SOLUTION BRIEF

Advance Your Attack Surface Management

Achieve strategic risk management through contextual analysis

Your assets are everywhere. So are your tools. appNovi seamlessly integrates with your existing security stack, efficiently transforming raw data from multiple sources into actionable intelligence in a centralized place. Our Cyber Asset Attack Surface Management solution offers unparalleled asset discovery and contextual analysis to provide security teams with an authoritative source of security data. Understanding your assets and their interconnectedness within the enterprise network enhances operational efficiency, minimizes incident resolution time, and optimizes resource allocation by providing a clearer view of network exposure and asset vulnerabilities.

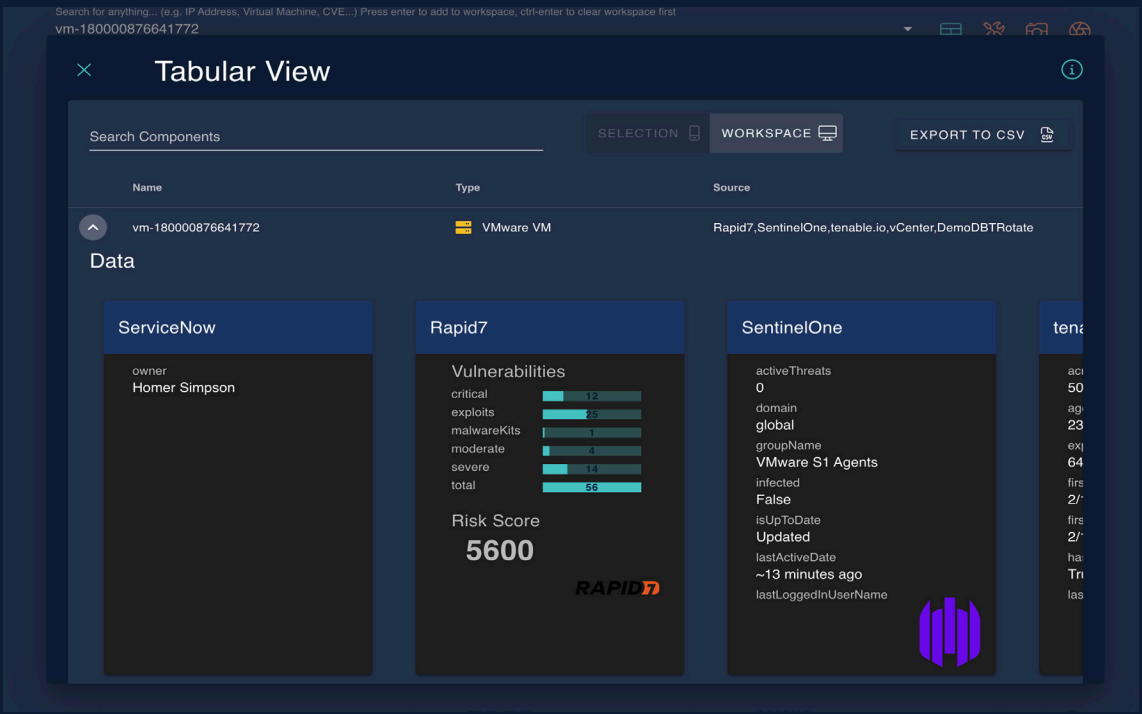
The Challenge

Cybersecurity teams have a responsibility to defend the network from attacks and identify and respond to incidents to resolve threats. Compelled by security alerts from different security tools, security analysts must gather all of the appropriate data to make informed decisions. However the effort to find, manually aggregate, and review data from your network and security tool data lakes obligates an incredible amount of time of each analyst. Without effective contextual correlation across datasets (and data lakes), the trustworthiness of data is low, security analysts' efficacy is heavily impeded, prioritization isn't specific to the business, and the resolution of security incidents is often partial or unable to complete due to uncertainty.

The result for large complex networks is inefficiency and ineffectiveness of remediation of risk.

SOLUTION BRIEF

Why appNovi



appNovi excels at identifying your attack surface and assets, while effectively mapping their connectivity within the network.

