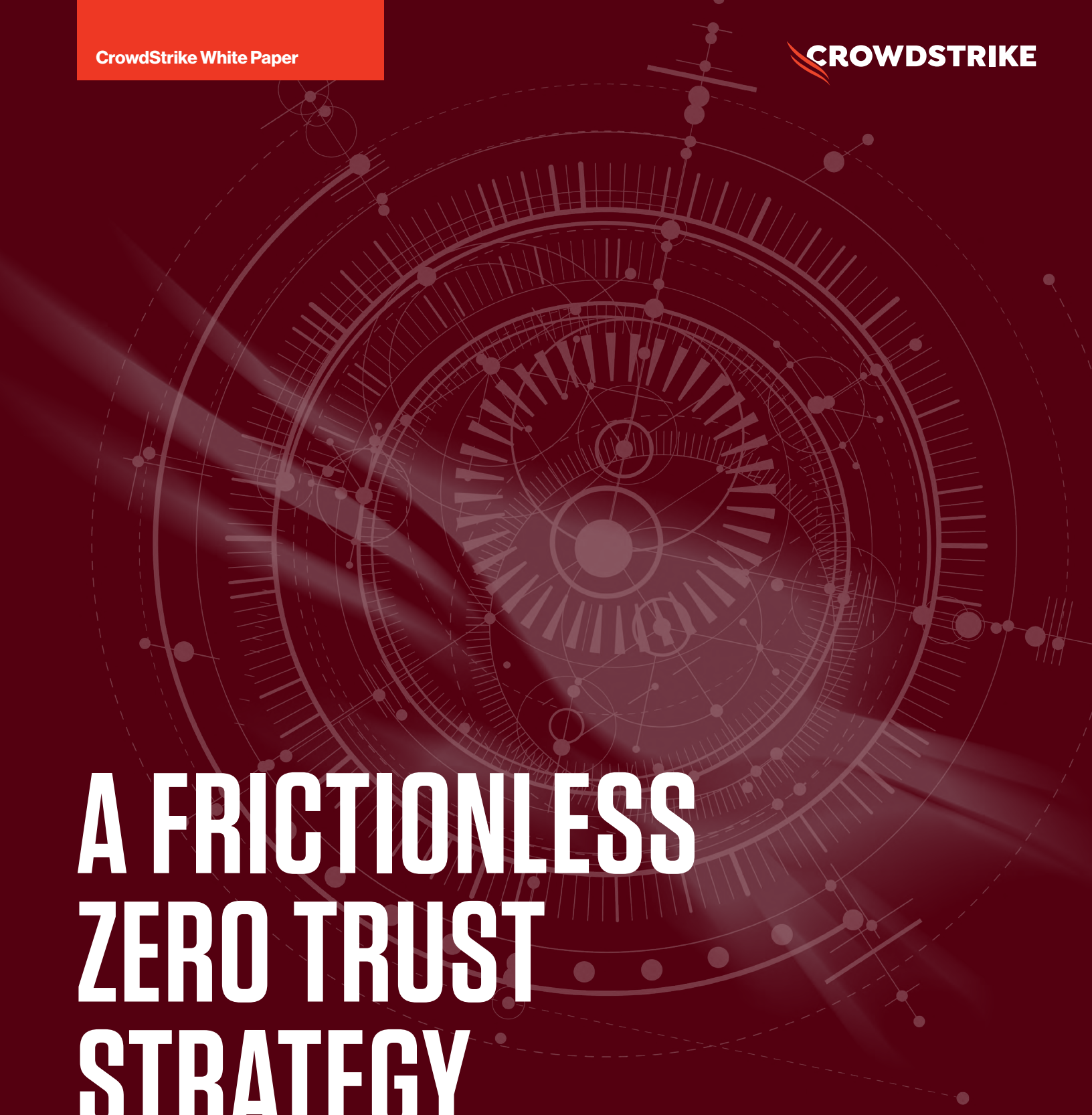
CrowdStrike White Paper

CROWDSTRIKE



A FRICTIONLESS ZERO TRUST STRATEGY

No enterprise builds their organization with the intent to be complicated or difficult to support and keep secure – but no two networks are ever identical. From organic to acquisitional growth, networks and organizations become complex. Add to that complexity a constant push from executive stakeholders to modernize, whether that's embracing cloud services or simple business transformation by improving internal systems, change and increased risk is inevitable.

