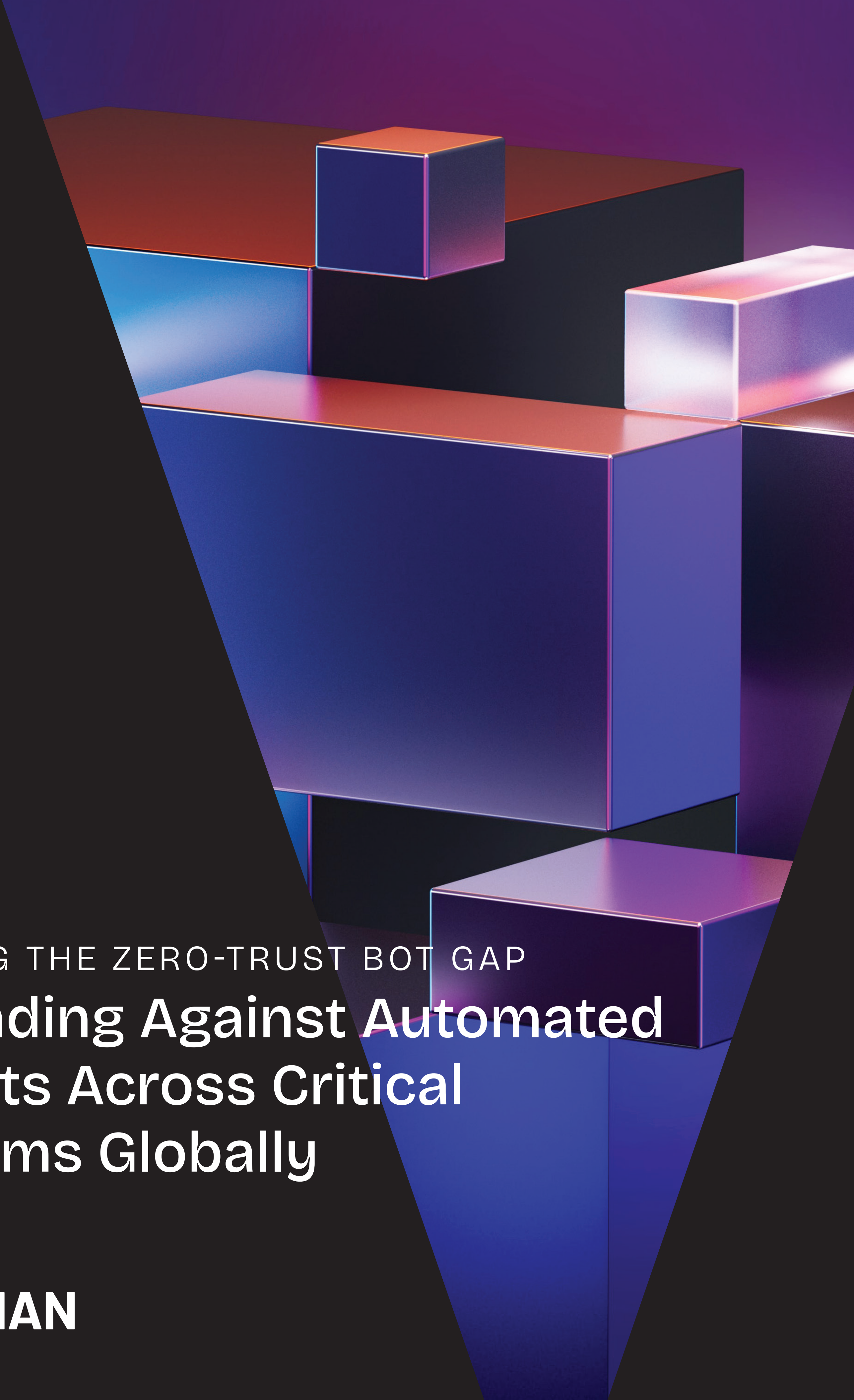

CLOSING THE ZERO-TRUST BOT GAP

Defending Against Automated Threats Across Critical Systems Globally

HUMAN

INTRODUCTION

The evolution of cyber threats has pushed organizations to adopt zero-trust architecture as a gold standard for securing critical systems. Zero-trust moves beyond traditional perimeter defenses, emphasizing continuous verification, strict access controls, and granular monitoring. However, automated adversaries—operating at machine speed—present a persistent and sophisticated challenge to this framework.

Modern bots are no longer simple scripts. They are intelligent, adaptive, and capable of mimicking human behavior to infiltrate systems undetected. Bots exploit trusted states by hijacking authenticated sessions, blending into legitimate network traffic, and manipulating authentication processes. This ability to operate with precision at scale threatens foundational zero-trust principles, including identity verification, workload integrity, and data security.

