CrowdStrike White Paper

CROWDSTRIKE

FALCON ZERO TRUST RISK SCORE

CONTENTS

OVERVIEW

Falcon Zero Trust's Risk Score is dynamic computation resulting from the activities and the behavior of a user or computer account. It is based on all account information available, and, to a large extent, represents the likelihood of the account being successfully breached by a malicious attacker or of an insider going rogue.

This likelihood is expressed as a number from 0 to 10. The higher the number, the larger the probability for the account to become a vector or conduit of an attack.

HOW RISK SCORING WORKS

Every security expert understands that risk is relative, changing, and dynamic: that is why the risk score must be constantly adjusted. Falcon Zero Trust follows this approach and expands it by constantly evaluating multiple activity-based elements and factors (see Activity-Based Factors in the FAQ for examples). The factors belong to 3 major categories:

- Actual account characteristics
- Results of the account's activities
- The metadata associated with the account including organizational security information

Some of these factors are long-lasting and others, such as network events, have a temporary and passing effect, but all of them are processed and computed by Preempt's proprietary algorithm. As the monitored account evolves, their respective risk score can increase or decrease.

For example, a weak password will have a stable and long-lasting impact on a user's risk score until the password changes to a stronger one.

Now let's imagine that the same user for the first time accesses a server outside of their established baseline. Even though it may be merely a new server or a server accessed for the first time through a VPN, this activity definitely deserves attention and will contribute to the user's risk score. Its impact, however, will depend on the user type, their historical trend of access, etc, and may be substantially different in each particular case.

If the account is malicious or infected, or perceived by Falcon Zero Trust as exceptionally vulnerable, its related behavioral events will be flagged by Zero Trust cyber logic rules and increase the risk score.

Note: Falcon Zero Trust empowers end-users (via MFA validation) and security administrators to resolve and influence specific aspects of the score (see FAQ).

THE FALCON ZERO TRUST RISK SCORE MODEL

The Risk Score complements the machine learning profiling and the security rules by generating a predictive timeline of the likelihood that an entity is under threat or is becoming a threat.

While the Risk Score is used as a common building block in the User and Entity Behavior Analytics market, it is important to compare the capabilities and understand the value of the Preempt solution, which is:

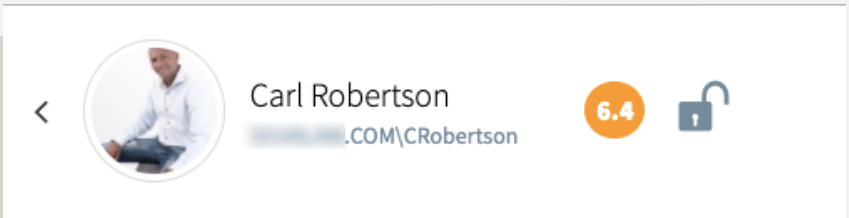
1. **Robust and extensible** - The risk scoring mechanism is built from the ground up in such a way that it can be extended and accept additional dimension inputs from third-party sources inside or outside the solution, such as Cloud Single Sign-On (SSO), email security gateways, Virtual Private Network (VPN) gateways, Next Generation (NG) firewalls, etc.
2. **Calculated for all accounts** - Falcon Zero Trust acknowledges that all network accounts (users, services, and devices) may pose a certain risk. All of them are scored individually and compared against each other. This score is unrelated to the ability to put entities, accounts, and endpoints on the Watch List, which raises their risk score.
3. **Definitive range to compare accounts** - The risk range is bound between 0-10 points to allow clear comparison between accounts. It is easier to compare risk scores with values of 7 to 8 and the strength of their contributing factors, as opposed to comparing risk scores that have no upper limit as they lack the notion of relative scale.
4. **Combination of real-time data and log sources** - The data Falcon Zero Trust uses to calculate the score is based on actual real-time user activities on the network. It is complemented by metadata context collected from events logs and by Active Directory data. The combination of real-time activities and their results (for example, a weak password or the use of a shared endpoint) with metadata from systems and logs makes this scoring more accurate and reliable than what is generated by simple log digestion systems.
5. **Dynamic and customizable** - Falcon Zero Trust's scoring algorithm uses variables that change over time. As a result, factors that become less important over time are re-evaluated and readjusted. For example, a password that never expires is a constant factor that that will impact the Risk Score until it is dealt with. On the other hand, account activity that triggers a security event will also affect the score, but its effect will decline over time in accordance with the event severity. Security administrators can modify the risk score for certain dimensions, as shown in the FAQ section.
6. **Trend evaluation** - Each account's risk score is logged, and the security administrator can evaluate it on an historic timeline. This allows them to observe which factors contributed to the risk score at any given time and assess whether a security event is merely coincidental or recurring, and thus, demanding more attention.

