



CrowdStrike and appNovi

Unify your security data to identify security control gaps, map the attack surface, and enable efficient non-disruptive incident response.

appNovi integrates with your existing tools to converge all data into a centralized data plane. Data normalization enables those without specialization or technical knowledge to search across and explore enterprise data, and more effectively communicate risk through visualization. Enterprises that implement a Cybersecurity Mesh Architecture platform like appNovi gain total asset visibility and network dependency mapping. The outcome is the ability to identify risk earlier and respond faster through more effective attack surface mapping, vulnerability prioritization, and shortened response times.

The Challenge

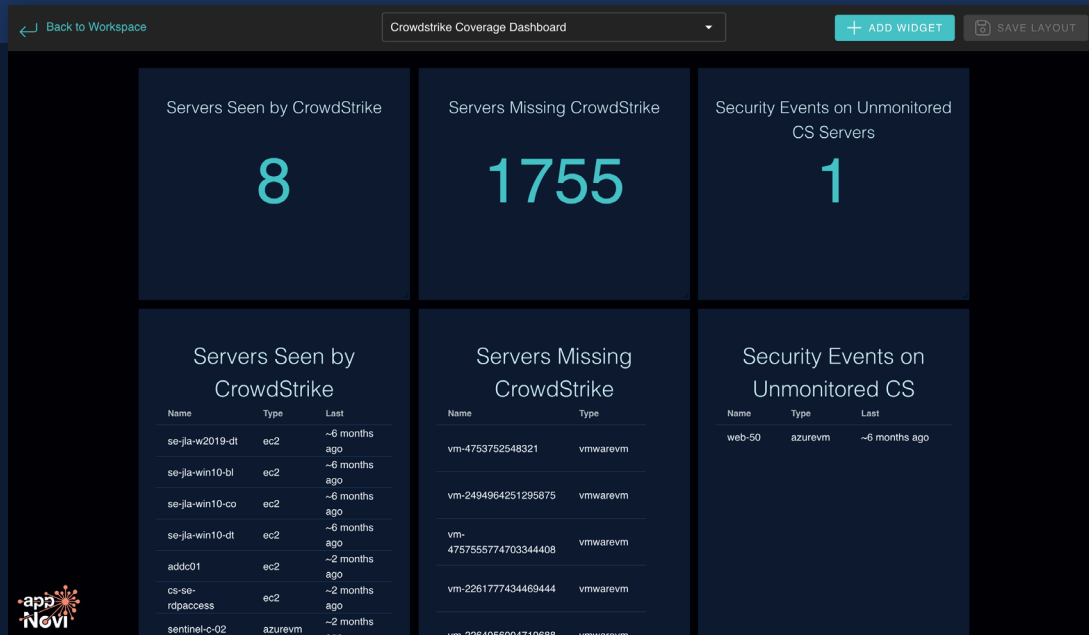
Many organizations don't have a tool problem, they have a data problem. Ineffective security operations centers (SOCs) can spend more time on manually aggregating and analyzing data in spreadsheets than on making security decisions. Analysts can take hours to find, aggregate, and review data from your network and security tool data lakes in order to understand and resolve a potential incident.

Without effective contextual correlation across data sets and data lakes, the trustworthiness of data is low, the efficacy of SOCs is heavily impeded, prioritization isn't business-specific, and the resolution of security incidents is often partial or incomplete due to too much uncertainty.





CrowdStrike and appNovi



The Solution

Unify unmanageable data by integrating your existing network and security datasets across your growing environment in a single interface. appNovi contextually aggregates all of your network, security, and business data to visualize, analyze, and share cybersecurity analytics with relevant stakeholders. By integrating your existing business and security tools, including the CrowdStrike Falcon® platform, appNovi enables your team to contextually converge disparate data sources to drive meaningful outcomes that reduce risk to the business.

Built by practitioners for practitioners, appNovi, combined with rich security data across endpoints, workloads, and identities from the Falcon platform, ensures that your entire attack surface is identified and mapped, vulnerabilities are prioritized based on business context, and incident response teams efficiently visualize and analyze their security data to make informed and effective incident resolution decisions.