The zero-trust bot gap highlights a significant vulnerability in traditional implementations. Closing this gap requires an integrated approach—one that leverages real-time behavioral analytics, artificial intelligence, and automated response mechanisms to detect, mitigate, and neutralize bot-driven threats effectively.

HUMAN Security, a recognized leader in bot detection and mitigation, delivers solutions purpose-built to secure sensitive data, protect critical systems, and fortify zero-trust frameworks against automated adversaries. By addressing the zero-trust bot gap, organizations can enhance operational continuity, bolster public trust, and defend their infrastructure against the most advanced cyber threats.

This white paper explores the pillars of zero-trust, analyzing the specific risks posed by bots and how HUMAN's advanced capabilities empower organizations to achieve resilient, future-ready cybersecurity.

Identity Pillar

Challenge:

Identity verification is foundational to zero-trust. However, traditional methods like multi-factor authentication (MFA) often fail against bots that exploit stolen credentials and hijack authenticated sessions.

Needed Change for Zero-Trust:

Move beyond static authentication methods to continuous verification that integrates bot detection at every session stage.

How HUMAN Helps:

- **Continuous Identity Verification:** Combines MFA with ongoing human-versus-bot checks to ensure that authenticated sessions remain controlled by legitimate users.
- **Behavioral Analytics:** Detects unusual login patterns, synthetic identities, and credential stuffing attempts driven by automated attackers.
- **AI-Enhanced Behavioral Analytics:** Utilizes advanced machine learning models to analyze vast interaction data, identifying subtle anomalies in user behavior for higher accuracy in detecting synthetic identities and credential stuffing.
- **Incident Response:** Immediately isolates compromised accounts, revokes session tokens, and blocks malicious automation.
- **User Education:** Trains staff to recognize suspicious login prompts and report anomalies, reinforcing a security-aware culture.

Example: 2021 Microsoft Exchange Server Vulnerabilities

In this case, bots bypassed MFA by exploiting stolen credentials, highlighting the limits of static verification. Zero-trust requires real-time session monitoring to detect abnormal login patterns and prevent automated threats. HUMAN's solutions introduce continuous human-versus-bot checks to validate authenticity throughout the session, ensuring compromised accounts are immediately neutralized.

Device Security Pillar

Challenge:

Traditional device verification focuses on compliance at onboarding but fails to detect bot-driven threats operating silently on otherwise authorized devices.

Needed Change for Zero-Trust:

Implement real-time behavioral monitoring and integrate bot detection directly with endpoint security tools.

How HUMAN Helps:

- **Global Device Reputation Insight:** Identifies if a device ID has previously exhibited malicious activity across monitored ecosystems.
- **Real-Time Behavioral Analysis:** Detects abnormal device usage patterns that suggest automated control.
- **Integration with EDR/UEM:** Prompts device isolation, revalidation, or stricter compliance checks upon detecting automation-driven anomalies.

Example: 2021 U.S. Department of Homeland Security (DHS) Device Compromise via SolarWinds Supply Chain Attack

The SolarWinds attack exploited trusted software to infiltrate government networks. Zero-trust must extend to real-time device monitoring for anomalous activity, even on pre-verified devices. HUMAN's solutions detect behavioral deviations indicative of automation, enabling organizations to isolate compromised devices before bots can exploit their access.

Network Security Pillar

Challenge:

Bots exploit network trust by blending into normal traffic, establishing command-and-control channels, or moving laterally to compromise additional resources.

Needed Change for Zero-Trust:

Adopt dynamic micro-segmentation informed by bot detection to prevent lateral movement and continuously monitor traffic for anomalies.

How HUMAN Helps:

- **Micro-Segmentation:** Informed by bot detection signals, enforces tighter network segmentation and denies lateral movement by automated adversaries.
- **Continuous Monitoring:** Identifies unusual traffic patterns, suspicious connections, and abnormal data transfers that signal bot-driven exploitation.rs.
- **Incident Response:** Rapidly isolates affected segments, blocks malicious traffic, and initiates remediation steps upon detecting a bot-driven breach attempt.

Example: 2021 Colonial Pipeline Ransomware Attack

Attackers used compromised credentials to navigate laterally through the network. Traditional segmentation proved insufficient. Zero-trust requires bot-aware segmentation policies to detect and block automated lateral movement. HUMAN's continuous traffic analysis and segmentation tools enforce dynamic restrictions, minimizing the attack surface.

