IDENTITY AND ACCESS MANAGEMENT

Identity Security Posture

Your digital identity is the key to accessing your virtual world.
Can you afford to lose it?

MICROSOFT
ENTRA ID

ACTIVE
DIRECTORY

ENTRA
CONNECT

ENTRA
CLOUD SYNC

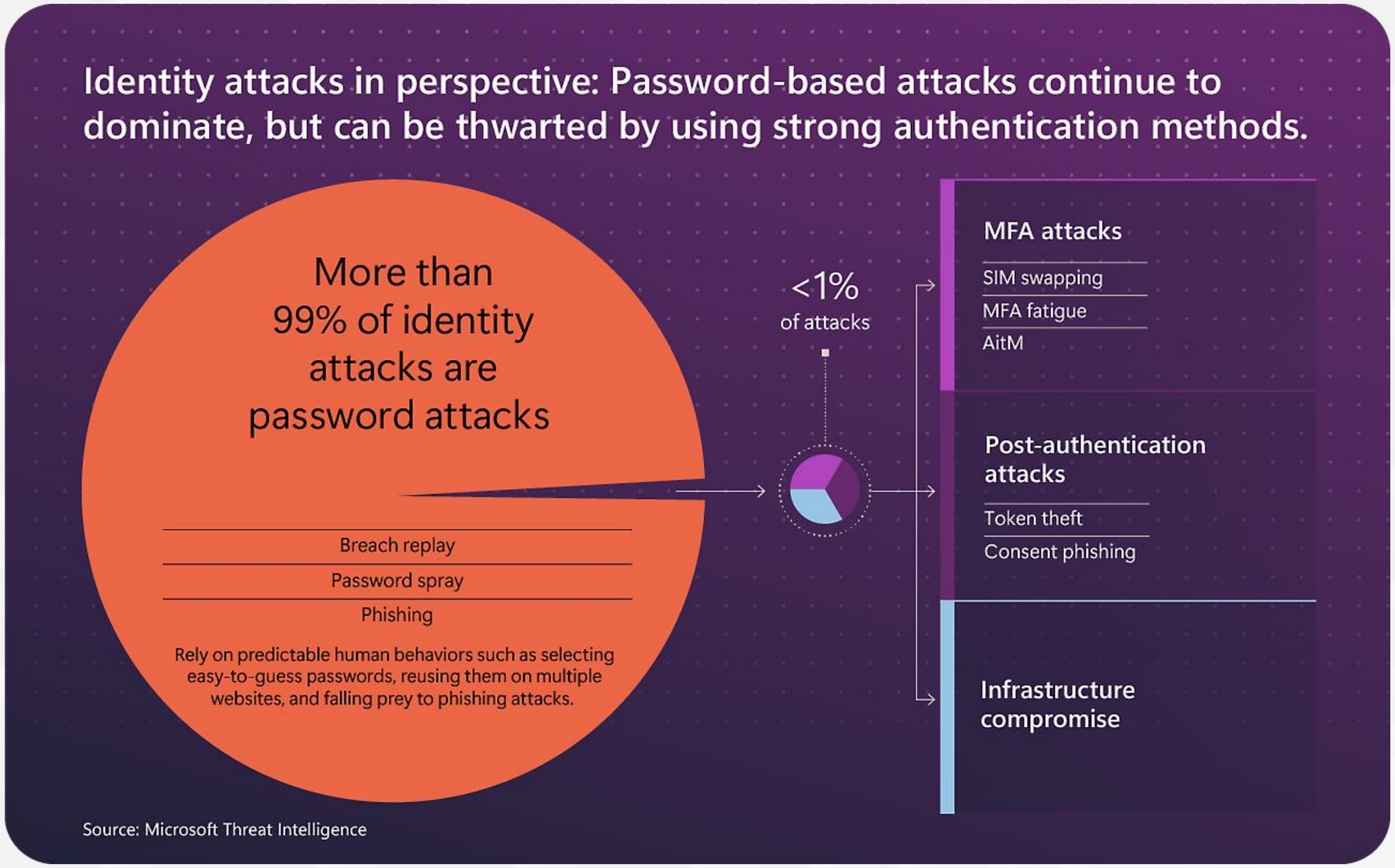
REPLY
CLUSTER

INSIGHTS ON IDENTITY ATTACKS

As organizations move to the cloud and adopt SaaS applications, **identities** are becoming increasingly **crucial** for accessing resources.