Whether your motivation is business transformation initiatives, or if you merely have a mandate to reduce risk or recover from incidents, a Zero Trust strategy is the best and safest path to achieve your goals - and guarding the Identity Store is key to a solid Zero Trust strategy. Falcon Identity Protection can help you achieve Zero Trust with Zero Friction to your workforce.

THE NEED FOR ZERO TRUST

Zero Trust has been envisioned as 'Trust none, unless otherwise explicitly allowed'. Organizations are accelerating their digital transformation initiatives along with a remote workforce. With a parallel increase in attack sophistication leveraging user credentials, Zero Trust has become a necessary strategy in every enterprise.

- **'Castle and moat' network defences are outdated** – Traditional, perimeter-based technologies like firewalls, VPNs, VLANs are less effective today in flat networks, than they ever were over a decade ago. The perimeters are dissolving. Users are no longer accessing applications and resources from within the corporate network, and from company- issued (managed) endpoints. The applications, resources and data are not only inside the enterprise perimeter, but also in multi-cloud environments.
- **Static policies are antiques** – Access policies defined through firewall rules, VLAN ACLs, and VPNs are rigid. Static access policies cannot scale up with or adapt to the dynamic application environments and changing secure access requirements that have moved beyond static perimeters. With an explosion of remote and cloud users as well as applications, static authentication policies slow down the organization's capability to rapidly adapt to change, where change is core to the new business model in user behavior, roles, and access patterns.
- **Large and expanding attack surface is real** – The changing business models and digital transformation have dissolved the perimeters and added layers of complexity across the organizations' IT environment. Users authenticate locally or remotely, to on-premises resources or cloud apps, from managed and unmanaged endpoints, to access distributed applications, all of which increases the attack surface of the organization.

According to the latest data breach reports from Ponemon and IBM, the mean time to detect a breach is over **280 days** and mean time to contain the breach is over **70 days.** Imagine the breadth and depth of damage the hacker could do lurking inside your network, undetected.

According to the 2020 Cost of a Data Breach report, "compromised credentials were the costliest and most frequent threat vector."

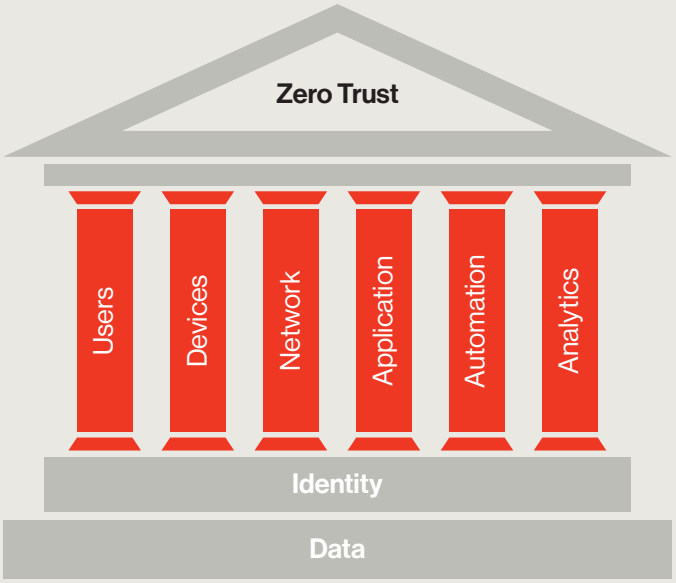
WHY SECURE WORKFORCE IDENTITIES?

Organizations must approach Zero Trust from a user perspective, as their identities are the last line of defense. A Zero Trust strategy focuses on securing the identity layer and strengthening user authentication – i.e. wrapping security around identity, as that's where most of the compromises happen. Having said that, be it Zero Trust or the principle of least privilege, it all ties down to one basic requirement: Securing access to applications or resources with the least friction to the user.