Workload Pillar

Challenge:

Government workloads—including cloud-hosted services, CI/CD pipelines, and mission-critical applications—are prime targets for automated attacks aiming to disrupt operations or insert malicious code.

Needed Change for Zero-Trust:

Implement real-time workload monitoring to detect and isolate bot-driven anomalies during development and deployment.

How HUMAN Helps:

- **Baseline Normal Behavior:** Continuously monitors workloads, establishing normal operation patterns to quickly identify deviations caused by bots.
- **Immediate Containment:** Upon detecting malicious automation, isolates affected workloads, blocks suspicious processes, and prevents malware spread.
- **Machine Learning-Driven Detection:** Refines detection models with real-time threat intelligence, staying ahead of evolving bot tactics.

Example: 2023 UK Ministry of Defence Contractor Hack

Automated attacks targeted CI/CD pipelines to compromise military data. Zero-trust frameworks must enforce strict behavioral baselines for workloads and flag deviations caused by automation. HUMAN's AI-powered workload monitoring identifies malicious patterns, preventing bots from disrupting mission-critical operations.

Data Pillar

Challenge:

Automated adversaries excel at large-scale data scraping and exfiltration, posing severe risks to sensitive citizen information, military intelligence, and government research.

Needed Change for Zero-Trust:

Integrate bot detection into data access controls, monitoring for automation in real time and blocking non-human requests.

How HUMAN Helps:

- **Strict Access Controls:** Ensures only verified human actors can query or download sensitive datasets.
- **Continuous Monitoring:** Detects non-human data access patterns—such as rapid, bulk extraction attempts—and blocks them instantly.
- **Data Classification and Encryption:** Combines bot detection with robust encryption and labeling, ensuring that even if a data request appears legitimate, suspicious automation is promptly challenged.

- **AI-Enhanced Data Monitoring:** Detects and responds to large-scale automated scraping and exfiltration attempts with greater precision.

Example: 2022 U.S. Office of Personnel Management (OPM) Data Exfiltration Attempt

Bots scraped sensitive records at scale, bypassing basic access controls. Zero-trust mandates continuous monitoring of access patterns, flagging excessive or rapid data queries. HUMAN's solutions detect and block bot-driven scraping, protecting sensitive datasets even during legitimate-looking access attempts.

Visibility & Analytics Pillar

Challenge:

Security tools often lack the ability to distinguish human activity from bot behavior, leading to investigative delays and noise in incident reports.

Needed Change for Zero-Trust:

Enhance analytics with bot-specific telemetry, integrating these signals into SIEM and UEBA systems to improve response accuracy.

How HUMAN Helps:

- **Clear Signals for SOC Teams:** Provides definitive indicators that highlight automated activities, helping analysts quickly identify genuine threats versus benign anomalies.
- **Enhanced UEBA & SIEM Efficiency:** By eliminating bot noise, tools can focus on actual human-driven anomalies, reducing false positives and investigative overhead.
- **Threat Intelligence Sharing:** Integrates bot detection intelligence with threat intel platforms for proactive detection of new automated TTPs.
- **Advanced Dashboard & Investigation Tools:** Features enhanced dashboards and AI-powered investigation tools that provide comprehensive visibility into attack patterns and attacker profiles.

Example: 2020 ENISA Threat Landscape Report

Organizations struggled to filter bot-driven anomalies from legitimate activities, overburdening SOC teams. Zero-trust requires clear differentiation between human and automated behavior to improve response efficiency. HUMAN's bot intelligence provides actionable insights, allowing SOC teams to focus on real threats.

Automation Pillar

Challenge:

Bots outpace manual responses, overwhelming traditional workflows and escalating attacks before mitigation can occur.

Needed Change for Zero-Trust:

Integrate machine-speed response capabilities into automation tools like SOAR platforms, ensuring bots are neutralized in real time.

How HUMAN Helps:

- **Rapid Machine-Speed Decisions:** Integrates with SOAR platforms to immediately quarantine suspicious sessions, block malicious IPs, or disable compromised accounts.
- **Harmonized Response:** Orchestrates various security tools—EDR, SIEM, firewalls—to act collectively and decisively against automated attacks.
- **Reduced Analyst Burden:** Frees security teams from constant manual triage, enabling focus on strategic threats.
- **AI-Powered Mitigation Workflows:** Executes automated response workflows based on real-time threat analysis, ensuring that automated attacks are neutralized before they can propagate.

Example: 2021 U.S. Internal Revenue Service (IRS) Automated Bot Mitigation

Automated attacks targeted tax records, exposing the need for real-time responses. Zero-trust must adopt automated bot mitigation workflows that integrate with SOAR platforms to immediately quarantine sessions or block malicious IPs. HUMAN's AI-driven automation ensures threats are stopped before they propagate.

