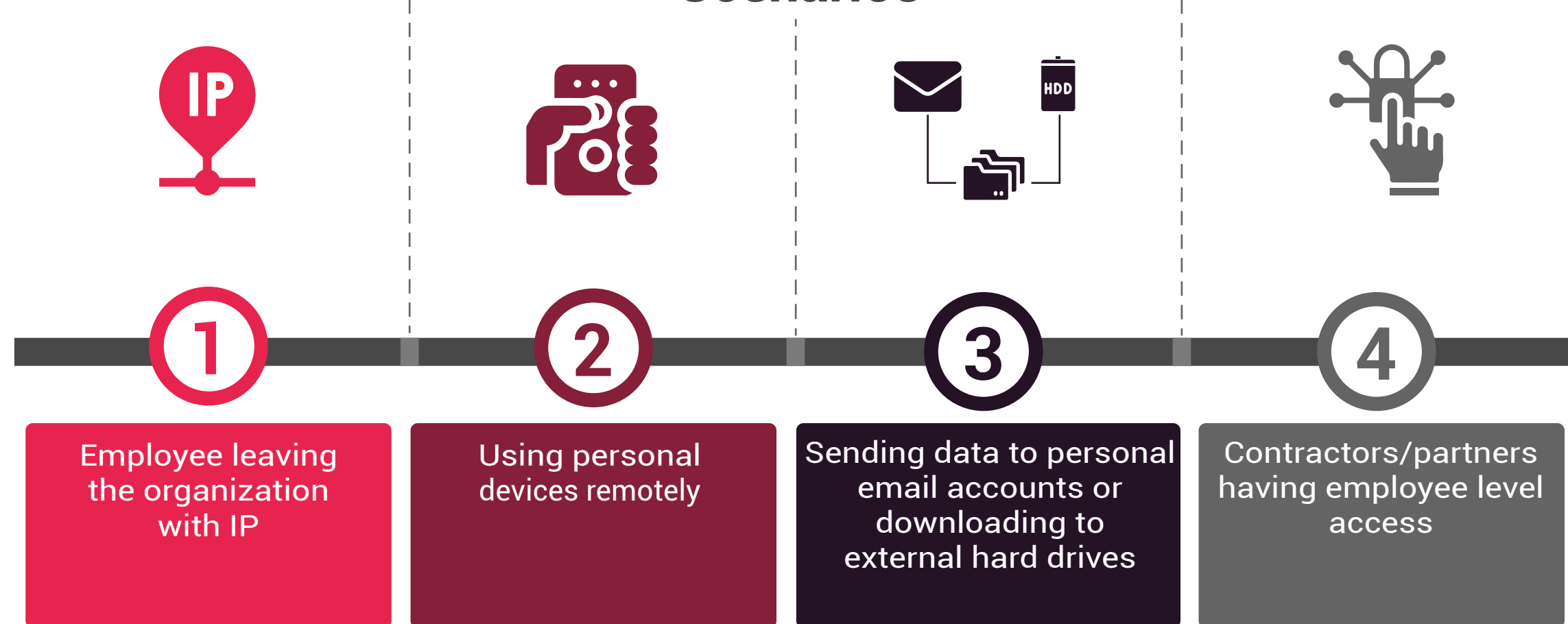


Insider Threat Protection

Semiconductor Industry

The increased usage of many semiconductors worldwide has drawn significant attention to the semiconductor industry for potential insider threats. While many organizations have implemented robust security measures to protect their systems, their most sensitive digital asset - their intellectual property - is at risk.

Scenarios



"Samsung Employee Allegedly Captures Sensitive Chip Manufacturing Information"

Source: WCCFTECH

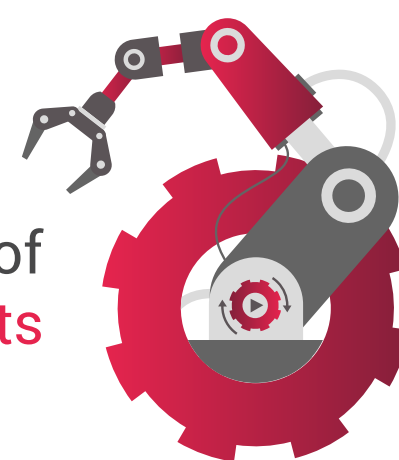
22% of the times, **Malicious insiders** are the reason for **security incidents** in a company

47% Increase in insider threats from 2018 to 2020

Source: TESSIAN

Manufacturing

is among the five industries with the highest percentages of **insider threat incidents** and **privilege misuse**.



Source: VERIATO

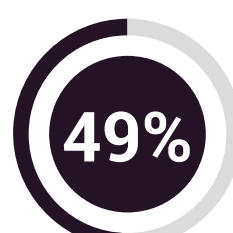


Major factors driving insider threats

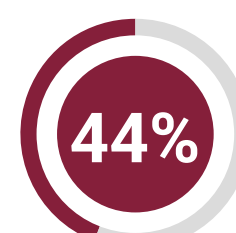
Source: TECHJURY



Fraud



Monetary gains



Intellectual Property theft

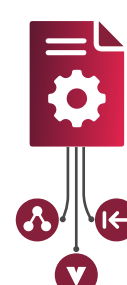


85% Organizations finding it challenging to determine the actual **damage** of an **insider attack**

Source: TECHJURY

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

Source: TECHJURY



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 every digital asset
- Tracks activities on a protected document in real-time
- Enables organizations to centrally define and modify usage controls such as:



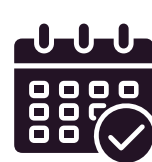
Who

can access the information



What

can they do with the information



When

does the access begin and end



Where

can they access the information