THE PILLARS OF ZERO TRUST?

Organizations are structured in several ways to enable users access applications and resources, on-premises and in the clouds. Organizations considering Zero Trust to secure workforce identities should weave through the six fundamental pillars - Users, devices, network, applications, automation and analytics - to achieve unified visibility, detection, and enforcement.

SIX PILLARS OF A ZERO TRUST SECURITY MODEL



ORGANIZATIONS SHOULD CONSIDER A ZERO TRUST STRATEGY FOR THE FOLLOWING SCENARIOS

1 Dynamic environments with applications on premises and in the cloud, with an explosion of users trying to access them from anywhere

2 Organizations that are accelerating their digital transformation initiatives

3 Organizations that want to reduce the mean time to detect threats and user compromise, whether from social engineering, compromised passwords, malicious insiders, stealthy administrators, etc.

IDENTITIES (USERS)

Continuous visibility, threat detection, and real-time response are key requirements to protect the identity store (e.g. Microsoft Active Directory, Azure AD, Okta SSO, etc.) from cyber threats. Understand who your users are, and their authentication pattern across boundaries (on-premises and clouds). Distinguish human users from programmatic accounts (service accounts) and ensure that every account gets the right access to applications and resources. To do this, security needs dynamic user behavior profiles to understand both threats and risks.

MANAGED & UNMANAGED ENDPOINTS (DEVICES)

The endpoint from which the user authenticates to access applications is part of enabling Zero Trust for workforce identities. These endpoints could be managed (issued by your organization) or unmanaged. Monitoring and controlling authentications from these endpoints are important to reduce the attack surface and maintaining a consistent security posture.

NETWORK

Technology such as network segmentation reduces the attack surface from the outside, but most persistent compromises involve valid or current user credentials. In Zero Trust, when we talk about 'perimeter-less' networks, what actually has happened is that the perimeter has moved closer to the individual resource or application (referred to as micro-perimeter), instead of being at the edge of the network. For modern organizations, identity has become the new perimeter. Organizations should discover and prevent incidents automatically in real-time; including advanced AD/credential attacks, protocol attacks, lateral movement and privilege escalation attempts; across their network with identity-based segmentation.

APPLICATIONS/WORKLOADS

Workloads and applications distributed across on premises networks and clouds are accessed by users and programmatic accounts. The security and Identity and Access Management (IAM) teams must have granular understanding of application accesses, along with real- time analytics. This ensures that all resources, including legacy and proprietary applications, are accessed in a secure manner from any location. A Zero Trust system should apply identity verification (e.g. multi-factor authentication/MFA) when the risk increases.

AUTOMATION

It's not enough to log events to correlate and analyze later. Zero Trust means security automation, in discovery, tracking, and monitoring. Identity-aware access rules or policies should be defined and automated with a clear understanding of the

Technology such as network segmentation reduces the attack surface from the outside, but most persistent compromises involve valid or current user credentials.

sensitivity of the data and applications, the end users, and their anticipated access behavior. For example, if there's an anomalous access request to a sensitive data/application, the user could be challenged with MFA for identity verification – which, if the credential is confirmed through step-up authentication, auto-resolves this access incident without involving IT or the security team. If the attempt is denied, this should be correlated against other activity and auto-escalated for further analysis, bringing down the mean time to detect and resolve incidents without error-prone manual effort. If need be, incidents can be brought to resolution by integrating with SOAR and ticketing platforms – but from a single, centralized source of the truth for analysis that encompasses all assets and applications.

ANALYTICS WITH SECURITY VISIBILITY

Zero Trust is the ability to preempt threats by full visibility, correlation, and monitoring with actionable data and reporting capability at all levels – from executive to the security analysts. Security visibility and analytics play a key role in helping organizations move from being reactive to proactive. Security and IAM teams should be able to visualize the authentication footprint and user behavior analytics happening in real-time and use the collective information of authentication patterns to create baselines as well as review and refresh (as needed) the rules and authentication policies.

