SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection and Response Services for M365D

Brute Force or Stolen Credential Attacks

KEY BENEFITS

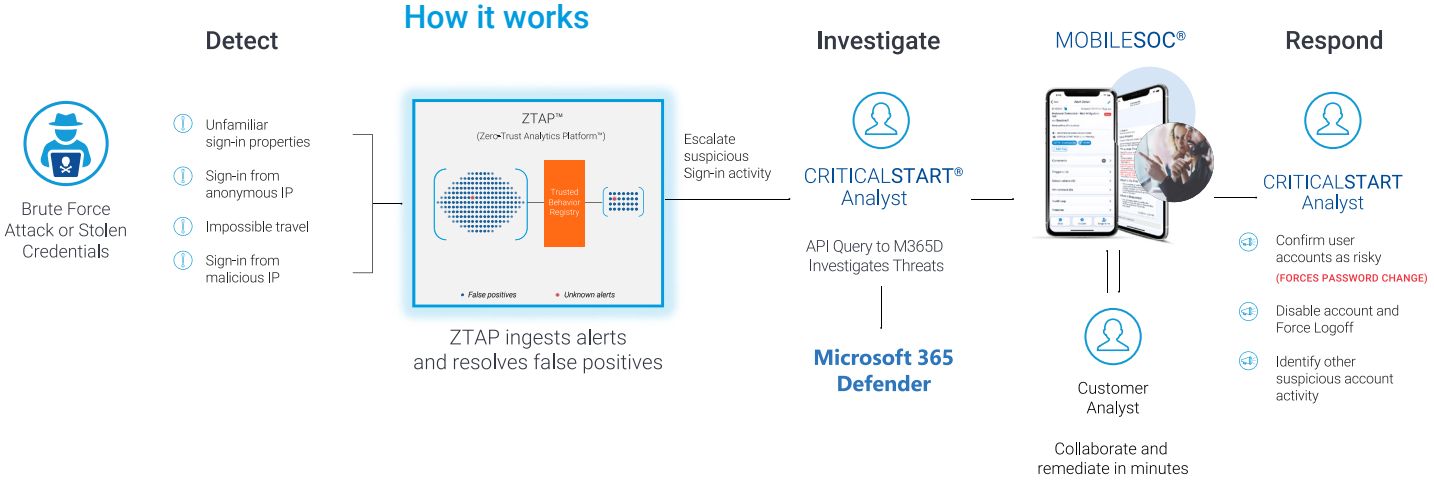
- ✓ Prevent takeover of user's credentials
- ✓ Obstruct lateral movement to other applications
- ✓ Stop adversaries from exfiltrating sensitive data
- ✓ Disrupt attacks against Cloud Apps
- ✓ Protect user identities and credentials stored in Active Directory

A brute force attack may be an old method based on password guessing trial and error, but it is still used by adversaries today because it's an effective way to enter your organization via a user's weak password – a computer can guess more than 100 billion passwords per second[1]. Once logged into a user's account, an adversary can change the password to create persistence in that account, attempt to exfiltrate data and move laterally - one of the most challenging areas of attack detection – to other applications.

Solution

Critical Start MDR Services for Microsoft 365 Defender (M365D) provide threat detection, investigation, and remediation options. The Critical Start Security Operations Center (SOC) leverages the Microsoft 365 Defender security suite to detect and disrupt brute force attacks.

How it works



Individual alerts from the Microsoft Defender Suite (Azure Active Directory and Defender for Cloud Applications) are ingested into ZTAP™, our Zero Trust Analytics Platform™, where automated investigation and triage occur removing false positives. True positives are escalated to our SOC for further enrichment and deeper human-led investigation and remediation.

For user accounts that have been identified as compromised, our Critical Start security analysts can:

- Isolate the threat and compromised user's account
- Disable the account and force logoff
- Force password change

For more information: www.criticalstart.com

CRITICALSTART®

 [1] https://theconversation.com/a-computer-can-guess-more-than-100-000-000-000-passwords-per-second-still-think-yours-is-secure-144418