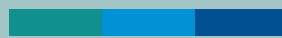.ray*NET*

// Vulnerability Monitoring

Protect your business from vulnerabilities & improve your long-term IT security

Are your business-critical resources at risk?

Despite the increasing sophistication of cybersecurity tools, cyberattacks are increasing both in number and severity, and they are getting faster. The growing complexity of IT infrastructures along with the centrality of digital solutions in almost every aspect of our work leave enough room for gaps, which bad actors can exploit to gain access to critical infrastructure.

In 2022, **17%** of all cyberattacks were executed by **ransomware**. The average duration of such an attack has reduced dramatically in recent years. Today, it takes less than 3.85 days from the publication of a vulnerability to an attempted cyberattack.

Are you able to respond that quickly and eliminate vulnerabilities in your business?

Average duration of ransomware attacks (in days)

60	
50	
40	
30	
20	
10	
0	

2019   2020   2021   2022
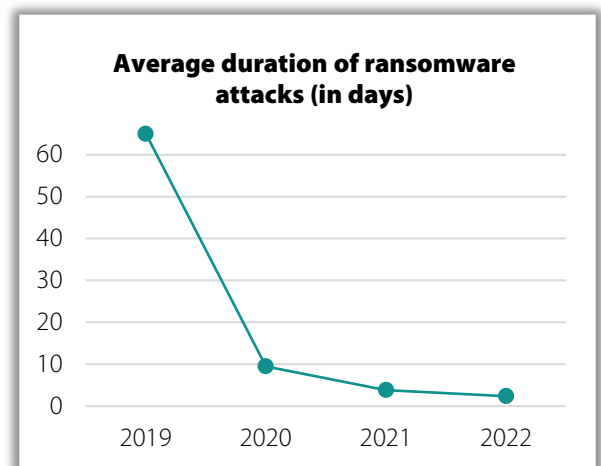
Source: IBM Threat Intelligence Report

Intelligent Vulnerability Monitoring for better IT security

If software is no longer supported and does not receive security updates, the user is the weakest link in the chain and the company is vulnerable to cyberattacks. IT managers therefore need a complete overview of their assets, including vulnerability information.

The **Unified Data Platform** delivers exactly this transparency and automatically enriches your asset information with essential market data from our **Technology Catalog**. The daily updated comparison with the NIST database provides you with classified vulnerability information in meaningful dashboards.

The intelligent scoring function enables you to take immediate action to eliminate vulnerabilities.
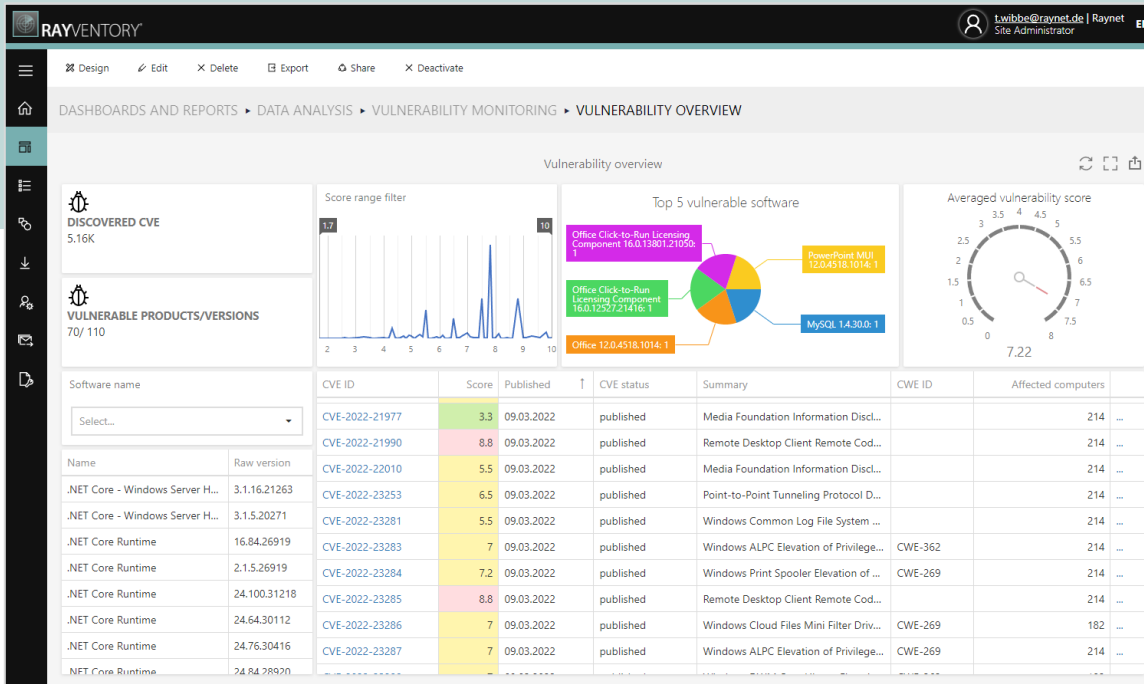
Your benefits