REALIZING THE ZERO TRUST PILLARS WITH FALCON IDENTITY PROTECTION: SEGMENT – AUTOMATE – VERIFY

Creating a Zero Trust security stack can be expensive and complicated, as many point solutions have offered solutions for each of the pillars – or one or two combined. And then when implemented, the different tools may or may not integrate and play well together, such that finding out what's going on in different parts of the network or cloud can require two to three dashboards or reports.

Falcon Identity Protection offers a central solution, with a solution which offers up Zero Trust security by controlling identity access through dynamic identity risk evaluation, preventing lateral movement through the network, and a flexible way to verify identity that is low hassle for the end user and allows business to continue with fewer but more meaningful checks. The path is defined through logical segmentation, security automation, and verifications.

SEGMENT

Segmentation is a critical element of mitigating risk in Zero Trust Models. Focusing on identity segmentation inhibits lateral movement for the bulk of breaches. Enterprises need to segment user accounts (employees, contractors, remote workers, and even privileged users) along with the endpoints into micro segments – with consideration to additional security for the most critical (or highly-regulated) systems.

- **All data sources and computing services are considered resources:** Entities such as laptops, desktops, physical servers and virtual machines are considered resources. All these endpoints are associated with users - human or programmatic - and are used to access enterprise applications and resources, on-premises or clouds. Falcon Identity Protection gathers this data, figuring out which users belong to which groups, which have credentials and privileges on which systems, and how they behave individually and as a group.
- **All communication is secured regardless of network location:** It does not matter to Falcon Identity Protection whether the endpoint which accesses resources is managed by the enterprise or not, is physically inside or outside the network or wider LAN - all access requests are met with the same security requirements and policies. All access requests are processed based on over 100 behavior analytics, including access locations, endpoint used, risk scores, thresholds, threats and more, before access is granted to a resource.

AUTOMATE

Zero Trust cannot rely on someone looking back at user behavior patterns and deciding if they were suspicious. Security needs to be automated and smart, taking in as much data as possible on every transaction to discover patterns, intent, anomalies, and incidents.

- **Access to individual enterprise resources is granted on a per-session basis:** With proprietary Artificial Intelligence and Machine Learning (AI/ML) capabilities, user trust is evaluated before access is granted to a specific resource. Additionally, if an incident is investigated by a human analyst and marked as safe, (e.g. known network scanner activity), Falcon Identity Protection learns from that designation and adopts the input as a valid and valued input to its automated learning and adjustments of user risk score and behavior pattern.
- **Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes:** Falcon Identity Protection allows for automated segregation of human and service accounts (programmatic), and along with 100+ behavioral patterns including the attributes associated with the account, the endpoint used to authenticate to a resource, account baselines, access locations, access deviations and continuous assessment of changing risks. All of these determine how Zero Trust permits access to a resource. Falcon Identity Protection - Zero Trust solution comes with out-of-the-box dynamic policy templates built around behavior, user attributes, thresholding, and customizable segmentation rules, that can be defined to make resource accesses deterministic.

VERIFY

The old model of Trust but Verify is replaced by Verify against patterns and known actions, against credential health and behavioral analytics. Zero Trust means dynamic verification and establishing normalcy so that the abnormal stands out more quickly.