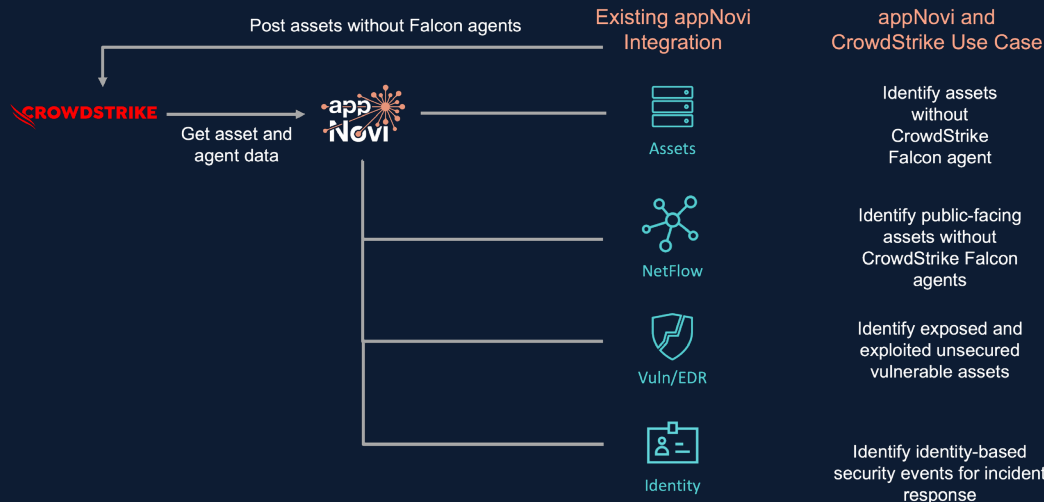
The Business Value

Use Case	Solution	Benefits
Overcome unmanageable data	Integrate, converge, and deduplicate your asset inventories and automate security control gap analysis	Align to CIS core controls 1 and 2, eliminate manual security control gap analysis, orchestrate remediation, and maximize existing tool usage
Make decions that reduce business risk	Achieve network and business context to understand which assets are most critical to the business and are contextually exposed	Demonstrate return on tools, personnel, and resources through risk reduction from the business perspective
Eliminate uncertainty of security actions	Understand the full business impact of security decisions to avoid network outages	Reduce mean time to respond (MTTR), increase remediation capacity with existing resources, and obtain assurance of non-disruption before making network changes





CrowdStrike and appNovi

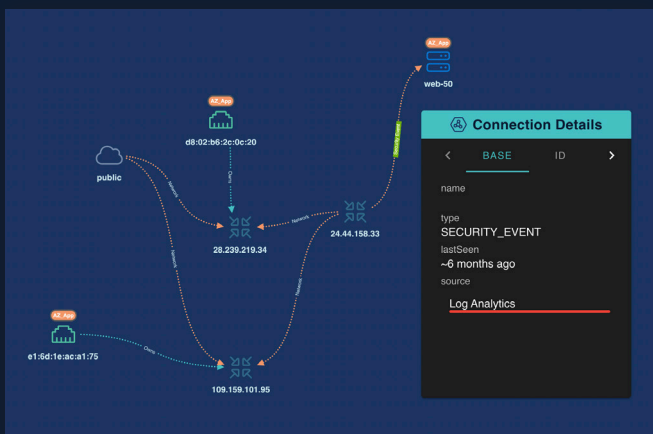


Key Benefits

- Use appNovi and CrowdStrike Falcon to identify unmonitored devices
- Prioritize business-critical assets
- Visualize threats with network and business context
- Communicate risk easily to non-technical stakeholders
- Maximize ROI of your CrowdStrike Falcon investment
- Uplevel junior analysts with abstraction and automation

The Technical Integration

Eliminate manual swivel-chair analysis efforts by experienced security analysts and engineers, and empower security operations teams to prioritize risk based on the business and avoid business-impacting outages. appNovi integrates with the CrowdStrike Falcon platform, leveraging APIs to converge security data and deduplicate cyber asset inventories to make efficient, informed, business-driven risk management decisions.



Key Capabilities

- Integrate and converge Falcon data with your other datasets to deduplicate cyber asset data sources
- Enrich and visualize security and device data with network and business context
- Enable effective communication of complex security subjects to non-technical stakeholders through effective reporting



About appNovi

appNovi is a cybersecurity mesh architecture platform that integrates with your existing network and security services. appNovi customers mesh and visualize their data to gain total asset visibility, identify security control coverage gaps, and enforce security policies using their existing tools.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.



Gain total asset visibility

©2023 appNovi