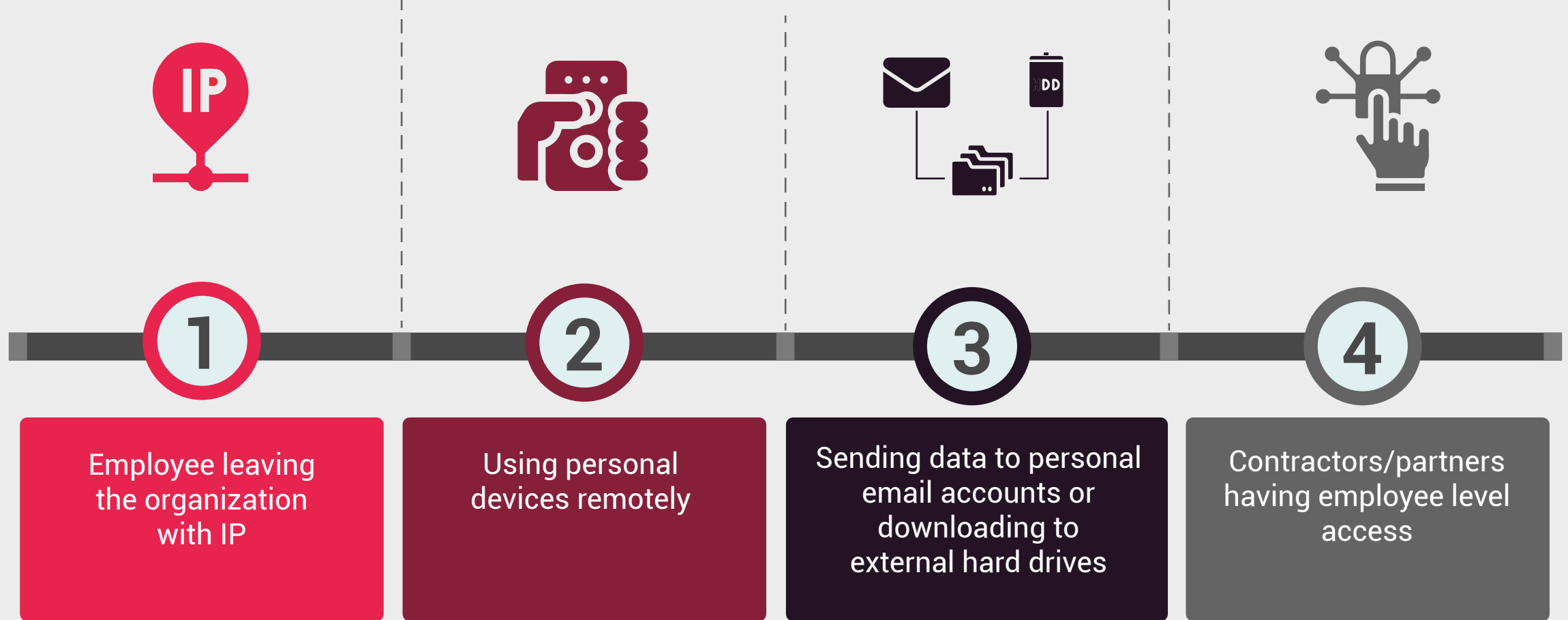


Insider Threat Protection

The Malicious Insider

Malicious insiders could be current or former employees or business associates with privileged access to sensitive data who misuse it maliciously for financial or personal incentives. This threat becomes more complex when the malicious insiders misuse the organization's sensitive data on the cloud because cloud data is often harder to track.

Scenarios



22% of the **times**, **Malicious insiders** are the reason for **security incidents** in a company

47% Increase in insider threats from 2018 to 2020

Source: TESSIAN

Healthcare and Finance



Industries facing most incidents involving employees **misusing privileges**

Source: TESSIAN



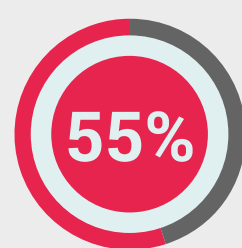
85% Organizations finding it challenging to determine the actual **damage** of an **insider attack**

Source: TECHJURY

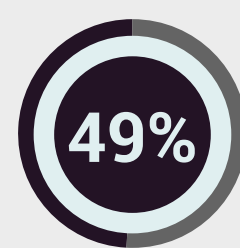


Major factors driving insider threats

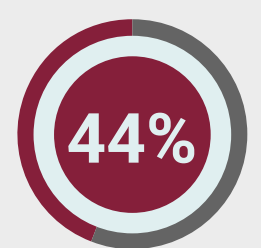
Source: TECHJURY



Fraud



Monetary gains



Intellectual Property theft



Departments **most vulnerable** to insider attacks

Source: TECHJURY

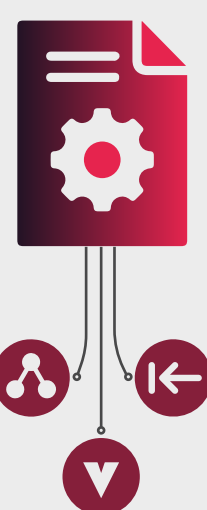
\$ 871,000 (per incident)
Cost of credential threats to an organization

Source: TECHJURY



\$755
Average cost of the incident due to criminal insider

Source: SWISSCYBERINSTITUTE



45% Employees **Download, Save, Send**, or otherwise **exfiltrate** work-related documents before leaving or after being dismissed from a job

Source: TESSIAN

Mitigate Insider Threats with a Solution That:

- Attaches persistent granular usage controls to documents and emails
- Tracks activities on a protected document in real-time
- Enables organizations to centrally define and modify usage controls such as:

Who	What	When	Where
can access the information	can they do with the information	does the access begin and end	can they access the information

Learn the importance of digital asset protection and control in the semiconductor industry

[Download Whitepaper](#)