Tenable / Qualys vs. Cronus

Tenable and Qualys are market leaders. Both cover continuous security, however their claim to fame is vulnerability management. Each try to bring extra insights and context to their findings to avoid a long list.

1. Neither Qualys nor Tenable have business insights on how their vulnerabilities correlate with the client's business processes. Cronus can filter and focus on vulnerabilities that threaten business processes
2. Neither Qualys nor Tenable can correlate how a hacker could use the vulnerabilities present on the client's network / web for lateral movement within the organization to reach critical assets. Cronus has built and patented its Attack Path Scenarios (APS)™ Technology that shows exactly that on a live map, 24/7.
3. Qualys is strong in cloud / web app security, Nessus is strong in infra vulnerability scanning and advanced analytics. Cronus has created "Infra-Web" technology that combines both web and infra to provide insights on hybrid attacks that start on the web and end in the DC.
4. Global scanning – Cronus can scan global network and showcase global attack path scenarios for global actionable insights between networks / sites.
5. Ease of use – Cronus is very easy to install and use, Qualys can be harder to use due to the complexity of the solution suite. Tenable is somewhere in the middle.

Criteria	Tenable (Nessus)	Qualys	Cronus CyBot
Continuous scanning	Yes	Yes	Yes
Web / App	No	Yes	Yes
Infra scanning	Yes	No	Yes
Attack Path Scenarios (Automated Penetration Testing)	No	No	Yes
Business Scenarios	No	No	Yes
Easy to use for IT management	Yes	Yes	Yes
Asset Management	Yes	Yes	Yes
Customizable reporting and dashboards	Yes	Yes	Yes
Continuous Security Monitoring (anomaly detection)	Yes	Yes	No
Global insights	No	No	Yes