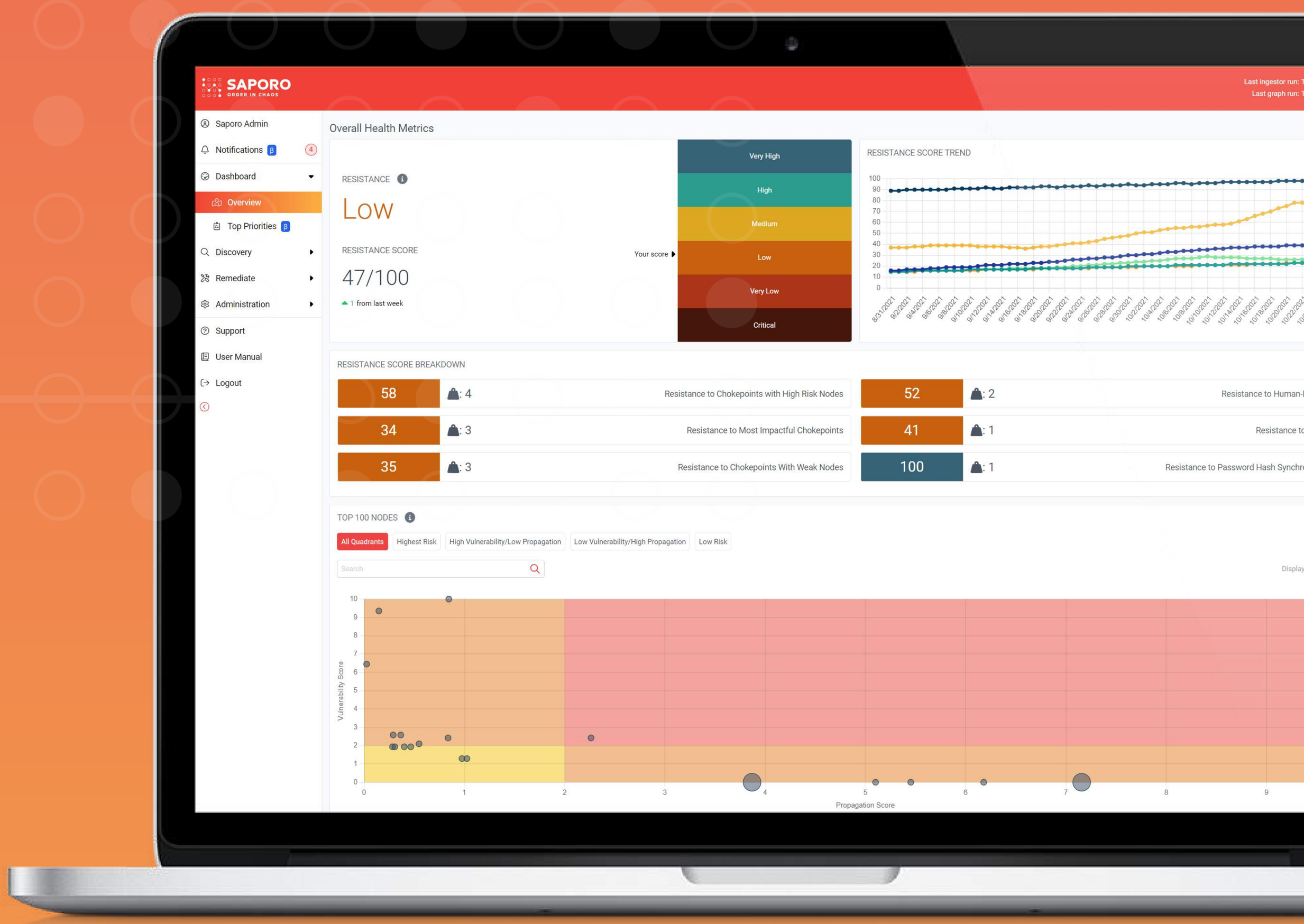
SAPORO
ORDER IN CHAOS

Discover your security gaps with

Identity attack path assessment



www.saporo.io

What is an identity attack path assessment

Saporo's extensive **identity attack path assessment** spans over a period of **three working days**, encompassing **two distinct sessions**: one dedicated to installation and another focused on reviewing the results.

What to expect from our basic offering:

Resistance score is provided that indicates how difficult it would be for an attacker to access critical assets in the xontext of your environment.

The **top 10 chokepoints**, or optimal locations to block the largest number of identity attack paths, to help you identify what is most critical and allocate resources efficiently.

The **top 50 dangerous assets** that have the potential to propagate attacks faster and easier than others, combining both high vulnerability and high propagability factors.

Actionable assessment report containing the **most important findings** and **our recommendations** for improving your security posture.

Our basic offering provides data exclusively from Active Directory and includes one attack model. However, for Azure users and a broader range of simulation models, we offer expanded options with customized pricing. For further details and inquiries, please don't hesitate to reach out to us at hello@saporo.io.

Why identity attack path assessment

An identity attack path assessment with Saporo can significantly reduce your internal attack surface by uncovering the most critical issues that other tools and services would most likely miss. Our innovative technology provides a comprehensive assessment to ensure the security of your valuable assets.

Risk Management
Assess your current risk level and establish your risk threshold in a different way. Saporo assessment surpasses the conventional approach of providing a simple list of security issues. Instead, it emphasizes the risks that would have the biggest impact on your specific environment, empowering you to make informed decisions regarding security measures.

Risk-aware transformation
Considering moving your IT infrastructure to the cloud? Protect your valuable assets and ensure a seamless transition by testing your resistance to potential security risks. Saporo helps you identify any misconfigurations that could threaten your cloud security posture.

Are you running regular pentests?
While pentests are great to test your ability to detect and respond to threats, they are narrow in scope. With this assessment, you can get a extensive picture of your identity related risks across millions of identity attack paths and hundreds of common configuration issues, which you can fix at once.

It’s simple and easy to start

Investing a small amount of time into your security now can dramatically reduce your attack surface and risk while saving you a significant amount of resources in the event of an attack.

We understand this. That is why we made Saporo fast and scalable.

- ☑ **Installation is done in a matter of minutes**
- ☑ **Our solution is agentless and only requires one read-only user**

Get all the perks with

Continuous Attack Surface Management

Don’t miss out on the full picture with Saporo up and running 24/7 and providing daily information about the impact of identity configurations! In addition to having all the assessment perks, our full subscription also offers:

IMPACT ANALYSIS

Adopt security-by-design principles by safely simulating changes before they’re implemented in a production environment.

LOGS

You can now get context for alerts from other systems with real-time monitoring of activity within supported directories.

INTEGRATIONS

Integrate your solution with Saporo using our open API or build a custom integration according to your needs.

ACCESS TO ALL MODELS

Tap into all of our models such as ransomware, chokepoints for DCSync attacks, chokepoints with high-risk nodes and many more.

ALL DATA SOURCES

Data ingestion and analysis from prominent sources such as Active Directory, Azure, AWS, and Okta, with more coming soon.

SUPPORTED DATA SOURCES

Microsoft Active Directory

Azure

amazon web services

okta

kubernetes (Coming soon)

GitHub (Coming soon)

Google Cloud (Coming soon)

salesforce (Coming soon)