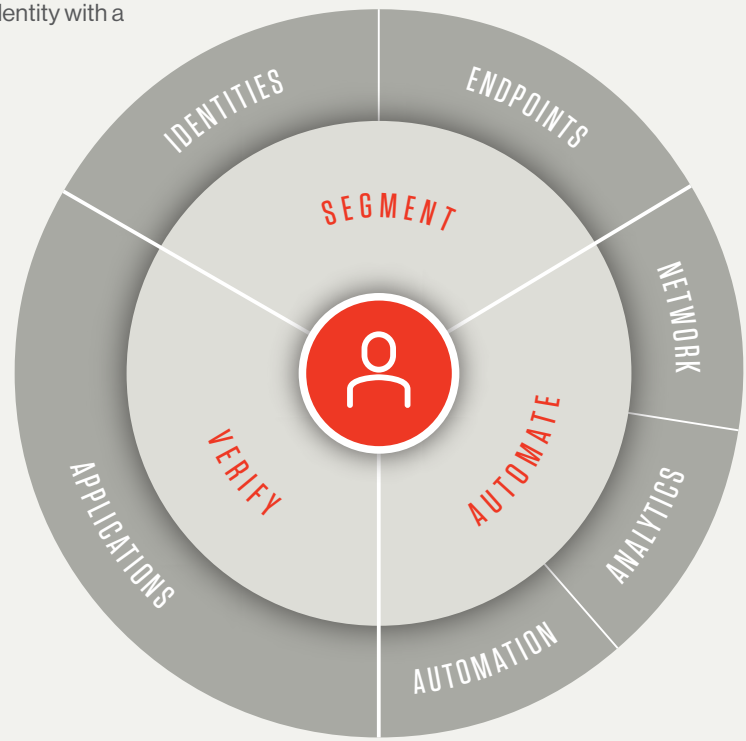
- **All resource authentication and authorization are dynamic and strictly enforced before access is allowed:** Continuous monitoring of authentication requests, access patterns, and behavior analytics are used to enforce Conditional Access (e.g. step up authentication using MFA). Falcon Zero Trust can extend MFA and SSO tools previously limited to cloud resources back into the network, offering legacy and proprietary resources the same rigor and level of access enforcement. Falcon Zero Trust's risk-based Conditional Access ensures frictionless user experience by triggering MFA only when the risk increases. Whether you have one site or multiple offices, Falcon Zero Trust offers consistency of policies, applications, and controls that won't slow business down by adding constant re-authentication for routine tasks with common sources and destinations.
- **The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture:** Falcon Zero Trust continuously collects data about access authentication and authorization requests, credentials, access patterns, resources accessed, endpoints used, and so on. Falcon Zero Trust offers a baseline of a 90-day window, in which the system relearns and adjusts the baselines on a cycle to improve authentication strategies, policy creation, enforcement, and the overall security posture of the enterprise.

CROWDSTRIKE'S FRICTIONLESS ZERO TRUST APPROACH

Falcon Zero Trust envelopes every workforce identity with a perimeter, and:

- Secures access to all resources from humans and programmatic accounts
- Enforces access control based on identity and the device used for access
- Audits all authentication traffic in real-time
- Automates and adapts policies in tune with changing behavior baselines
- Offers users options in terms of how to most effectively execute their step-up authentication

Adhering to Zero Trust's basic principle, the risk scores are developed inside-out around user roles, user-defined authentication policies, and the identity store instead of the traditional outside-in sources.



RISK-BASED CONDITIONAL ACCESS

Risk is a constantly changing score. When a user comes on board, or changes roles and teams, their behavior and access needs are going to be in motion. Working from home has changed the standard login hours for countless around the globe, and remote working includes anywhere that WiFi or mobile hotspot can afford.

Falcon Zero Trust performs user modeling of the user and their behavior as well as qualities of the session and endpoint, pulling many kinds of data from multiple sources to create a risk score for each user in the organization. This risk-based score acts as a gating decision point for step-up identification via MFA, in a way that's easier for users than a constant or absolute Challenge:Pass or Challenge:Fail.

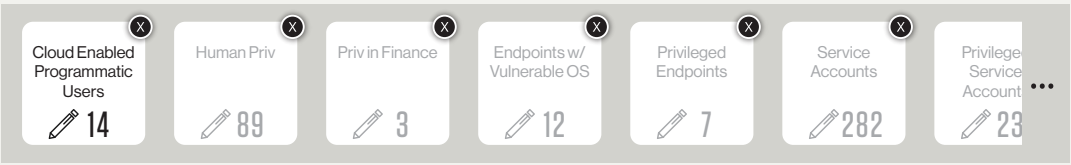
To apply this security assurance without a constant user friction, Falcon Zero Trust collects the context of each request to compare that activity against that user (and/or their group) baseline of activity. Falcon Zero Trust creates a dynamic fingerprint of that user within the system: Is it common for this user to travel? Has the user been seen recently from other locations? What is the reputation of the originating IP address and other characteristics of the VPN session (e.g. servers accessed, volume of outbound traffic) and user (e.g. its business role)?