You've already invested time and effort in your existing security stack – appNovi connects them all without agents or scanners. Our data convergence provides a comprehensive asset inventory, delivers actionable insights in minutes, and enables security policy enforcement.

Data-enriched attack surface mapping enables enterprise-wide risk detection, and vulnerability prioritization based on business impact, while data accessibility ensures efficient non-disruptive incident response. appNovi's intuitive platform makes security accessible across all levels of experience by abstracting security specializations.

Key Outcomes:

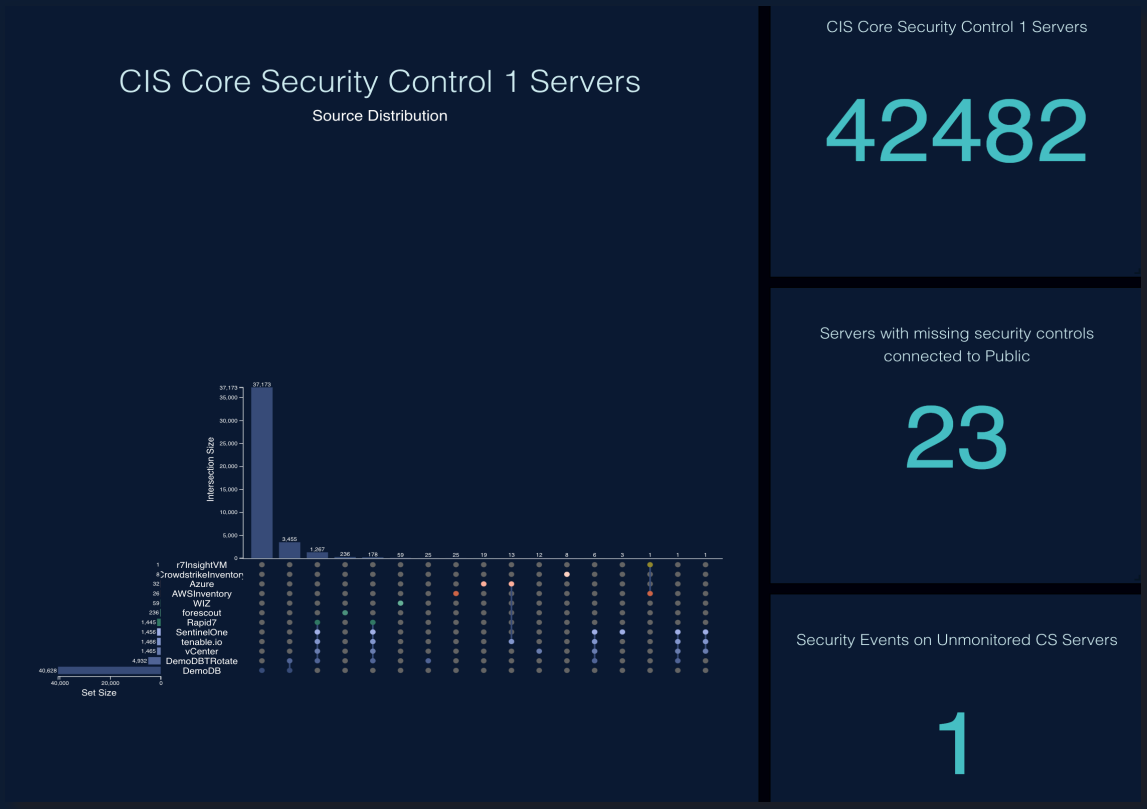
- Maintained asset inventories
- Security control verification
- Context-based vulnerability prioritization
- Security policy enforcement
- Attack surface reduction

Benefits:

- Simplified access to data
- Assurance of endpoint agent coverage
- Continuous compliance assessments
- Reduced costs

