# **Secure Baseline**

With the Secure Baseline scanning capability, you can compare your Operating Systems’ (Linux, Windows, Mac) existing configuration settings against established security frameworks like the CIS Benchmarks and DISA STIGs. Find security gaps and misconfigurations, and strengthen configuration based on scan results. Check for deviation from a secure state (configuration drift) by scheduling regular scans.

## **Secure Baseline Dashboard**

The Secure Baseline Scan dashboard provides an overview of how your previous or current baseline scans have performed or are performing. Through this, you can determine how vulnerable your instance is based on Operating System (OS) configuration settings and group policy practice.

The risk grades give you an easy way to compare previous and current risk levels based on scan results. Use the Secure Baseline Trend chart to see performance in secure configuration and policy management over time.



## **Discover Machines with the Lowest Scores to Prioritize Remediation**

Get a quick view of the top 10 machines that have the lowest pass scores to plan remediation and prioritize action items.



## **Secure Baseline History**

Any existing Secure Baseline scans that have either been completed or canceled are shown within the secure baseline scan history. You can see the number of completed baseline scans, overall failure rate, and a list of a scans with an overview of each scan result. Create mitigation plans starting with the lowest pass scores to comply with established security standards.