Constant challenge for login/password/MFA cycle multiple times in a day or session can wear on the user. With risk-based conditional access, Falcon Zero Trust gathers User Pattern Data and assesses actual risk by changes in behavior or anomalous detection. Then it sifts through the pattern of collected activities and authentications on the network to detect indications of malicious activity.

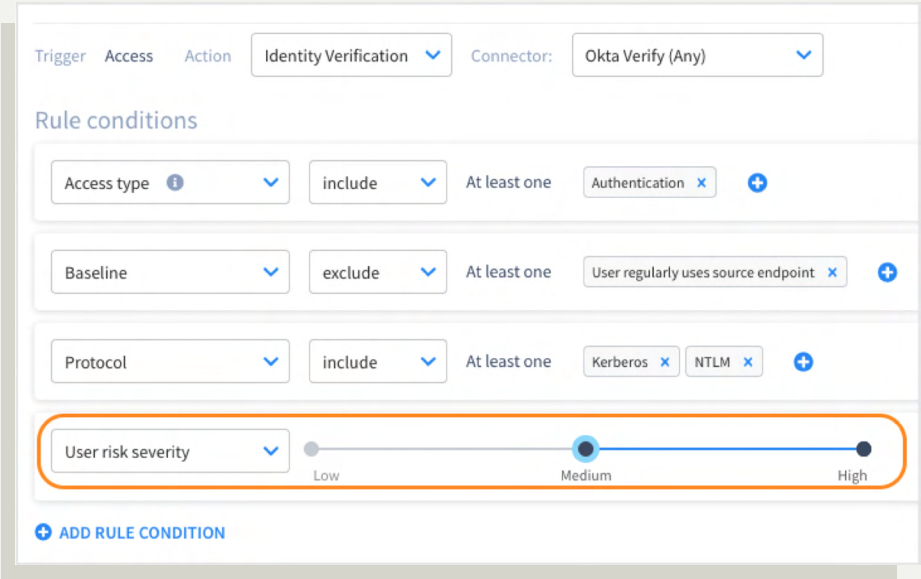
Falcon Zero Trust risk scoring adds a layer of security and automation to the identity and access management services, enhancing the MFA challenges with actionable data that is easy for users to embrace – because until the action is an anomaly, the challenges are fewer and the password fatigue is lower across the enterprise.

Falcon Zero Trust performs user modeling of the user and their behavior as well as qualities of the session and endpoint, pulling many kinds of data from multiple sources to create a risk score for each user in the organization.

CONDITIONAL ACCESS POLICIES FOR SEGMENTATION



There are multiple ways you can address conditional access and segmentation: By risk score, by thresholding, by rules by group or asset, or signature detection. Each of these contains granular options according to the organization, group, domain, and conditions of the identity attempting to access.



Some of the rules in the detection engine are static and based on known attack patterns and signatures. Obviously, signature-based rules are not sufficient to detect sophisticated attacks, and as a result the Falcon Zero Trust detection engine employs a variety of anomaly detection algorithms. These models run as a tuned ensemble and can detect various types of malicious activities such as privilege elevation, lateral movement, geographic anomalies, and more.

