Vulnerability Risk Score

Most organizations have many more vulnerabilities than they can patch. Vulnerability risk scores are used to prioritize these vulnerabilities so you can make intelligent decisions about which vulnerabilities to patch first.

Vulnerability risk scoring uses the following terms:

- **Entity Criticality Factor** – Portion of the Vulnerability Risk Score formula that represents the relative importance of an entity. It is derived from the entity's Business Criticality value.
- **Enhanced Risk Score** – A calculation of a risk factor that indicates the relative likelihood of a vulnerability to be exploited.
- **Vulnerability Definition Risk Score** – The sum of the risk scores of all of the instances of the vulnerability.
- **Vulnerability Risk Factor** – A value that is used in the Vulnerability Instance Risk Score equation that indicates the relative likelihood of a vulnerability being exploited.
- **Risk Reduction %** – The sum of the risk reduction percentage points of each vulnerability compensating control attached to the vulnerability. If the vulnerability has an approved exception, this value equals 0.
- **Vulnerability Instance Risk Score** – The risk a vulnerability instance, which is a vulnerability on an entity, poses to an organization. It comprises both an element of the importance of an entity and another element of the likelihood that the vulnerability will be exploited on that entity. This risk score uses the following formula:

```
Vulnerability Instance Risk Score = (Entity Criticality Factor * Vulnerability Risk Factor) * (1 -
                                    Risk Reduction %)
```