SOLUTION BRIEF

Maximize Security Controls and Agent Coverage

Validate that security and management agents are deployed and functioning across endpoints as they should be, identify coverage gaps, and control your attack surface

According to an industry report, 2% of agents fail per week, and **42% of endpoints are unprotected** in some manner at any given time[1]. **This leads to a lack of confidence in security control coverage and compliance with standards such as CIS, NIST, ISO 27001, PCI-DSS, HIPAA and SOC 2.**

COVERAGE GAPS

Malfunctioning Agents
28% of endpoints are unprotected due to broken or outdated agents[1]

Missing Agents
12% of endpoints remain unprotected by endpoint protection agents[2]

Misconfigured Agents
19% of agents require at least one repair within 30 days[3]

As traditional network perimeters give way to hybrid-work and cloud-based models, you rely heavily on a suite of agents for endpoint protection (EPP), endpoint and mobile device management (UEM/MDM), encryption, vulnerability assessment (VA), data loss prevention (DLP), zero trust network access (ZTNA), threat response and more.

But agents only provide visibility and control where they are correctly deployed and functioning. Coverage gaps occur when agents:

- Are not deployed on all endpoints
- Aren't running correct versions
- Don't have the latest security updates
- Aren't correctly configured
- Haven't communicated back to their management consoles

Agent-based management consoles are not good at showing you gaps in coverage. With 10 or more security agents[2] installed on every endpoint, manually consolidating and correlating data scattered across multiple siloed systems to compile accurate agent coverage is arduous, resource-intensive and error-prone.

Challenges

- Lack of confidence in policy vs. reality of endpoint security and compliance controls
- FTE time spent exporting data from many siloed systems and correlating manually
- Friction between security & IT teams due to lack of or inaccurate endpoint compliance reporting

Benefits

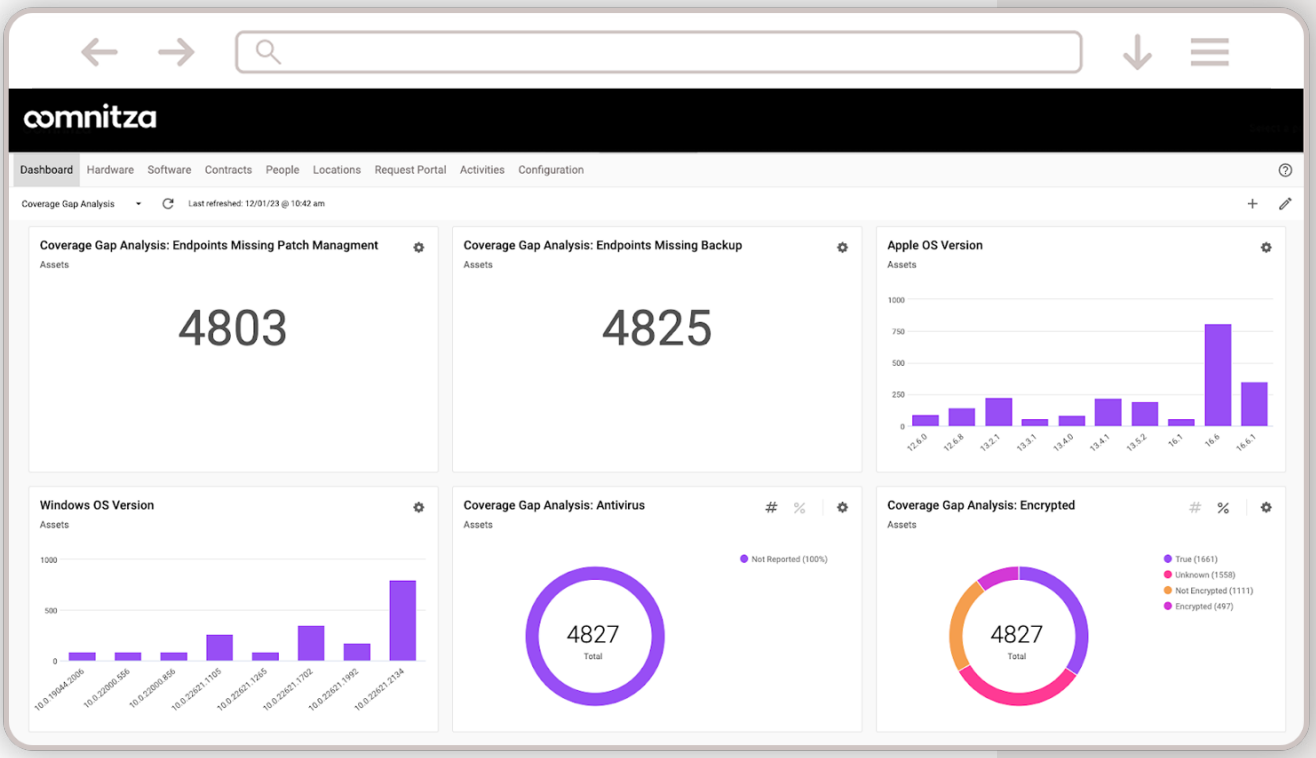
- Single system for automated endpoint coverage gap identification/reporting
- Confidence in endpoint compliance policies and controls being met
- Reduction in security exposures and attack surface
- FTE cost savings by eliminating manual efforts to support audit processes
- Improved alignment and collaboration between security and IT teams

Identify whether or not your agents are present and performing

Oomnitza integrates with all your IT and security tools, automatically aggregates and correlates data from these systems, and gives you insight into where agents are deployed, missing or malfunctioning.

You can monitor, report and automate actions to ensure agent coverage and health with Oomnitza:

- Visibility into assets whether or not an agent is present and functioning
- Integration of data from your management and security tools such as UEM/MDM, EPP, VA into one single source of truth
- Continuous monitoring of endpoint coverage and agent health
- Reporting on endpoint security posture for compliance policies & standards such as CIS, NIST, ISO 27001, PCI-DSS, HIPAA & SOC 2.
- Automated workflows to take action to fix security exposures and compliance gaps



"Oomnitza serves as a gatekeeper to make sure that the suite of security agents that we want deployed across our environment are actually deployed and running correctly. It stitches together all of the different security tools that we have on our endpoints."

Nemi George
VP, Information Security Officer & IT Operations
Pacific Dental Services

Learn more at
www.oomnitza.com

oomnitza

1 One hundred percent of endpoint security tools eventually fail (Global Endpoint Security Trends Report)
2 The Forrester Wave™: Endpoint Security, Q4 2023
3 Endpoints At-Risk: Too Many Security Tools are the Cause