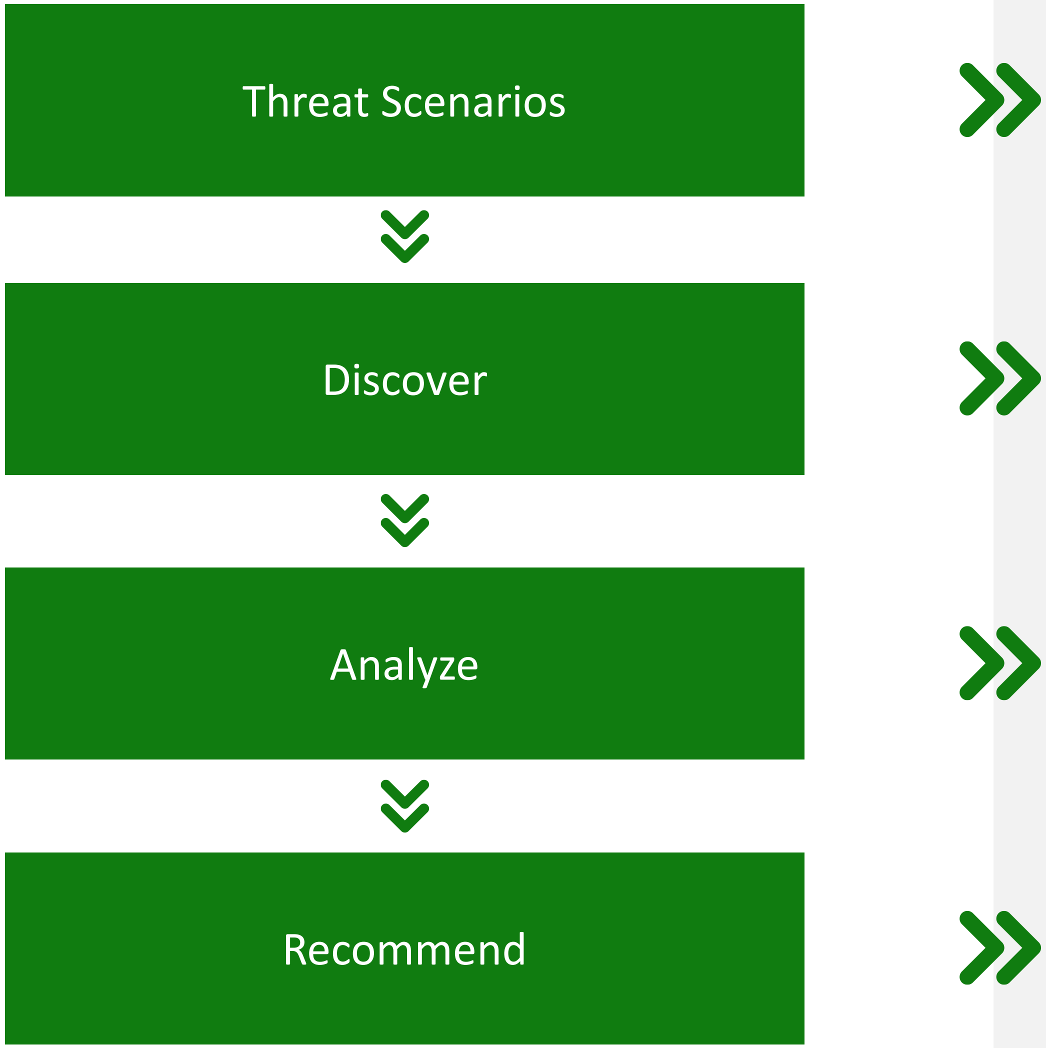
Cybersecurity Assessment

Discover vulnerabilities to your Microsoft cloud and on-premises environments.