FAQ

HOW TO INTERPRET THE RISK SCORE?

By default, all network accounts are sorted by the Risk Score on the Insights page.

The Risk Score is a number associated with a specific system account. For example, here is a user account with the Risk Score 6.4:



Note: If the Risk Score is not indicated, it means that the system does not have enough data to calculate it, not that the account risk is too low.

Risk score historic trend appears in the account card together with a breakdown of the factors that affected the score at each time.

The length and color of each bar represent the respective factor severity.

CAN A USER INFLUENCE THE RISK SCORE?

Yes, some factors can be controlled. You can, for example:

- Resolve incidents to lower their impact (for example, baseline deviation)
- Change weak or rotate aged passwords
- Disable stale accounts
- Validate identities via MFA, which automatically resolves incidents and builds trust.

WHAT IS INCLUDED IN THE RISK SCORE?

The Risk Score is made up of multiple factors that represent a holistic view of the account and what is known about it. The attributes that contribute to the Risk Score are based on the account activity or inactivity, its related metadata and dynamic specific characteristics, such as the password strength.

The activity-based factors are as follows:

Unusual Access to Service	**Unusual Use of Endpoint**
Unusual Access to Server	Daily Volume Anomaly
Identity Verification Denied	**Stale Usage (Account/Entity)**
Forged PAC	Golden Ticket
LDAP Harvesting	**Pass-the-Ticket**
Password Brute Force	Unusual Activity Times
User Brute Force	**Aged Password**
Use of Risky Endpoint	

The following Active Directory metadata affects the risk score:

Password Never Expires	**OS details (e.g. Vulnerable)**
Unmanaged Host	Administrative Role

The entity characteristics considered in the risk score are as follows:

Weak Password	**Exposed Password**
Shared endpoint	Shared User
Inactive Account	**VPN Usage**
Stale Host	Stale Account
Stale Service	**Watched Entity**
Stealthy privileges	Similar users comparison (aka peer groups)
Duplicate Local Administrator	**Account with SPNs**
Insufficient Password Rotation	Accounts Using DES Key Only
Privileged Endpoint Account	**Guest Account Enabled**
Kerberos Pre-Authentication For TGT Is Not Required	

The following risk factors are relevant to the domain configuration and affect entities:

NTLM V2 Compatibility	**Skeleton Key Vulnerability**
Password Policy Strength	Hidden Object

Note: This list changes over time. Falcon Zero Trust adds or remove factors according to its threat prediction cyber logic.

RISK SCORE BOOST

The boost is yet another factor that impacts the Risk Score. It can be applied when Falcon Zero Trust perceives additional potential damage, for example, if an alert that contributes to the score is repetitive or persistent. The score can be also boosted if a particular account:

- Has administrative rights
- Belongs to a power user: such as an executive manager role
- Is a server with specific critical roles

Falcon Identity Protection secures all workforce identities to accelerate digital transformation. Since 80% of all breaches involve compromised credentials, Falcon Identity Protection unifies identity threat detection and conditional access for on-premises and cloud identities. Threats are preempted and IT policy enforced in real-time using identity, behavioral, and risk analytics, protecting 4M+ identities across 400+ enterprises.