DATASHEET

Unlock Proactive Network Security with Intent-Based Automation

In today's ever-evolving threat landscape, siloed operations teams with reactive approaches to security incidents are no longer sufficient to defend against distributed cyber-attacks. NetBrain's **intent-based security and network automation platform – Next-Gen**, powered by a **live digital twin**, enables organizations to shift from reactive to proactive security by aligning with **Cybersecurity Mesh (CSMA)** and **Zero Trust (ZTNA)** principles. This approach provides continuous hybrid network observability via proactive security assessments to identify misconfigurations network-wide and stop threats before they escalate.

Modern SecOps Challenges

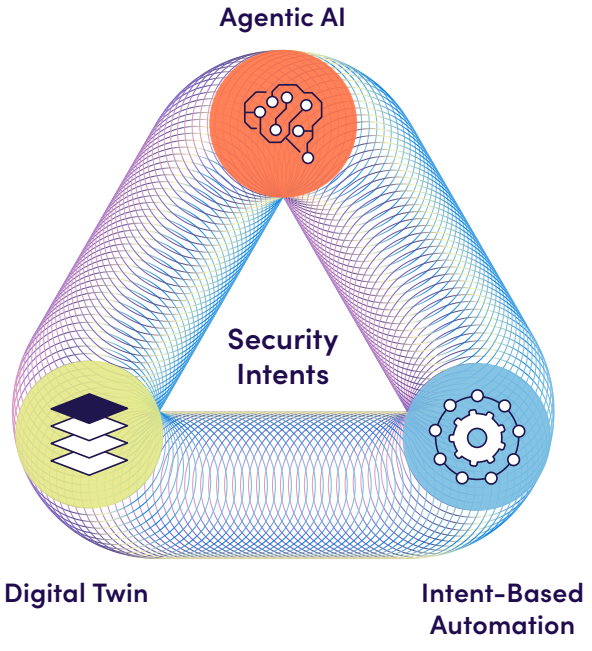
Security operations teams face persistent challenges, including:

- **Outdated documentation** that fails to reflect the current network state.
- **Configuration drift** that deviates from established security baselines.
- **Slow response and recovery times**, increasing organizational risk.

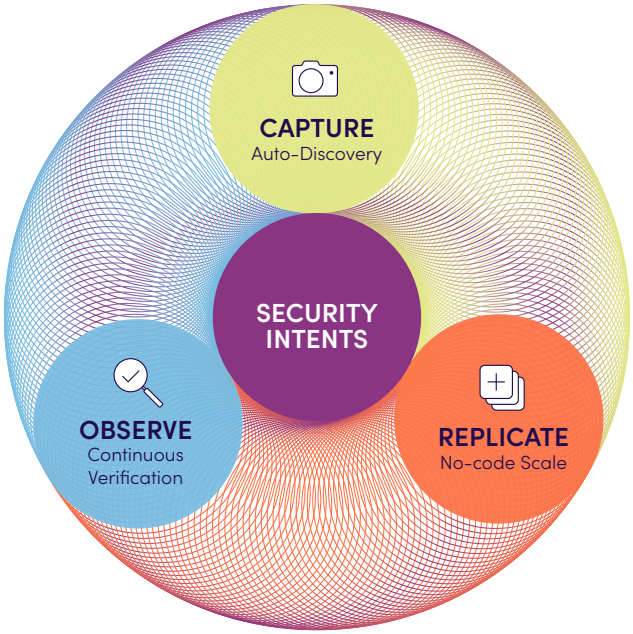
SOAR Smarter with Intent-Based Network Security Automation and Observability

NetBrain's Next-Gen platform leverages three core components to achieve Security Orchestration, Automation, and Response (SOAR):

1. **Digital Twin** – A live model of the hybrid network topology with flows and intents serves as the foundation for security validation.
2. **Intent-Based Automation** – This adaptive system monitors security policies, auto-discovers hybrid devices and intents,, and enforces compliance across the infrastructure.
3. **Agentic AI** – An intelligent orchestrator that connects security tools for faster, more accurate threat response.



Turn incident response into resilience with context-aware live network topology, attack path mapping, and orchestrated auto-remediation. Respond faster with AI and automation and prevent every attack using security intent to establish a proactive observability posture. Define what to assess and observe with seed intents and replicate them with no-code across the entire network for holistic monitoring and assurance.