ELEVATE SOLUTIONS

Engagement Methodology



Threat Scenarios

Discover

Analyze

Recommend

The engagement covers two commonly seen threat scenarios:

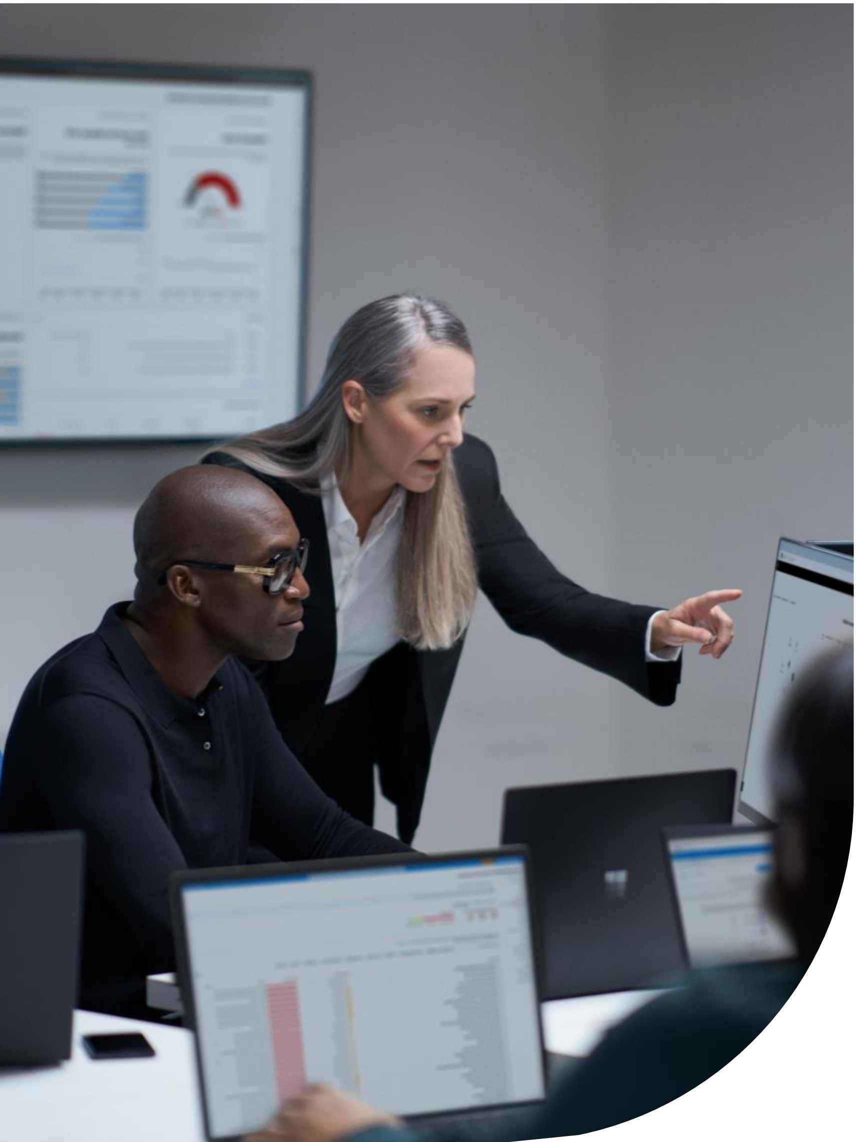
- Human-operated Ransomware
- Data Security risks from company insiders

Using the engagement tools, discover vulnerabilities within your production environment across cloud, servers and endpoints.

The vulnerabilities and risks are analyzed and prioritized to show how prepared your defenses are against the included threat scenarios.

Receive detailed recommendations from the assessment to help you prioritize the improvements to your cybersecurity posture.

