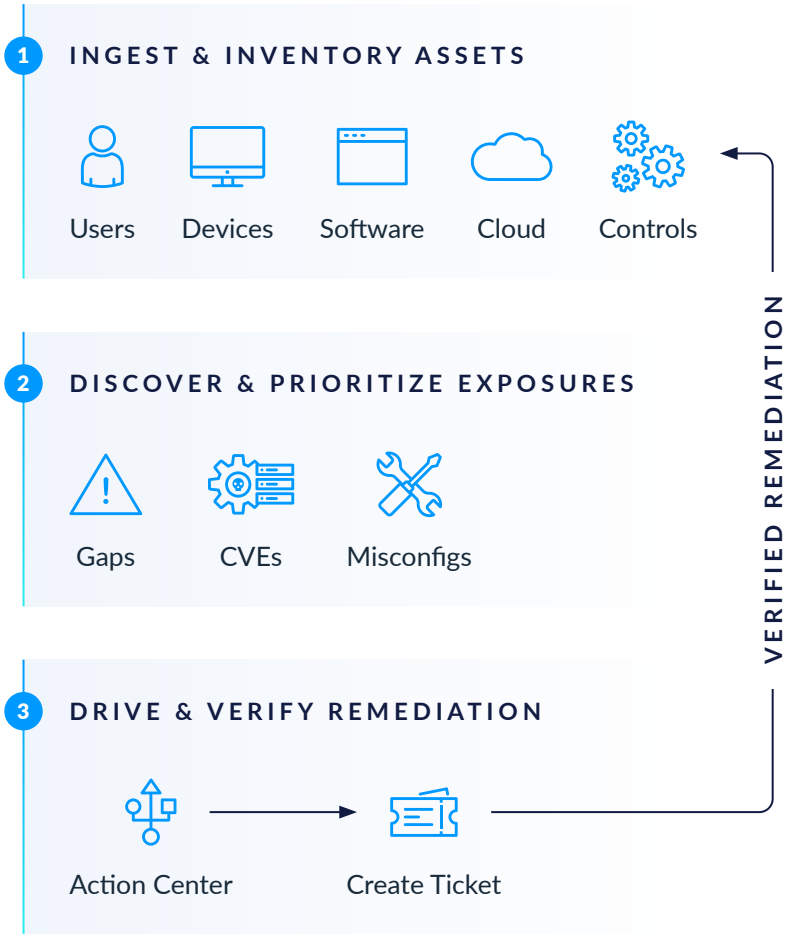
DATASHEET

# Aurora® Attack Surface Management

## Gain a More Complete View of Risk

Most organizations still lack a complete, current view of the assets, controls, and exposures across their environment. Aurora Attack Surface Management helps security teams close those gaps by continuously discovering assets, identifying missing or stale controls, prioritizing risk with business and threat context, and verifying remediation progress across internal, external, cloud, and end-user environments.

### Continuous Monitoring of the Entire Exposure Lifecycle




### Better Data

Unify asset, control, and exposure data from across the environment to create a more complete and current foundation for security decisions.

### Better Decisions

Prioritize what matters most with business and threat context, so teams can focus on the exposures that create the greatest risk.

### Better Outcomes

Track remediation progress and verify that risk reduction actually occurred, not just that a ticket was closed.

### Built to Connect

Integrates with solutions across the Arctic Wolf portfolio as well as the broader IT and cybersecurity ecosystem, helping you unify visibility without the need to rip-and-replace.

## Core Use Cases

### Complete Asset Inventory

- Aggregate, correlate, and deduplicate asset data in real time across your existing environment
- Build a continuously updated view of devices, users, software, applications, and cloud resources to reduce blind spots

### Remediation Tracking and Verification

- Streamline remediation with automated actions, workflows, and resolution tracking
- Verify that risk reduction actually occurred and measure progress over time with dashboards and reports

### Security Control Coverage Monitoring

- Monitor the presence and state of security controls across the environment
- Identify missing or stale controls and validate deployment, scan coverage, and compliance coverage

### Risk-Based Exposure Prioritization

- Unify vulnerabilities, misconfigurations, security gaps, and cloud findings in one view of attack surface risk
- Correlate exposures with threat intelligence and business context to focus on what matters most

## Turn Visibility Into Measurable Risk Reduction

Most security teams are still making decisions on top of incomplete or stale asset data. Aurora Attack Surface Management gives them a stronger foundation by unifying asset, control, and exposure intelligence from across the environment. This helps teams uncover what traditional scanning alone can miss, prioritize exposures with greater confidence, and verify whether remediation was successful. The result is a more credible path to reducing attack surface risk and a practical step toward broader exposure management.

1. **Severity:** Based on risk to the environment
2. **Open:** Number of assets impacted by vulnerability needing action
3. **Total:** Total number of assets impacted by vulnerability including those that are snoozed or accepted as risky
4. **7-day change:** Increase or decrease in the number of assets based on remediation effectiveness + new findings
5. **Avg age & compliance:** Avg number of days assets have been associated w/ vulnerability and impacted assets within or outside SLA


6. Status detail of impacted assets
7. View, add, or change actions like automated remediation workflow
8. Additional vulnerability description and details including observation, impact, and recommendations



AW_DS_AASM_0426