# Risk Fabric eliminates clutter and noise, sending only prioritized and actionable findings to GRC

The Security Risk Management Challenge

GRC programs are increasingly becoming enterprise mainstays that are meant to increase the efficiency of audit, compliance, risk, and security processes. Increasingly, new security risk management processes that require large amounts of data are overwhelming traditional GRC systems. The challenge for any GRC program is to eliminate the noise, and feed only the relevant and actionable information into the GRC system.

As a domain of GRC, security risk management is no exception to the problem of too many systems and too much data. Vulnerability, configuration check, scan and pen test results, along with security tools such as data loss prevention, end point protection, and SIEM collectively produce tens of millions of rows of data. The problem becomes even more complex when enterprises try tying it all together to report on and maintain compliance with regulatory standards and manage third party vendor risk.
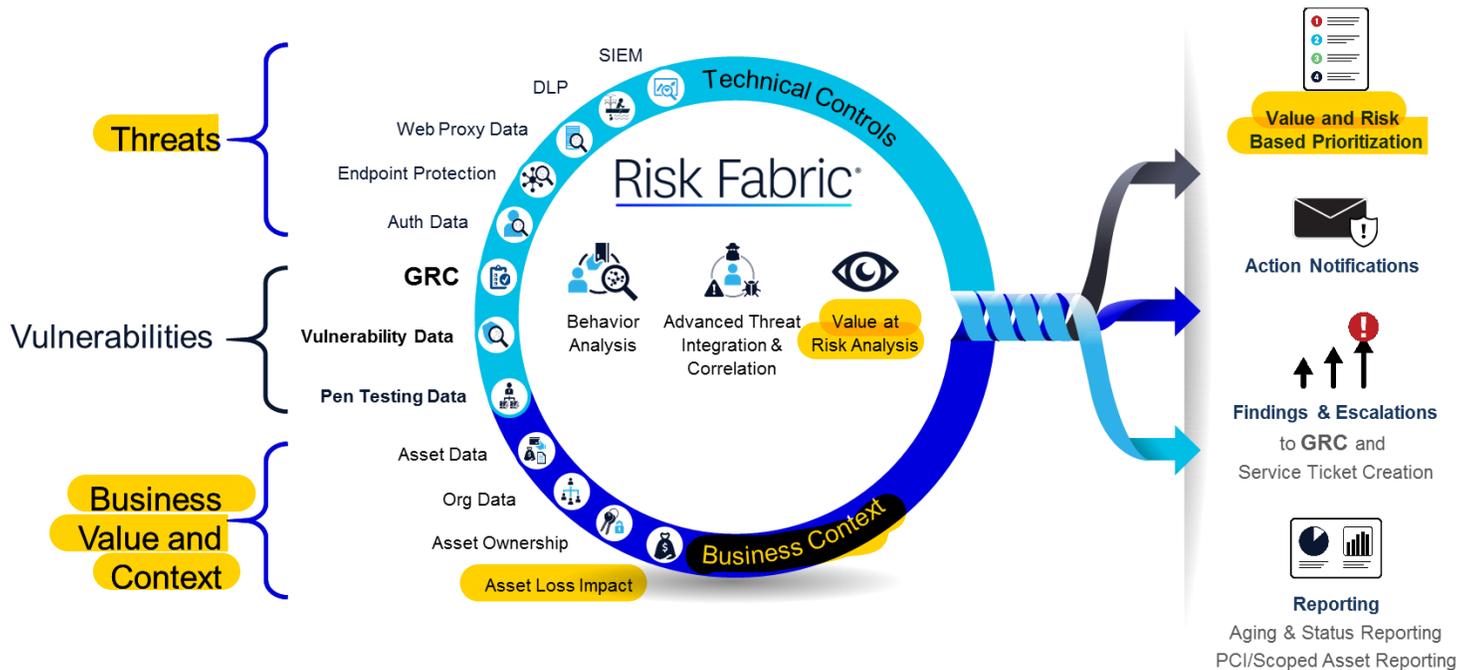
Making the Most of GRC

The automation and integration provided by Risk Fabric® gives enterprises comprehensive cyber risk analytics while enhancing and optimizing the capabilities of GRC. The platform correlates large data sets from vulnerability and configuration scans with hosts, applications and asset owners, as well as additional threat context from security tools such as data loss prevention, SIEM, and end point protection. Using proprietary analytics, the platform then presents high quality lists of vulnerabilities, prioritized in the context of asset risk and value. Risk Fabric's bi-directional interface can automatically create findings in the GRC tool or they can be actioned in the response portal for security staff to track remediation, create exceptions, and manage false positives.

Reducing the footprint of GRC findings to those that have already been vetted and prioritized, minimizes noise and enhances the ability to remediate the most important issues. Additionally, dashboard integration and attestation management optimize the satisfaction of risk and compliance requirements.