POLICY RECOMMENDATIONS

1. **Implement Continuous Verification**
   - Integrate multi-factor authentication with real-time human authenticity checks
   - Establish ongoing behavioral analysis to detect non-human patterns

2. **Enhanced Threat Detection**
   - Adopt micro-segmentation informed by bot detection signals
   - Implement workload-level protection with continuous monitoring
   - Encrypt and classify data with strict access controls

3. **Advanced Technology Integration**
   - Leverage AI and machine learning for adaptive threat detection
   - Integrate bot intelligence into existing security platforms
   - Develop automated response mechanisms

4. **Organizational Culture**
   - Conduct regular security awareness training
   - Foster a culture of proactive threat detection
   - Establish metrics to measure bot mitigation effectiveness

Phased Zero-Trust Bot Gap Mitigation Approach

Phase 1: Assessment and Planning

- Conduct comprehensive bot vulnerability assessment
- Map existing security architecture against zero-trust principles
- Identify critical systems and potential bot infiltration points
- Develop a prioritized mitigation roadmap

Phase 2: Foundational Implementation

- Start with high-impact areas: Identity and network security
- Select pilot programs for initial deployment
- Establish baseline metrics for bot detection and mitigation

Phase 3: Advanced Integration

- Expand bot detection capabilities across all zero-trust pillars
- Implement advanced AI-driven detection mechanisms
- Develop continuous improvement framework

FUTURE OUTLOOK

As bot threats continue to evolve in sophistication and scale, the integration of artificial intelligence and machine learning into zero-trust frameworks will become increasingly vital. AI-driven solutions, like those developed by HUMAN Security, offer the adaptability and intelligence required to anticipate and counteract emerging automated threats. Future advancements may include:

- **Granular Behavioral Biometrics:** Enhanced methods to distinguish between human and bot activities with higher precision.
- **Predictive Analytics:** Improved capabilities to forecast and preempt bot-driven attacks before they occur.
- **Deeper Integration with Threat Intelligence Platforms:** Providing more comprehensive and actionable threat intelligence to bolster proactive defenses.
- **Enhanced Automation Capabilities:** Further automation of threat detection and response processes to keep pace with the rapid evolution of bot tactics.

These advancements will ensure that zero-trust architectures remain resilient and proactive in safeguarding critical infrastructure and sensitive data against automated threats.

CONCLUSION

The increasing sophistication of bot threats demands urgent and innovative action. By bridging the zero-trust bot gap, organizations can reinforce the integrity of their security frameworks while safeguarding sensitive systems and data.

HUMAN Security's solutions, built on a foundation of advanced AI, real-time analytics, and unparalleled scalability, empower government agencies and enterprises to meet these challenges head-on. By integrating intelligent bot detection into zero-trust architectures, organizations can neutralize automated adversaries, maintain operational resilience, and uphold public trust in an era of evolving threats.

The path to securing critical systems begins with addressing the zero-trust bot gap—and the time to act is now.

SOURCES

1. **Greenberg, A.** (2021, March 5). Chinese Hacking Spree Hit an 'Astronomical' Number of Victims. *Wired*. Retrieved from **https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/**
2. **Goodin, D.** (2022, October 5). NSA: Someone hacked military contractor and stole data. *The Register*. Retrieved from **https://www.theregister.com/2022/10/05/military_contractor_hack/**
3. **Cybersecurity and Infrastructure Security Agency (CISA).** (2021, May 11). *DarkSide Ransomware: Best Practices for Preventing Business* Disruption *from Ransomware Attacks*. Retrieved from **https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a**
4. **Cybersecurity and Infrastructure Security Agency (CISA).** (2020, December 17). *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*. Retrieved from **https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a**
5. **U.S. Government Accountability Office.** (2022, November). *DOD Cybersecurity: Improved Controls Needed to Protect* Sensitive *Data and Systems*. Retrieved from **https://www.gao.gov/assets/gao-23-105084.pdf**
6. **The Times.** (2023). *China hacked Ministry of Defence target in breach of contractor systems*. Retrieved from **https://www.thetimes.com/uk/politics/article/china-hacked-ministry-defence-target-military-personnel-6wzbvsrct**
7. **European Union Agency for Cybersecurity.** (2020). *ENISA Threat Landscape 2020*. Retrieved from **https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020**
8. **Internal Revenue Service.** (2021, October 22). *IRS Enhances Security Measures to Protect Against Automated Attacks*. Retrieved from **https://federalnewsnetwork.com/cybersecurity/2024/08/irs-working-to-improve-data-security-after-major-tax-return-leak/**
9. **HUMAN Security, Inc.** (2024, August 6). *HUMAN Security Enhances Decision Engine with AI-Derived Capabilities*. Retrieved from **https://www.humansecurity.com/newsroom/human-security-enhances-decision-engine-with-ai-derived-capabilities**