- Get a complete overview of your current vulnerabilities
- Improve your IT security by patching and updating applications with vulnerabilities
- 24/7 access to vulnerability information including criticality rating
- High level of reliability & security through automated vulnerability detection
- Minimize your support efforts with regular software updates
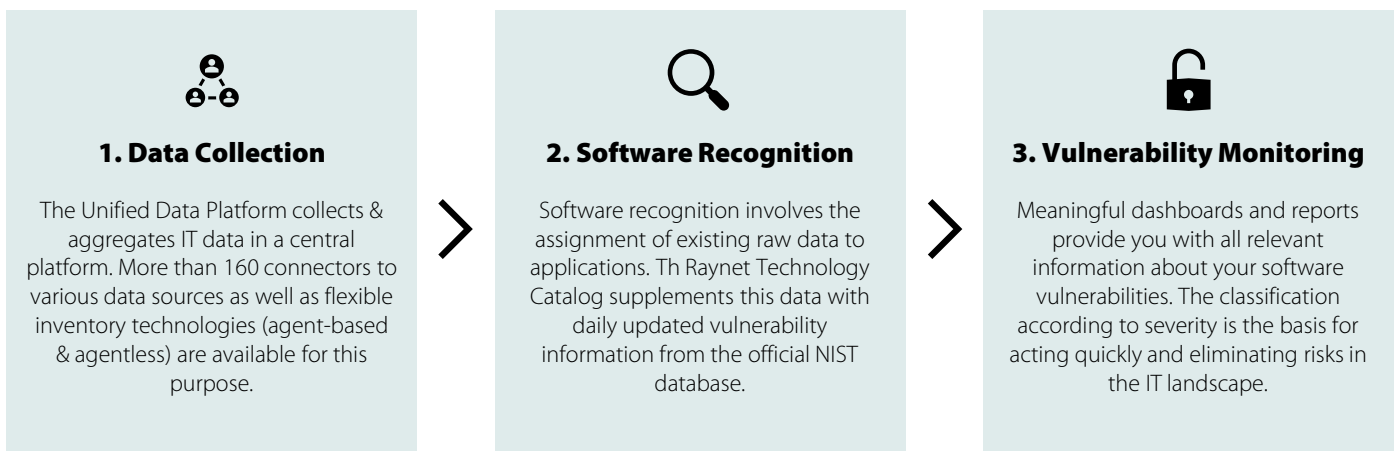
Discover to Manage

www.raynet.inc.com

Vulnerability Monitoring

Three steps for sustainable Vulnerability Monitoring

1. Data Collection

The Unified Data Platform collects & aggregates IT data in a central platform. More than 160 connectors to various data sources as well as flexible inventory technologies (agent-based & agentless) are available for this purpose.

2. Software Recognition

Software recognition involves the assignment of existing raw data to applications. Th Raynet Technology Catalog supplements this data with daily updated vulnerability information from the official NIST database.

3. Vulnerability Monitoring

Meaningful dashboards and reports provide you with all relevant information about your software vulnerabilities. The classification according to severity is the basis for acting quickly and eliminating risks in the IT landscape.

Why Raynet?

Because we offer you a quick way to map your entire IT landscape based on the highest data quality and help you to automatically classify critical vulnerabilities and increase your long-term IT security.

As a global software vendor with market-leading solutions and complementary managed services, we make successful end-to-end management of IT projects and operations possible.

Following the mission **Discover to Manage**, our vision is that all companies worldwide achieve transparency and security as well as optimization of their IT investments by using our technologies.

Get in touch

For more information, call our sales team at **+49 5251/54009-0** or write to them at **sales@raynet.de**.

Discover to Manage   **www.raynet.inc.com**