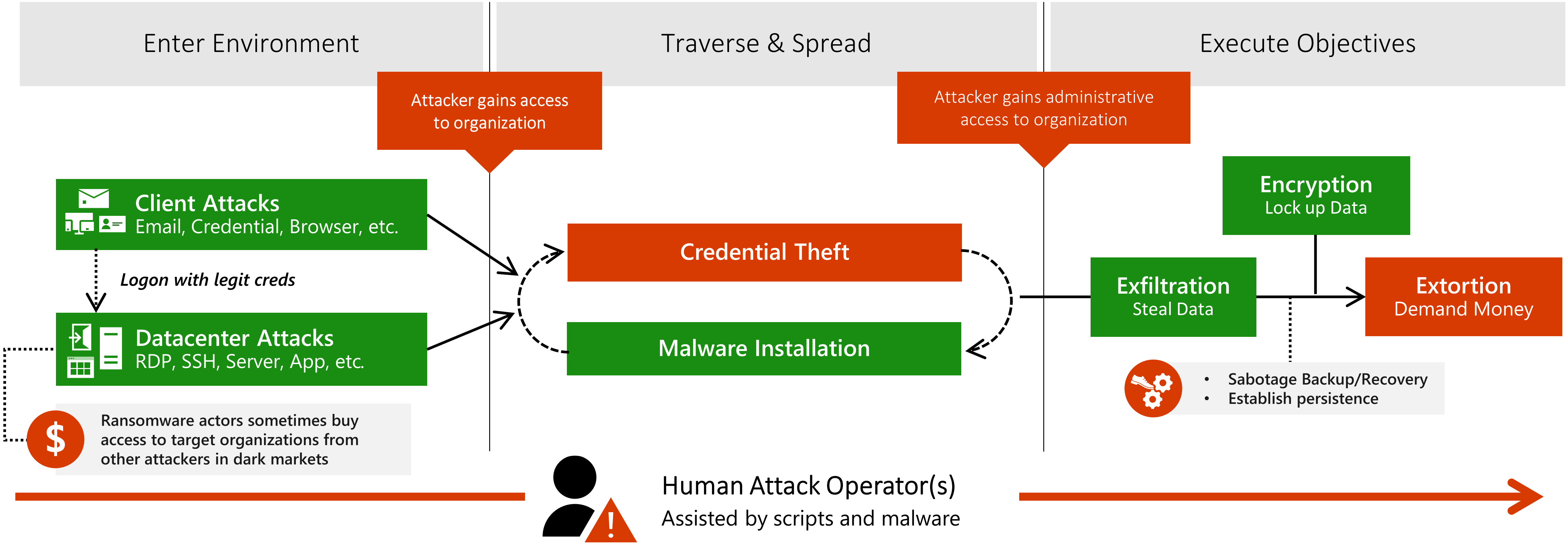
Top Human-operated Ransomware Concerns



Organizations struggle with maintaining basic cybersecurity hygiene	98%	of ransomware attacks can be traced to common configuration errors in software and devices. [1]
Ransomware attacks have been steadily increasing	37%	of all businesses and organizations were hit by ransomware in 2021. [2]
Recovering from a ransomware attack is costly	$1.85M	Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.[3]

Human-operated Ransomware Overview

Human-operated ransomware is the result of an active attack by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.