Cybercriminals exploit legitimate and **authorized identities** to steal **confidential data**, and access credentials in various ways like phishing, malware, data breaches, brute-force/password spray attacks, and prior compromises.

Password-based attacks on users constitute most identity-related attacks, supported by massive infrastructure that threat actors have dedicated to combing the digital world for passwords.



REPLY CLUSTER

WHY IDENTITY SECURITY

Conducting an identity **security assessment** helps ensure that user identities are **well-protected**, which in turn safeguards sensitive data from unauthorized access. Moreover, an assessment allows to identify and address any weaknesses in their security configuration. By doing so, the overall **security posture** can be strengthened, making it harder for potential attackers to exploit **vulnerabilities**. By proactively identifying and fixing vulnerabilities, the risk of cyberattacks, such as phishing or unauthorized access, is significantly **reduced**.

This proactive approach not only helps in maintaining a **secure environment** but also enhances the overall user experience. Users can enjoy a more reliable and secure system, with fewer disruptions due to security breaches.

MOST COMMON IDENTITY SECURITY RISKS

- Phishing
- Account hijacking
- Unauthorized access
- Privilege abuse
- Man in the Middle (MitM)
- Credential stuffing

REPLY CLUSTER

ASSESSMENT GOAL

OVERVIEW

Customer Cloud or **Hybrid IAM** implementation based on **Microsoft** product and services will be assessed to verify that configuration and Identities conform to Cybersecurity and vendor **best practices**. Entra ID tenants, Active Directory Forests and Entra Cloud Sync / Entra Cloud Connect configurations will be analysed and compared to **security baselines**. Customer will be provided with a report with containing a **list of remediation** to improve security posture.

IDENTITY SECURITY CHALLENGES

- **Complexity of IT Infrastructure**
- **Adherence to best practices**
- **Comprehensive report**
- **Continuous maintenance**
- **Correct misconfigurations**
- **Continuous monitoring**

REPLY CLUSTER

ACTIVE DIRECTORY

Increasing security posture in Active Directory and Entra

ASSESSMENT

Assess the current security level using market-leading and Microsoft built-in tools to find vulnerabilities.

ANALYSIS

Report analysis to identify the main security risks and possible impacts.

DESIGN

Design of a remediation path to increase security posture.

REMEDIATION

Implementation of the defined remediation and execution of a second confirmatory assessment.

REPLY CLUSTER

ENTRA ID

Increasing security posture in Microsoft Entra

SECURE SCORE

Identity secure score functions as an indicator for how aligned the tenant is with Microsoft's recommendations for security.

ANALYSIS

Report analysis to identify of the main security risks and possible impacts.

DESIGN

Design of a remediation path to increase security posture.

REMEDIATION

Implementation of the defined remediation and execution of a second confirmatory assessment.

REPLY CLUSTER

ENTRA CONNECT / CLOUD SYNC

Follow the best practice on Entra Connect and Cloud Sync

SOURCE ANCHOR

Configure the best suited Active Directory attribute to be used as source anchor for the cloud identities.

HIGH AVAILABILITY

Setup a highly available infrastructure to support the Hybrid Identity architecture.

VERSION UPDATE

Update the involved systems to the latest version to always have support available.

SYNC RULES ANALYSIS

Review and cleanup of the custom sync rules to decrease complexity.