Hybrid-Cloud Network Visibility

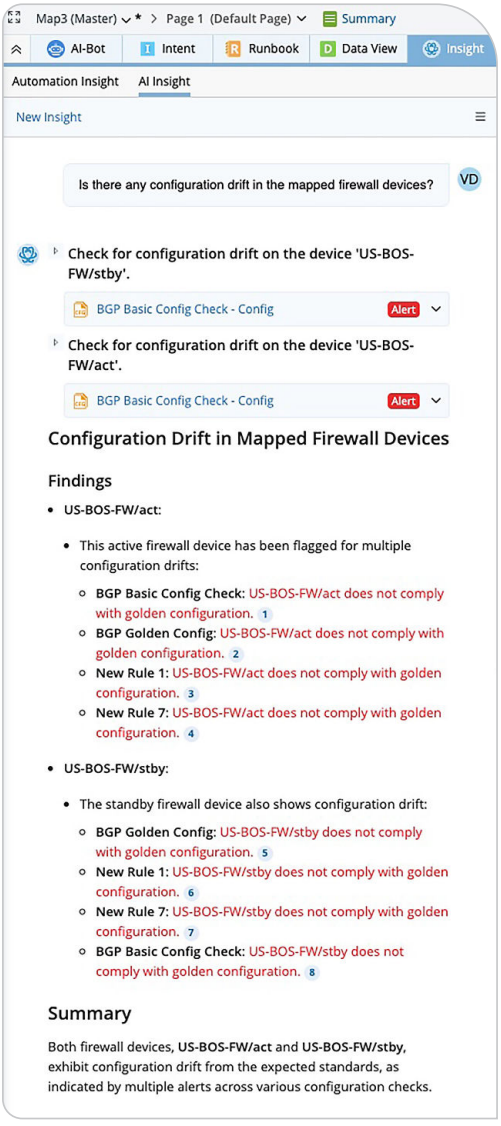
NetBrain helps organizations maintain security standards by providing auto-discovery and dynamic network mapping and pathing to visualize and remediate security configuration drift.

- **Dynamic Map Powered by Digital Twin:** For hybrid network mapping and pathing with real-time policy compliance monitoring.

Incident Detection & Response

Accelerate incident resolution by combining AI Insight with real-time diagnosis, automation, and remediation. The platform continuously monitors the network to identify policy violations - triggering instant alerts and AI-driven corrective actions. Key capabilities include:

- **Automated Threat Diagnosis and Response:** AI-driven automation runbooks enable auto-diagnosis, auto-remediation, and AI-powered documentation of troubleshooting workflows. AI Insight lets you query network automation using Agentic AI in natural language to analyze previously imported SME-created knowledge documents, find associated automation, and perform reason-based actions to achieve desired results.
- **Seamless 3rd-Party Integrations:** API integration with Splunk SIEM, ServiceNow, and other leading tools for automated cross-platform diagnosis and remediation.
- **Instant Asset Locator:** One-IP Table for immediate IP/MAC address lookup

