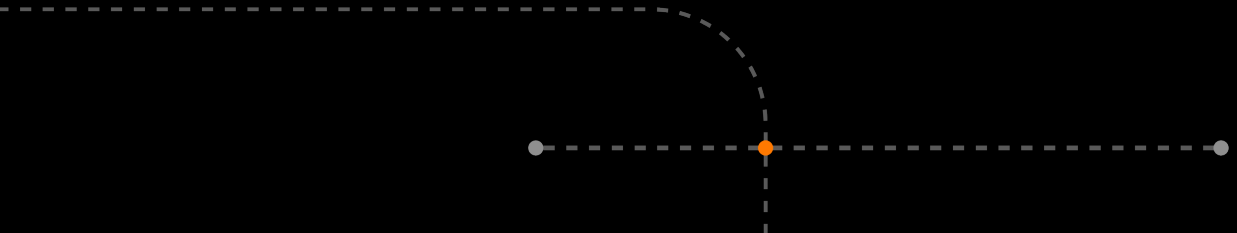
Orange
Cyberdefense

Risk-Based Vulnerability Management

Prioritizing remediation to reduce your attack surface



orange™

The attack surface continues to grow and diversify…

+23 000
vulnerabilities in 2022
including 17 000 critical*
* National Institute of Standards and Technology

80% **are patched in +30 days***
* Security Navigator 2023

…It's impossible to patch everything!

Challenge

Always more vulnerabilities, lack of visibility and guidance to conduct an effective vulnerability management program.

How to…

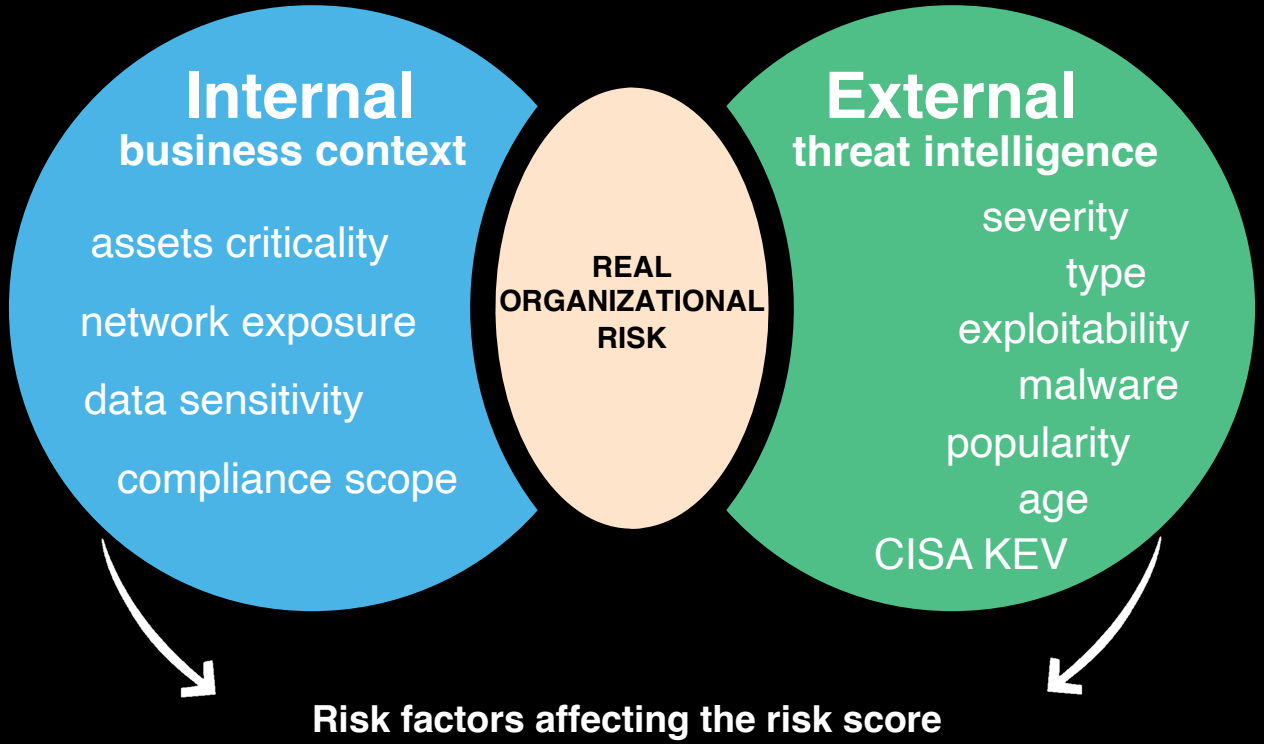
- Have a better visibility on your assets and so on your attack surface?
- Ensure that the scan data is accurate and well managed to avoid being overwhelmed?
- Ensure that the information is contextualized for an effective vulnerability management programme?
- Address the prioritization and remediation challenged using a risk-based approach?