REPLY CLUSTER

APPROACH

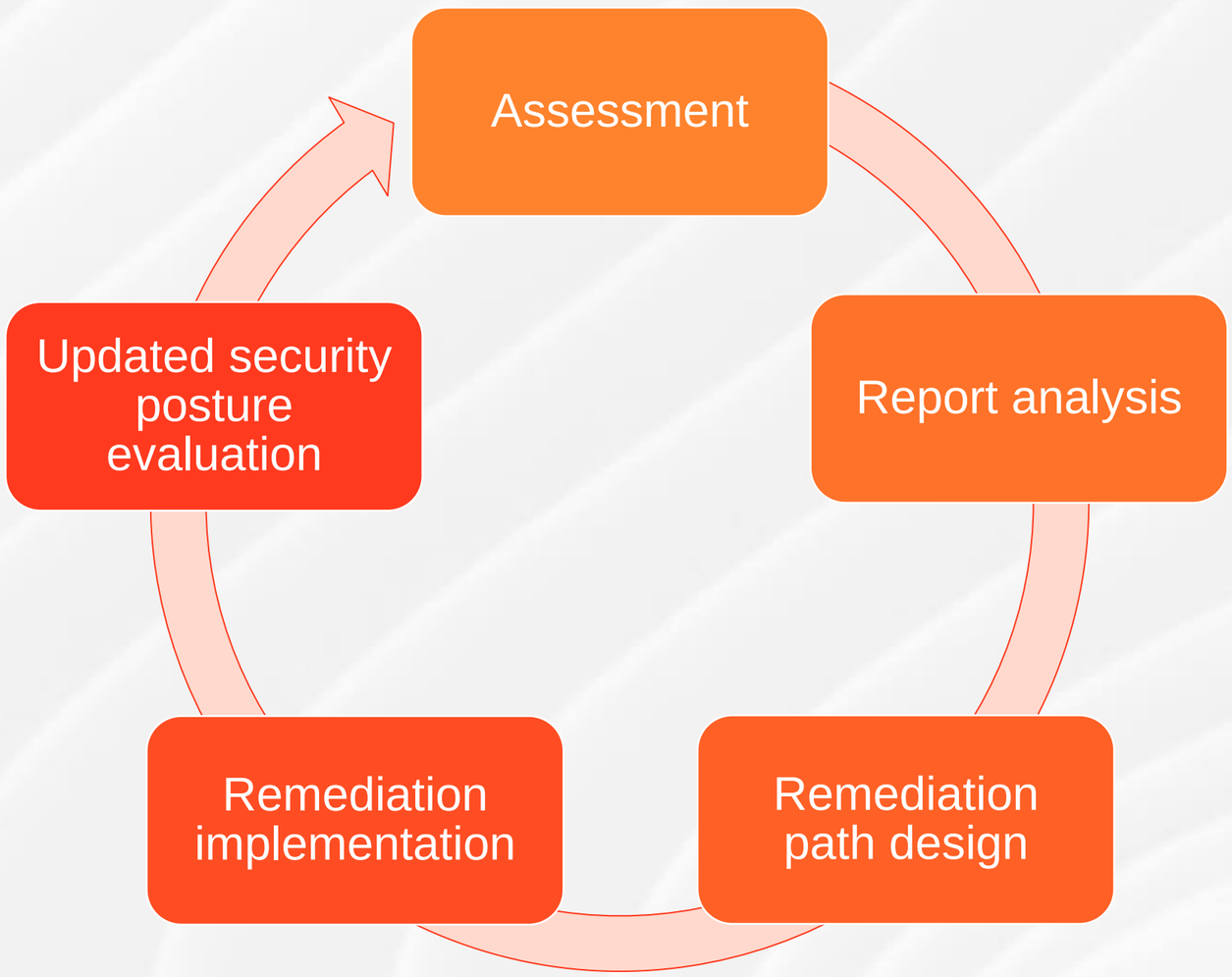
A structured approach to security

The assessment will produce a report containing a list of remediation to improve security posture on the Identity Systems in scope. From the vulnerabilities highlighted in the report a remediation path will be designed, which will aim to solve the most critical issues first and then gradually the ones with lower priority. After the first remediation implementation a new assessment will be run to check the updated security posture. Moreover, a monitoring process will be enabled to monitor if solved vulnerabilities arise again and to run new security checks when available.

The lifecycle of each Identity System is independent and the activities of each one can be performed in parallel.

SECURITY POSTURE LIFECYCLE

FOR EACH SYSTEM IN SCOPE



REPLY CLUSTER

IDENTITY AND ACCESS MANAGEMENT

REPLY CLUSTER

Contact us!

Riccardo Bellatreccia

r.bellatreccia@reply.it

Andrea Di Fonzo

a.difonzo@reply.it

WWW.CLUSTERREPLY.IT