SOLUTION BRIEF

Attack Surface Identification and Mapping

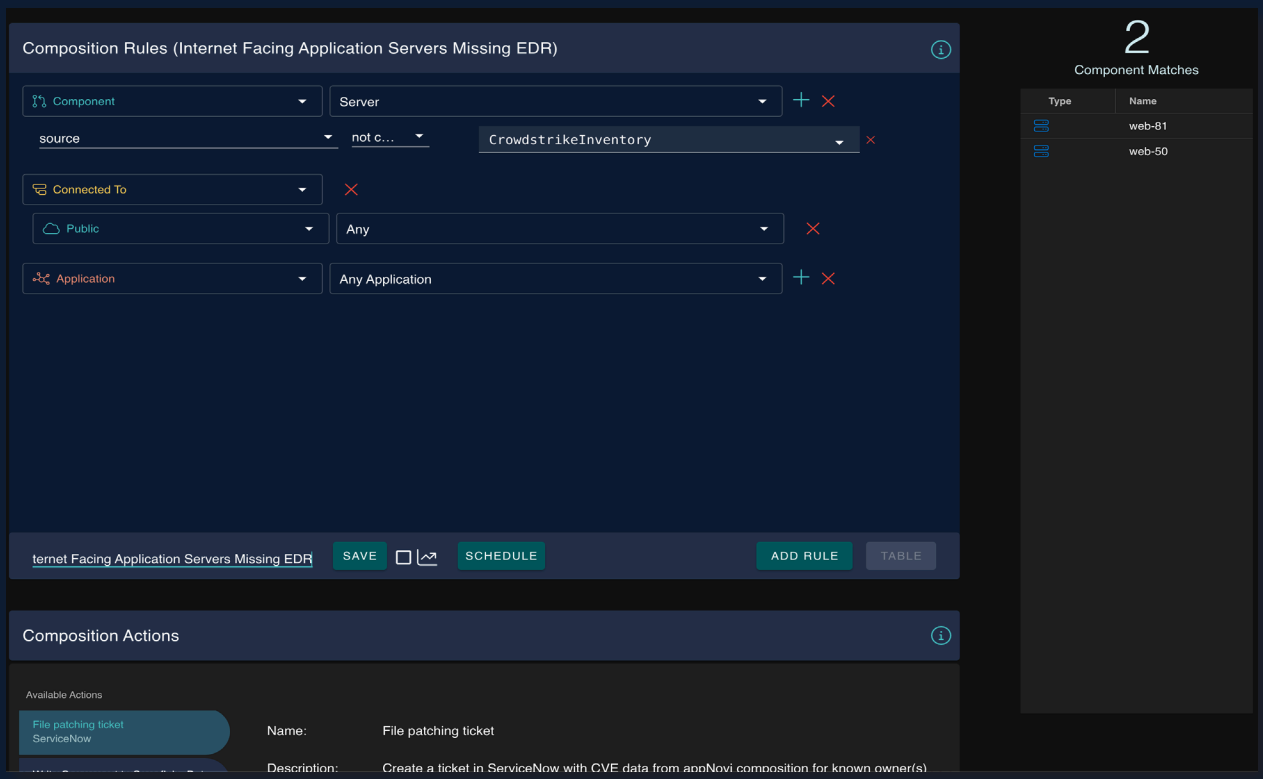


appNovi's innovative approach to Cyber Asset Attack Surface Management provides a comprehensive model for attack surface discovery, mapping, and reduction. It integrates network, asset, user, vulnerability, and security alerts to offer a clear understanding of threats, and business impacts, to deliver a source of truth to security and stakeholders for effective decision-making.

Networks consist of different environments with different tools and teams monitoring them – appNovi integrates all of them to provide a unified view of your environment by mapping it from the inside out.