What is risk-based vulnerability management?

> *Don’t try to patch everything; focus on vulnerabilities that are actually exploitable. Go beyond a bulk assessment of threats and use threat intelligence, attacker activity and internal asset criticality to provide a better view of real organizational risk.*

www.gartner.com

Business context and threat intelligence correlated to focus on the real organizational risk



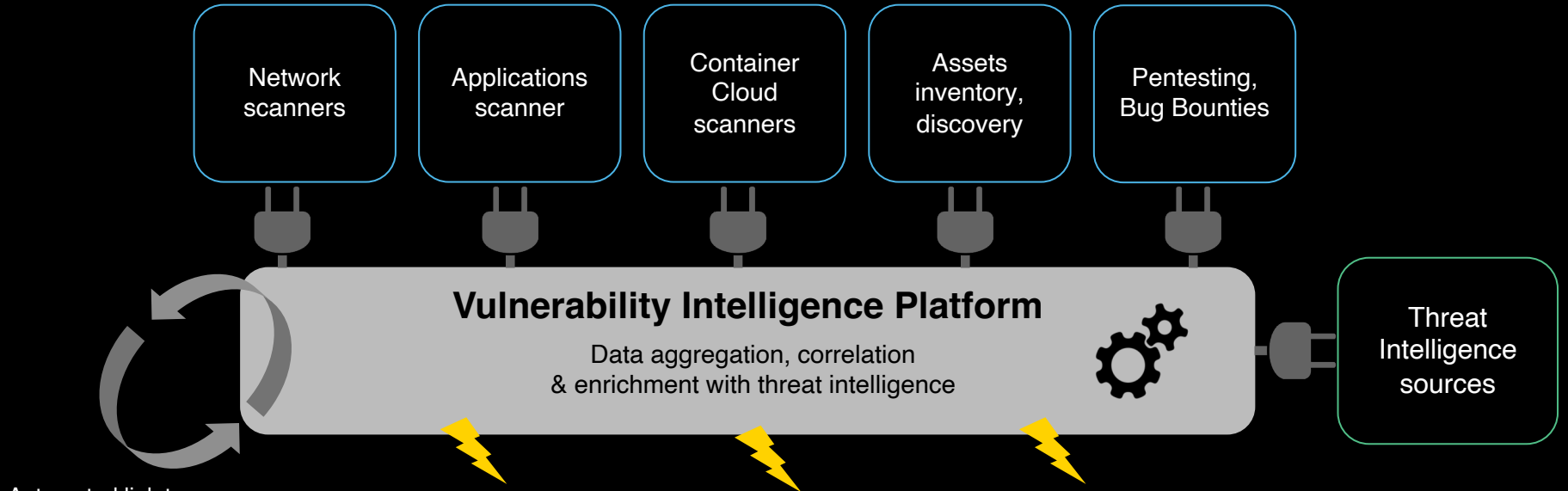
How to embrace a risk-based vulnerability management?

Adopt a risk-based approach for vulnerability management

to reduce the attack surface and become a harder target for threat actors

Risk-Based Vulnerability Management

All vulnerability related data consolidated in the Vulnerability Intelligence Platform



Risk Scoring
Leveraging advanced technology and real-world data that serves as a compass for all risk operations

Risk Prioritization
Prioritizing by correlating the threat landscape as well as your environment and business context

Consolidated view
Customized dashboard and reports with actionable measurements that guide remediation efforts

Orange Restricted

Orange Cyberdefense

Orange Restricted