Booz Allen

Vellox Ranger™

A Booz Allen® Product

Don't Let Discovery Outpace Defense

AI is accelerating the vulnerability landscape on both sides – *attackers* can now explore a broader set of weaknesses at a fraction of the cost, while *defenders* are uncovering flaws earlier and in far greater volume. Yet every potential fix still demands rigorous validation, thorough testing, and careful deployment into production.

Recent advances in frontier AI models, like Anthropic's Claude Mythos, have underscored the urgency of this challenge – zero-day vulnerabilities can be identified and weaponized at scale in near real-time. What once took days or weeks is now compressed into minutes, drastically shrinking the window between vulnerability discovery and exploitation.

Frontier Vulnerability Discovery by the Numbers

Since May 2026

Up to **20x** as many Firefox vulnerabilities patched monthly by Mozilla as the previous year's monthly average.[i]

5x increase in CVEs disclosed by Palo Alto Networks compared with its "typical" monthly volume.[ii]

3x as many vulnerabilities patched by Microsoft in July as in June. Microsoft's 2026 year-to-date total of 1,380 already exceeds the 1,250 patched in all of 2020, the previous annual record.[iii]

Manage and Prioritize this Volume of Data with Vellox Ranger™

Frontier models don't just surface more vulnerabilities – they surface them faster than any team can review. Teams have become overwhelmed with the flood of vendor patches and new vulnerabilities discovered across their enterprise assets. The problem isn't a shortage of options; it's deciding which ones are worth acting on first.

Vellox Ranger solves this by building a living map of your actual environment – assets, topology, telemetry, and existing rules – and using it to test every candidate threat against two questions: Is it exposed here? Would an attacker actually use this path in this environment? Only candidates that clear both move forward. Everything else is noise, filtered out before it reaches your team.

What survives that filter becomes Vellox Ranger's output: a focused, ranked set of detection rules built for your specific systems and tools – not generic signatures. Generated directly from your environment, each rule can deploy the moment a threat is confirmed, with or without a patch. These are compensating controls in action – detection logic that monitors unmitigated vulnerabilities, gives you line of sight into your highest-priority risk areas, and buys your patch and remediation teams time to catch up.

The payoff is time. Autonomous attackers act in minutes. Vellox Ranger turns an overwhelming flood of possible threats into the few that matter and turns each of those into an action your team can take today.

Key Product Features

Environment-First Rule Generation
Builds detection logic from customer-provided environment context, including assets, vulnerabilities, topology, telemetry assumptions, and existing detections.

Data Integration & Processing
Growing list of turn-key connectors such as Tenable, ServiceNow, eMASS, GitHub/Lab. Can support environment, threat, and vulnerability data from frontier LLMs (Mythos, GPT-Cyber, etc). Ad-hoc file upload also available when persistent connections are not preferred.

Threat Intelligence Relevance Filtering
Includes threat intelligence and filters it through the customer environment so relevant threats drive rule generation and irrelevant noise stays out of the backlog.

MITRE ATT&CK Coverage Mapping
Maps detection coverage and relevant exposure to MITRE ATT&CK® Coverage Mapping owned by the MITRE Corporation, giving teams a structured view of coverage, gaps, and improvement over time.

Automated Assessment of Existing Rules
Uses existing rules as context, helping preserve what works, identify improvement opportunities, and avoid starting every refresh cycle from zero.

SIEM-Native Rule Adaptation
Adapts detection logic for execution environments such as Splunk SPL, Microsoft KQL, Elastic EQL, and CrowdStrike FQL.

Governed PR/MR Delivery
Stages rule changes through GitHub pull requests or GitLab merge requests, keeping review, approval, modification, and deployment control with the security team.

Long-Lived Rule Lifecycle
Treats rules as durable objects with stable identity, lineage, and version history, so each cycle builds on prior work.

Workflow-Informed Improvement
Engineer edits, comments, descriptions, and review decisions become context Vellox Ranger can use to improve future outputs.

Triggered Ruleset Refresh
When new files are uploaded or connected sources are synced, Vellox Ranger reevaluates the environment and generates new or improved detection logic against the updated terrain.

[i] https://www.theregister.com/security/2026/05/08/mozilla-says-ai-helped-squash-423-firefox-security-bugs/5235438

[ii] https://www.paloaltonetworks.com/blog/2026/05/defenders-guide-frontier-ai-impact-cybersecurity-may-2026-update/

[iii] https://www.pcworld.com/article/3191612/microsofts-july-patches-fix-over-600-flaws-shattering-last-months-record

Booz Allen

About Booz Allen

Booz Allen is an advanced technology company. We build commercial-grade products and solutions for America's most critical defense, civil, and national security priorities.

NYSE: BAH

Request a demo to see Vellox Ranger in action.

Experience how Vellox Ranger understands your environment to create detection logic deployable through workflows you trust

boozallen.com/vellox-ranger **info@vellox.bah.com**