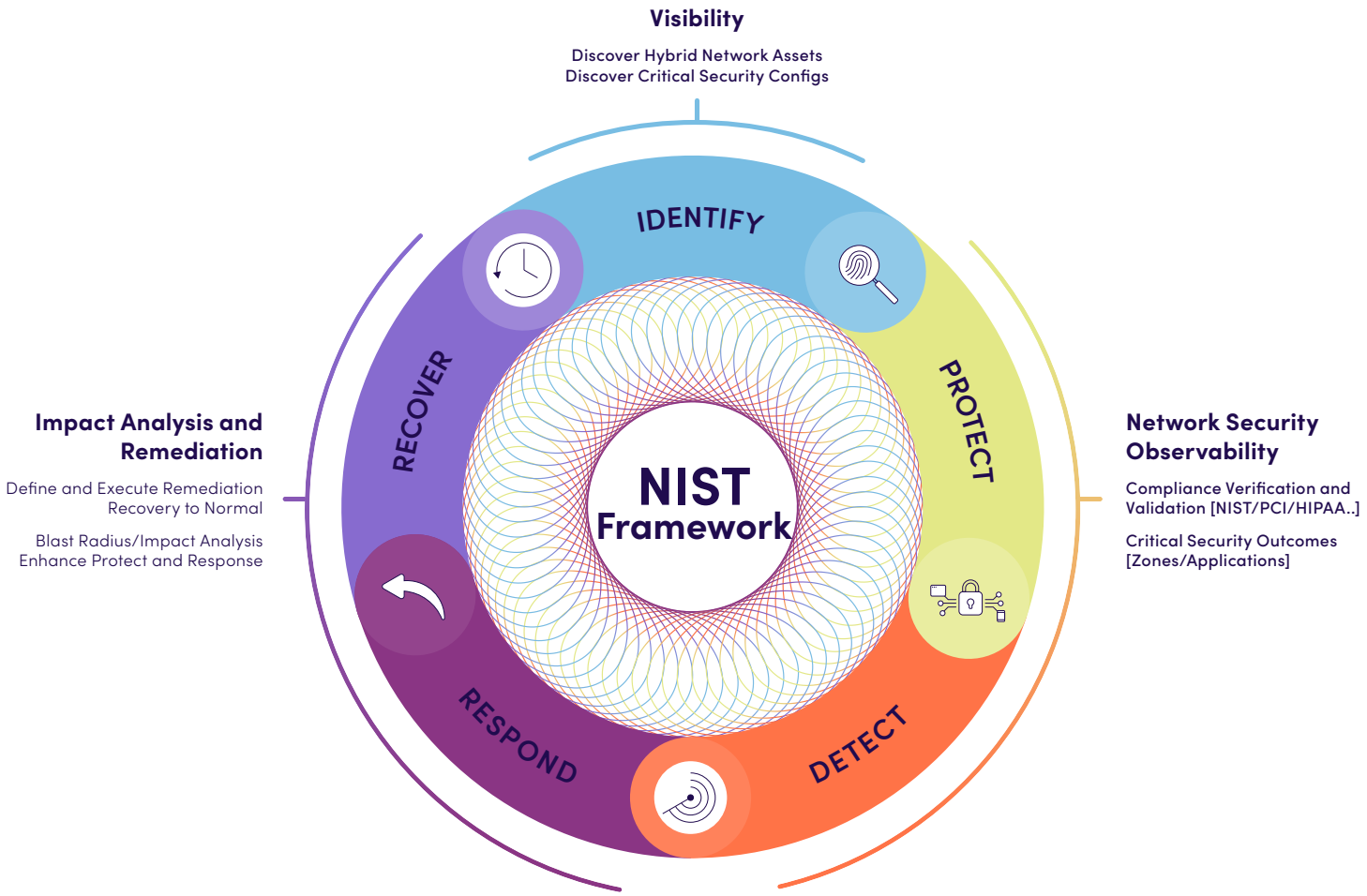


Continuous Assessment - From Reactive Response to Proactive Resilience

Post-attack assessments use Intent as automation to help identify similar risks across your entire network.

Continuous security assessments help you defend network security with customizable observability dashboards and alerts with:

- **A Golden Assessment Library** of pre-built risk assessments.
- **Full stack observability** by monitoring vulnerabilities, traffic flows across DMZ and production zone boundaries to enforce security baselines, detect and auto-remediate drift.
- **Assess NIST Compliance** - Automated compliance (NIST/PCI/HIPAA) assessment for device hardening and access policies and regulatory compliance through continuous network assessment and auto-remediation.
- **Assess Access Controls** - The platform enables continuous validation of critical security controls, including AAA, ACLs, TACACS, and segmentation rules.



Cloud Network Security

Extend protection to cloud environments with:

- **Multi-layered security checks** (Network, Server, Data, Application).
- **Continuous monitoring** for defense-in-depth.
- **Built-in automation assessments** to enforce cloud security policies.

Security Intent - A Force Multiplier for Security Operations Teams

NetBrain transforms network data into actionable intelligence, enabling teams to:

- **Stop chasing alerts** by automating investigations.
- **Visualize every attack path**—whether on-premises, hybrid, or cloud.
- **Break down silos** between SecOps and NetOps.
- **Build self-defending networks** that adapt to evolving threats

Experience the power of proactive intent-based security with NetBrain!

Test-drive these features in our interactive experience lab, or explore the capabilities using your own network data to run a secure network assessment in minutes.