SOLUTION BRIEF

Vulnerability Management

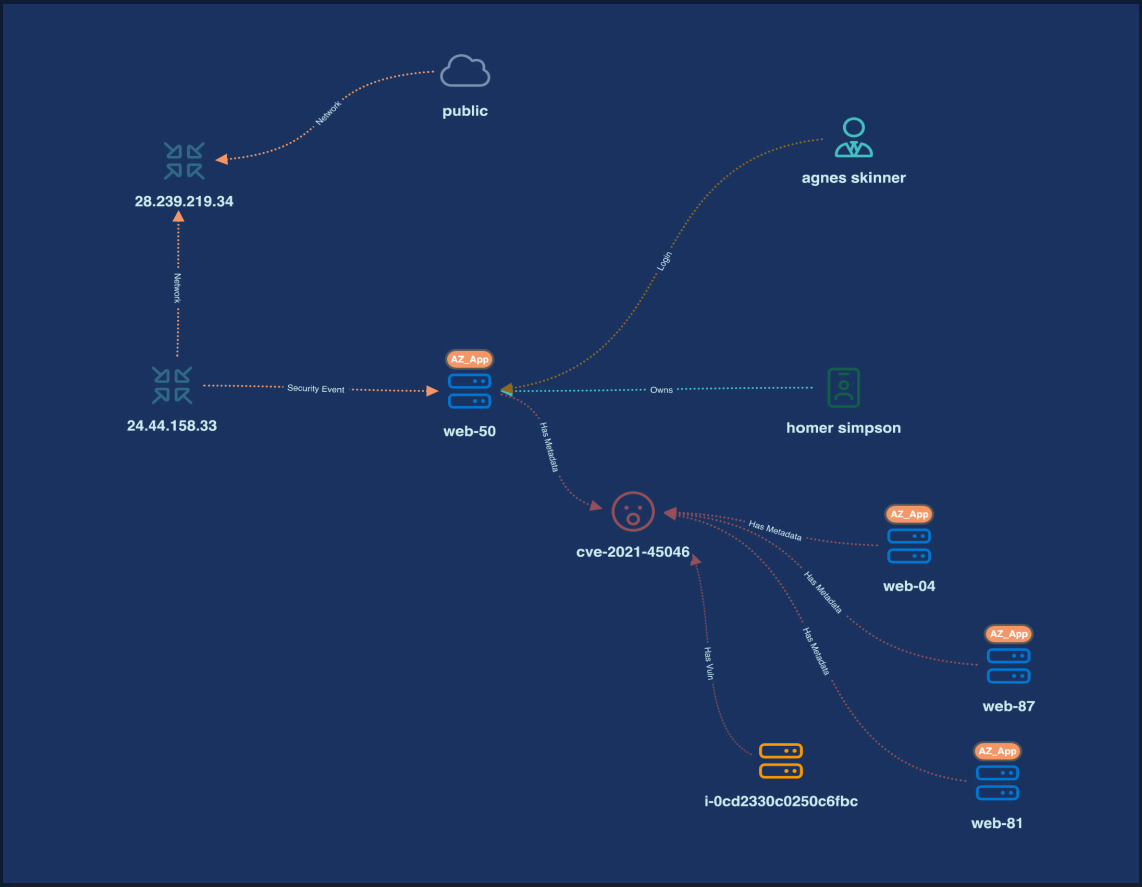


appNovi's holistic view allows organizations to prioritize security measures based on actual risk, rather than just on siloed perspectives of assets.

The authortiative source of data enables a more strategic approach to cybersecurity, focusing on the most critical vulnerabilities and potential attack paths, which is essential for effective risk management and incident response. appNovi correlates users to assets to improve remediation coordination and reduce escalations or wait times.

SOLUTION BRIEF

Incident Response



appNovi provides an immediate understanding of an attack's blast radius and insights for actionable strategies to mitigate risk. This approach streamlines analysis, enhances mitigation and remediation understanding, and drives efficient resolution of security incidents. When an alert warrants investigation, security teams can interrogate and explore their data. It's as simple as specifying a point in time – appNovi visually renders the steps taken by an adversary to reduce analysis and ensure clear communication and support collaboration.

SOLUTION BRIEF

appNovi Technology Partners

Integrate the security stack to gain a holistic picture of your security

appNovi integrates the existing security stack to provide a complete and authoritiative source of data. Security teams use appNovi to automatically maintain cyber asset inventories including infrastructure, devices, users, applications, code, and more. The converged data set enables security agent gap analysis, vulnerability priortization, and optimized incident response.