APPENDIX: MAPPING HUMAN SECURITY'S CAPABILITIES TO ZERO-TRUST ACTIVITIES

To provide a comprehensive understanding of how HUMAN Security's solutions align with zero-trust principles, the following table maps HUMAN Security's capabilities to specific zero-trust activities and their desired outcomes. Detailed mappings can be found below.

Zero-Trust Activity Mapping

Zero-Trust Activity	Outcome/Goal	HUMAN's Contribution
Identity		
1.2 Conditional User Access	Dynamically control user access based on risk	Detects malicious automation attempts, enabling denial or step-up auth.
1.3 Multi-Factor Authentication (MFA)	Require multiple factors to authenticate users	Flags bots brute-forcing MFA, ensuring only humans pass.
1.6 Behavioral, Contextual ID, and Biometrics	Enhance risk-based access with behavioral analytics	Identifies non-human patterns, improving UEBA fidelity.
1.7 Least Privileged Access	Limit user access to only what is needed	Blocks automated privilege escalation attempts.
1.8 Continuous Authentication	Continuously validate user sessions	Prevents bot takeovers mid-session with ongoing checks.
Device		
2.1 Device Inventory	Only known and authorized devices gain access	Adds global reputation data, warning if a device is historically malicious.
2.2 Device Detection and Compliance	Ensure devices meet security posture	Signals EDR/UEM if device shows risky automated patterns, prompting isolation.

Zero-Trust Activity	Outcome/Goal	HUMAN's Contribution
2.3 Device Authorization with Real-Time Inspection	Continuously verify device integrity	Detects suspicious automation on trusted devices, maintaining device trustworthiness.
Workload		
3.2 Secure Software Development & Integration	Integrate security into DevSecOps pipelines	Detects malicious automation at runtime (e.g., Code Defender).
3.3 Software Risk Management	Secure supply chain and code integrity	Flags bots introducing or exploiting malicious code.
3.4 Resource Authorization & Integration	Dynamically manage resource access based on attributes	Differentiates human from bot requests, ensuring correct access decisions.
3.5 Continuous Monitoring & Ongoing Authorizations	Near real-time visibility into app security	Immediate revocation or adjustment of access when automation is detected.
Data		
4.3 Data Labeling and Tagging	Consistent and accurate data classification	Detects automated scraping, protecting sensitive data.
4.4 Data Monitoring and Sensing	Capture metadata and detect malicious data use	Flags non-human patterns signaling automated exfiltration attempts.
4.5 Data Encryption & Rights Management	Protect data at rest and in transit	Prevents bots from accessing even encrypted content.
4.6 Data Loss Prevention (DLP)	Detect and mitigate data exfiltration attempts	Identifies large-scale automated scraping for immediate DLP action.

Zero-Trust Activity	Outcome/Goal	HUMAN's Contribution
Network		
5.3 Macro Segmentation	Establish network perimeters	Prevents automated sessions from pivoting between segments.
5.4 Micro Segmentation	Granular segmentation based on identity/app	Blocks non-human patterns before bots move laterally.
Automation & Orchestration		
6.1 Policy Decision Point & Orchestration	Centralize and automate policy enforcement	HUMAN signals inform PDPs to allow, challenge, or block requests.
6.2 Critical Process Automation	Automate repetitive security tasks	HUMAN's intelligence triggers SOAR runbooks to quarantine bots.
6.5 Security Orchestration, Automation & Response (SOAR)	Enable rapid incident response	Detection prompts immediate playbook actions, neutralizing threats quickly.
Visibility & Analytics		
7.1 Log All Traffic	Comprehensive visibility into events	Distinguishes human from automated traffic, improving log value.
7.2 SIEM	Centralize and correlate security logs	Enhances correlations, filtering out bot-driven noise.
7.3 Common Security and Risk Analytics	Unified analysis of multiple data types	Improves baseline accuracy, reducing false positives.

Zero-Trust Activity	Outcome/Goal	HUMAN's Contribution
7.4 User and Entity Behavior Analytics (UEBA)	Detect behavioral anomalies	Identifies non-human patterns, refining threat detection.
7.5 Threat Intelligence Integration	Leverage threat intel for proactive defense	Adds bot indicators to threat intel, detecting emerging TTPs early.

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**