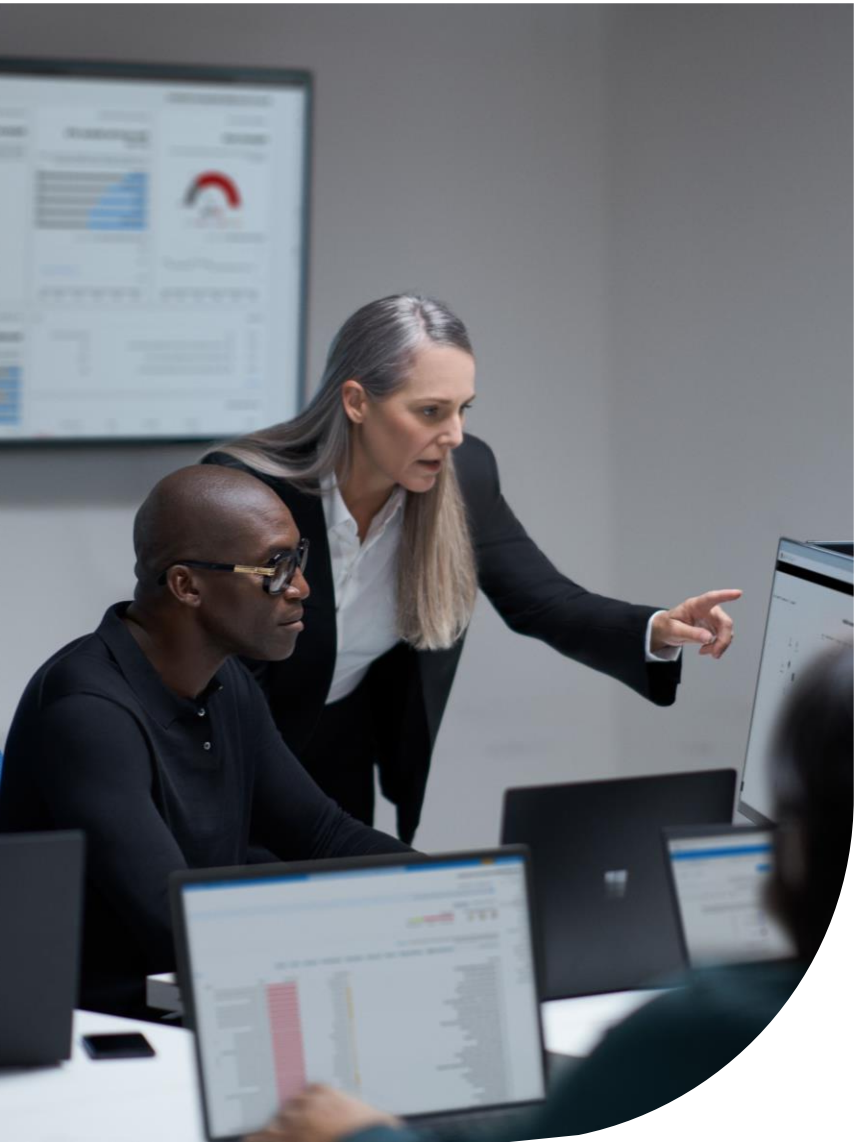


- Sabotage Backup/Recovery
- Establish persistence

Ransomware actors sometimes buy access to target organizations from other attackers in dark markets

