JOINT SOLUTION BRIEF

Tenable and appNovi

The integration between appNovi and Tenable provides a solution to visualize the contextual exposure of vulnerabilities and analyze the impact on business-critical applications

Every organization must identify business risk and prioritize security response for effective resolution. Legacy vulnerability scanning solutions identify network assets and their vulnerabilities, but without business context, scan results inundate security teams. Through simple, smart, and scalable integrations, appNovi empowers Tenable.io and Tenable.sc customers to visually understand contextual exposure of vulnerabilities and their impact on business-critical applications for the enablement of an effective vulnerability management plan.

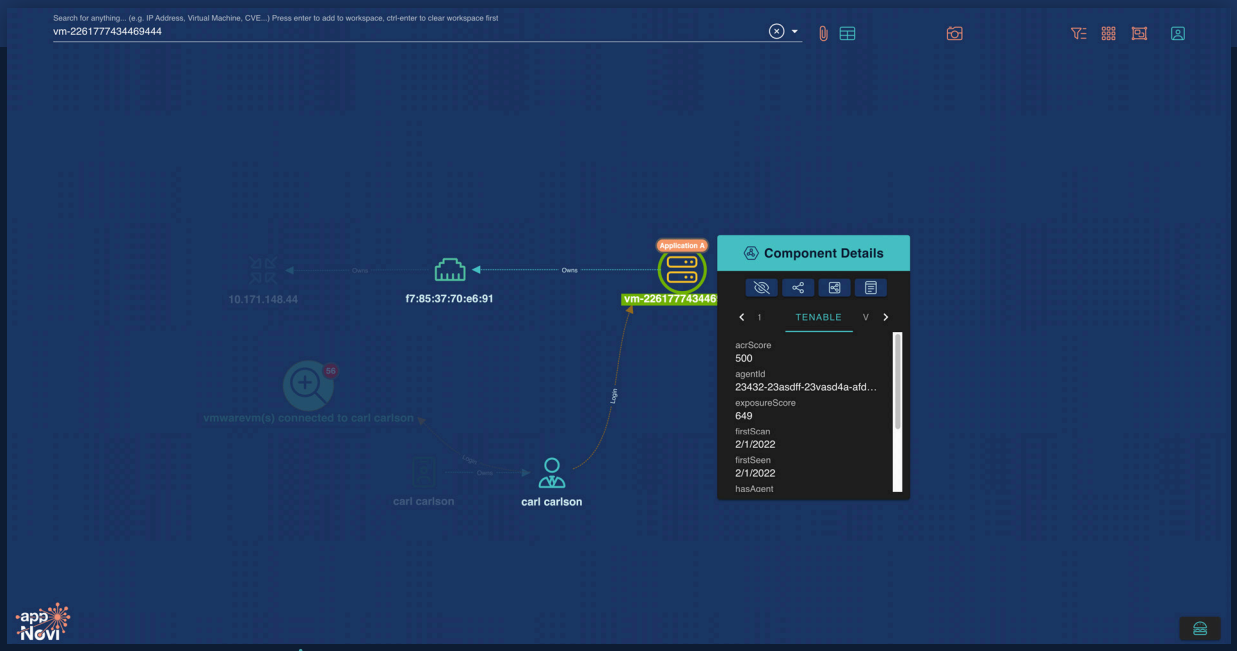
The Challenge

Vulnerability scan and/or correlation results often overwhelm teams by volume alone. Security analysts then manually correlate logs and CMDB data to assess vulnerable assets' business importance and exposure. This tedious process results in prolonged and ineffective risk reduction efforts exacerbated by new vulnerability disclosures and consequent investigations every week.

Without the effective correlation of network, business, and vulnerability data, all vulnerabilities are treated equally which results in wasted efforts, uncertain business-risk reduction, ineffective patch prioritization, and an immeasurable attack surface.

JOINT SOLUTION BRIEF

appNovi and Tenable



The Solution

The appNovi solution converges Tenable vulnerability data with application component data through a contextual correlation with network flows. The visualization of cybersecurity, network, and business application data is presented in an intuitive interface understandable by technical and non-technical stakeholders. The visualization and analytics of security data enables the streamlined prioritization of vulnerabilities based on business impact to applications and critical infrastructure to empower cybersecurity teams to make informed decisions.

appNovi provides the differentiation between similar vulnerabilities across hundreds of assets to identify and prioritize the most critical incidents for resolution to reduce the most amount of risk to the business.

Joint Benefits

appNovi provides the ability to aggregate and visually display your data lakes for consumption across multiple teams and business stakeholders.

appNovi integrates with Tenable.io and Tenable.sc to empower your team to:

- Understand exploitable vulnerabilities across your network
- Prioritize response based on asset relevance to critical applications
- Communicate technical risk to non-technical stakeholders through visualized threats
- Construct and maintain business-specific risk perspectives
- Respond effectively to newly disclosed vulnerabilities

About Tenable

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

About appNovi

appNovi provides a Cybersecurity Mesh Architetcure (CSMA) platform for security visualization and analytics. appNovi integrates with your existing network and security solutions for security control gap idenitfication, effective attack surface mapping, vulnerability prioritization, and incident response.