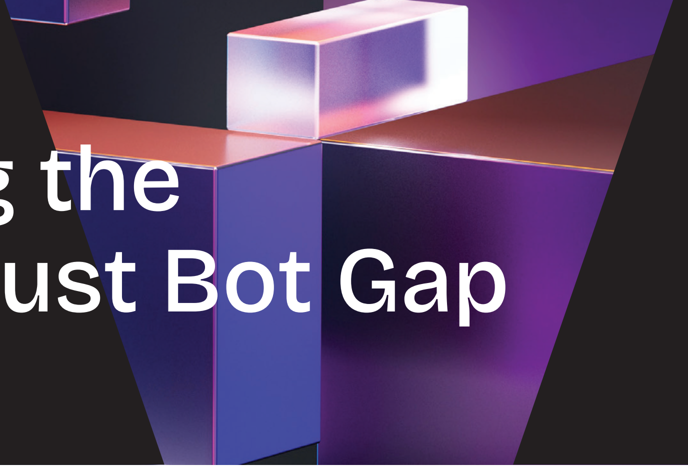
HUMAN



Closing the Zero-Trust Bot Gap

As cyber threats evolve, organizations have increasingly adopted zero-trust architecture (ZTA), which prioritizes continuous verification, strict access controls, and granular monitoring. However, automated threats from sophisticated bots present a unique challenge. Bots can bypass traditional defenses by exploiting authenticated sessions and blending into network traffic, undermining critical aspects of zero-trust, such as identity verification and data security. Closing the "zero-trust bot gap" requires integrating behavioral analytics, AI, and automated response mechanisms to effectively combat bot-driven threats.

Zero-Trust and Bot Challenges

Identity Verification: Traditional methods, like Multi-Factor Authentication (MFA), are vulnerable to bot attacks using stolen credentials. Zero-trust requires continuous verification that includes bot detection throughout the session.

Device Security: While device compliance is typically verified during onboarding, bots can silently exploit authorized devices. Real-time behavioral monitoring is necessary to detect and respond to these threats.

Network Security: Bots use network trust to move laterally and compromise systems. Zero-trust requires micro-segmentation and continuous traffic monitoring to prevent this.

Workload Security: Automated attacks targeting cloud-hosted services and CI/CD pipelines can disrupt operations or insert malicious code. Zero-trust needs real-time monitoring to detect anomalies during workload development.

Data Security: Bots excel at large-scale data scraping and exfiltration. Zero-trust frameworks must integrate bot detection with data access controls to prevent automation from accessing sensitive data.

Visibility & Analytics: Security tools often struggle to differentiate between human and bot behavior, leading to delays in threat detection. Zero-trust must enhance analytics with bot-specific telemetry for more accurate responses.

Automation: Bots outpace manual responses, requiring zero-trust systems to integrate machine-speed automation for immediate threat neutralization.

How HUMAN Security Helps

HUMAN Security provides advanced bot detection solutions across zero-trust's core pillars, helping organizations strengthen their defenses. Key capabilities include:

- **Behavioral Analytics:** Detects anomalous patterns in login, device, and network behavior, identifying bot-driven activities like credential stuffing or lateral movement.
- **AI-Powered Detection:** Continuously improves threat detection models with machine learning, helping organizations stay ahead of evolving bot tactics.
- **Automated Response:** Integrates with security systems like SOAR platforms to automate the mitigation of bot-driven attacks, including session isolation and IP blocking.

Examples of Bot Attacks

- **2021 Microsoft Exchange Server Attack:** Bots exploited stolen credentials, bypassing MFA. HUMAN's continuous identity verification mitigated this risk by monitoring sessions for abnormal login patterns.
- **2021 SolarWinds Supply Chain Attack:** Bots moved laterally through trusted devices. HUMAN's real-time behavioral analysis detected anomalous device activity, helping isolate compromised devices.
- **2022 U.S. OPM Data Exfiltration:** Bots scraped sensitive data using automated queries. HUMAN's bot detection solutions blocked rapid, non-human data access, protecting sensitive datasets.

Policy Recommendations

- **Continuous Verification:** Integrate real-time bot detection with authentication and access control systems.
- **Enhanced Detection:** Adopt micro-segmentation and continuous monitoring at the workload and device levels.
- **AI Integration:** Leverage machine learning and AI-driven solutions to enhance threat detection and automate mitigation.
- **Security Culture:** Regularly train staff to recognize and report bot-related anomalies.

Implementation Guidance

Organizations should take a phased approach to close the Zero-Trust Bot Gap:

- **Phase 1:** Assess bot vulnerabilities and map existing security architecture.
- **Phase 2:** Implement bot detection in high-priority areas, such as identity and network security.
- **Phase 3:** Expand bot detection across all zero-trust pillars, integrating AI for continuous improvement.

Future Outlook

As bot threats grow more sophisticated, zero-trust frameworks will need further advancements, such as predictive analytics and deeper integration with threat intelligence platforms. These innovations will ensure proactive defenses, keeping pace with the evolving nature of automated threats.

To safeguard critical systems and sensitive data, organizations must address the Zero-Trust Bot Gap by integrating intelligent bot detection and automated responses into their zero-trust architectures. HUMAN Security's AI-powered solutions enable organizations to neutralize bot-driven threats and maintain resilient cybersecurity, ensuring protection against the most advanced automated adversaries.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit **www.humansecurity.com**