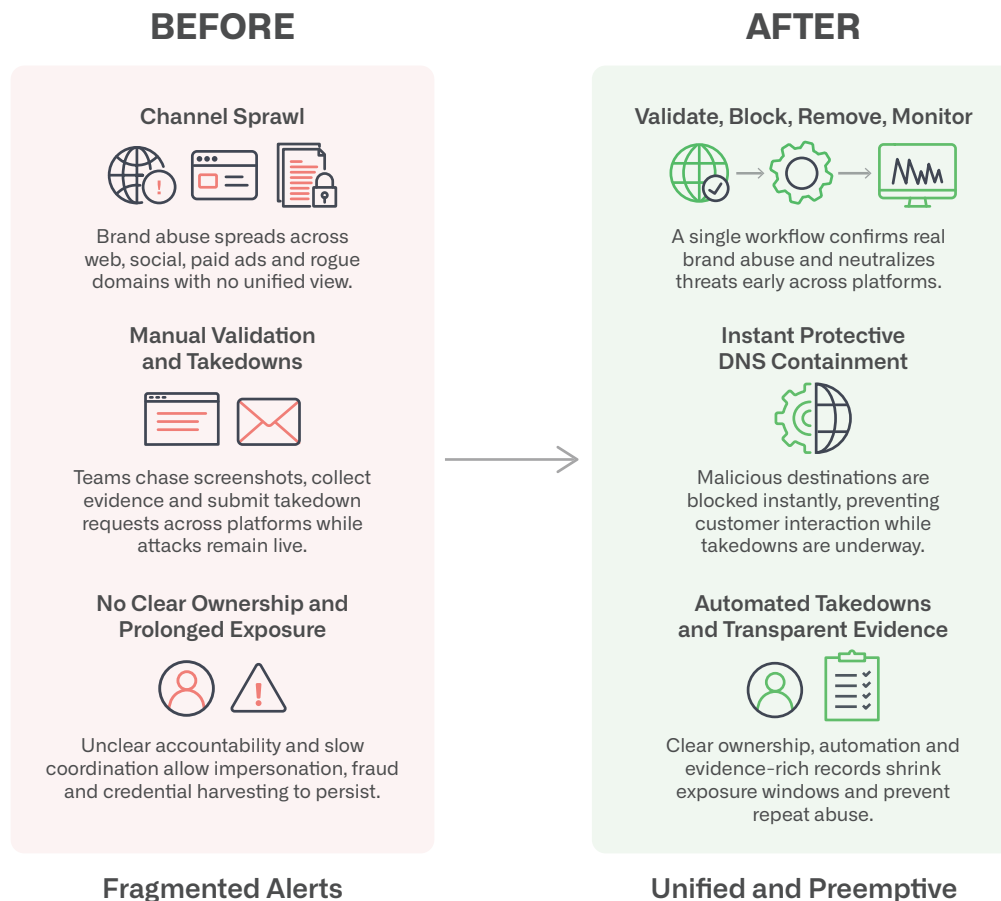


Figure 3. Before and after: From fragmented alerts to unified, preemptive disruption

Automation at Every Phase

Effective brand protection requires speed and scale that manual workflows cannot achieve. Infoblox automates discovery, validation, containment, takedown and ongoing monitoring to eliminate delays and reduce analyst burden.

Key Automation Capabilities

- Continuous discovery of impersonation, phishing, fraud and credential abuse across web, social, ads, apps and marketplaces
- AI-driven validation with visual confirmation and defensible evidence
- Automated takedowns with end-to-end status tracking and verification
- Stay-down monitoring to prevent re-registration and recurring abuse
- Integration with existing security, legal and case management workflows

This automation transforms brand protection from a reactive, ticket-driven process into a preemptive, outcome-driven program.

Immediate User Protection during Active Attacks

While takedown actions are underway, protection begins immediately, closing the critical exposure window attackers rely on.

Infoblox enables organizations to:

- Block access to confirmed malicious destinations through DNS-level enforcement
- Protect employees and managed devices from connecting to impersonation infrastructure
- Deploy browser warnings and safeguards to reduce customer interaction during takedown operations

By combining automated disruption with immediate containment, organizations prevent clicks, credential theft and payment fraud even as attacker assets are being removed.

Sustained Disruption and Attack Suppression

Stopping brand abuse requires more than initial takedown. Attackers routinely relaunch campaigns using new domains, ads and accounts as soon as infrastructure is removed. Infoblox suppresses repeat abuse by continuously monitoring for re-registration, reuse and variations of previously disrupted assets.

Infoblox enables organizations to:

- Detect repeat attacker activity by correlating new assets with historical abuse patterns
- Validate recurrence quickly without restarting manual investigation workflows
- Disrupt re-launched campaigns before they can scale or reach customers
- Break cycles of repeated response that drive operational cost and analyst fatigue

This sustained approach ensures that removed threats stay removed, delivering durable protection rather than short-lived wins.

PREVENT CUSTOMER HARM AND REVENUE LOSS

STOP BRAND ABUSE BEFORE IT REACHES CUSTOMERS AND DISRUPTS BUSINESS OUTCOMES

Brand protection does not need to be reactive, manual or resource-intensive. With Infoblox, organizations shift from chasing incidents to preventing impact, reducing fraud, customer harm and operational overhead.

By acting earlier in the attack lifecycle and automating disruption at scale, teams can eliminate attacker infrastructure before campaigns spread, protect users immediately during active threats and keep malicious assets down once removed. The result is measurable risk reduction, stronger brand trust and consistent protection during high-visibility business moments, without increasing headcount.

Success across Real Customer Implementations

- A global retailer prevented large-scale phishing and impersonation campaigns with sub-minute detection and same-day takedowns, reducing customer fraud before complaints occurred.
- A high-growth fintech achieved **49x ROI in three months** by automating external threat disruption and eliminating the need for additional analyst resources.
- An entertainment and live events organization protected ticket revenue during peak on-sale periods by removing cloned sites fast enough to stop fraud at scale, even during traffic surges.

Infoblox enables faster, smarter and more consistent brand protection, from early detection to verified takedown to sustained prevention.

KEY CAPABILITIES

Continuous external threat discovery identifies brand impersonation, phishing, fraud, rogue apps and credential exposure across domains, web, social platforms, ads and marketplaces.

AI-driven validation with evidence confirms real threats using visual analysis, infrastructure context and indicators of abuse, reducing false positives and accelerating action.

Immediate containment and user protection block access to confirmed malicious destinations through DNS-level enforcement and deploy browser warnings while takedowns are in progress.

Automated disruption and takedowns remove malicious websites, ads, profiles and apps at scale with status tracking, proof of action and verified completion.

Stay-down monitoring and outcome reporting detect re-use and re-registration of attacker assets, prevent recurrence and provide clear reporting that demonstrates risk reduction.



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