Human Attack Operator(s)
Assisted by scripts and malware

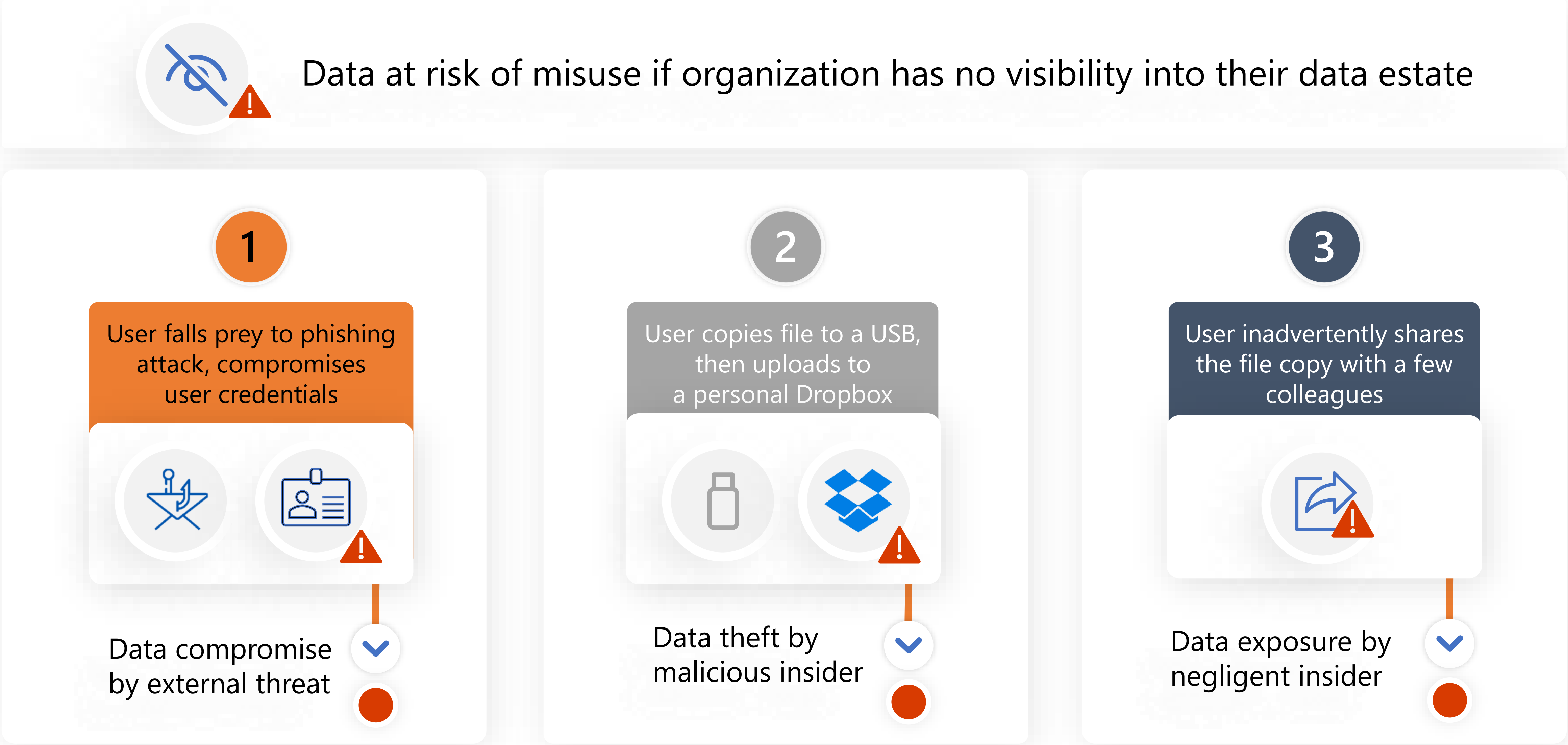
Top data security concerns



Data security incidents are widespread	83%	of organizations experience more than one data breach in their lifetime[1]
Malicious insiders account for 20% of data breaches, adding to costs	$15.4M	Total average cost of activities to resolve insider threats over 12 month period[2]
Organizations are struggling with a fragmented solution landscape	80%	of decision makers purchased multiple products to meet compliance and data protection needs[3]

1. Cost of a Data Breach Report 2022, IBM
2. Cost of Insider Threats Global Report 2022, Ponemon Institute
3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

Data security incidents can happen anytime, anywhere



Data at risk of misuse if organization has no visibility into their data estate

1

User falls prey to phishing attack, compromises user credentials

Data compromise by external threat

2

User copies file to a USB, then uploads to a personal Dropbox

Data theft by malicious insider

3

User inadvertently shares the file copy with a few colleagues

Data exposure by negligent insider

What we’ll do during the engagement

Analyze your environment and current cybersecurity maturity level based on v8 of the CIS Critical Security Controls.

Define scope & deploy Microsoft Defender Vulnerability Management and Insider Risk Analytics in your production environment.

Perform a vulnerability assessment and assist with the prioritization of vulnerabilities and misconfigurations across your organization.

Perform a data security assessment, discover and evaluate sensitive information and potential insider risks in your organization.

Plan next steps on how to improve your cyber and data security posture and how we can work together.