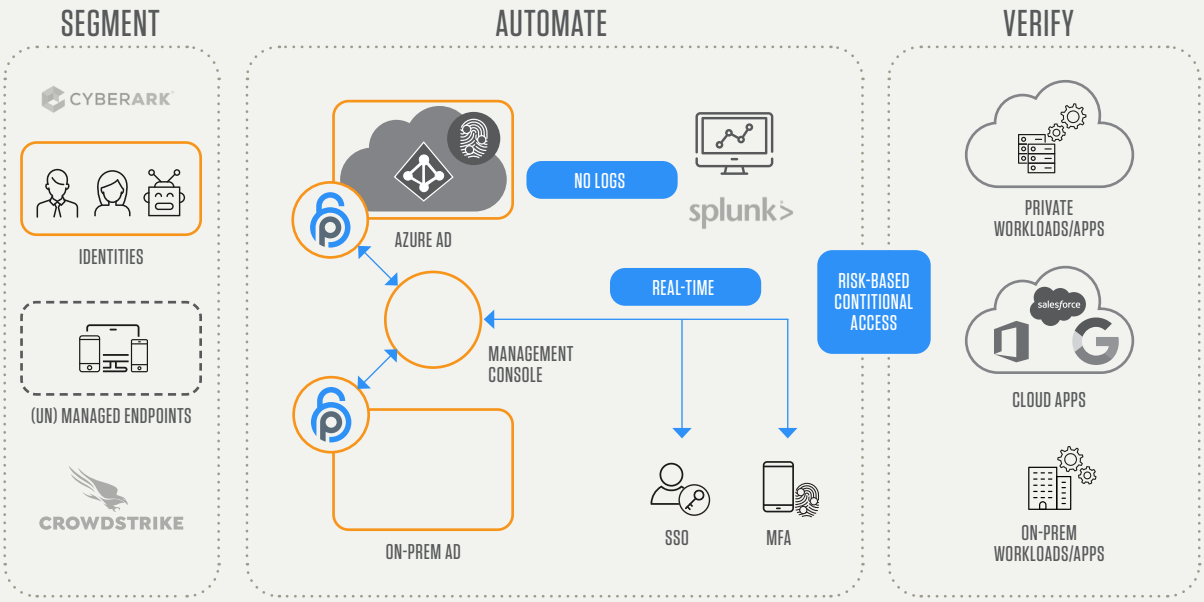
OPERATIONALIZING ZERO TRUST WITH FALCON ZERO TRUST

The Falcon Zero Trust approach to authentication allows you to standardize how your enterprise handles identity store risk. The three organizational steps of operationalizing a Zero Trust strategy are Adoption, Implementation, and Maintenance.

Falcon Zero Trust is quick to set up and offers near immediate risk assessment and identification of weakness. The time to value lies in hours to understand your total identity store census – users, privileged users, shadow users, and service accounts along with each of their respective weakness or lack of use.

Falcon Zero Trust integrates with current security stacks, adding risk score and real time information to make other solutions smarter, and extend their reach. Falcon Zero Trust with Password Access Management solutions automates password rotation, allowing one interface to help enterprises quickly identify all outliers and comply with regulation. Falcon Zero Trust works with all the major MFA vendors, extending their reach both in the cloud and to on premises resources, even legacy systems – without causing password fatigue on the part of the users. With plug ins for all the SSO vendors, the solution allows for customer choice for authentication, providing full visibility, risk, and threat detection to SSO activities without an endpoint agent required. Falcon Zero Trust even has plugins to some of the major Security Orchestration, Automation, and Response (SOAR) vendors and SIEM systems – providing detailed contextual information about any IP and device, the user accounts associated with it, and known threats. For the experienced SIEM or SOC analyst, Falcon Zero Trust provides APIs in CEF and LEEF format to help build rules and events of interest.

DEPLOYMENT MODEL



Phase 1

Falcon Zero Trust sensors on the Domain Controller and adapters on the cloud for federation services (e.g. ADFS, PingFederate, Okta, Azure AD, etc.) provide additional visibility into cloud users and their roles. This also adds threat detection capabilities like risky geo-location and policy deviations by building behavior baseline. The solution can provide data back to the identity federation service in the form of a user risk score, or it can take action directly via policy. Falcon Zero Trust has API based connectors and the ability to control activity on other SSO platforms with minimal additional effort. Deployment of the management and data collection can be completed in a half day. Customers gain immediate value from the added visibility into their users and begin to reduce their attack surface.

Phase 2

By installing sensors on Active Directory Domain Controllers, alongside the management appliance and cloud adapter, Falcon Zero Trust provides intelligent Conditional Access with full visibility and control, on-premise and clouds, to detect and stop sophisticated threats on credentials and the identity store along the MITRE ATT&CK kill chain - for example, privilege escalation (credential spray, brute force, compromised passwords), lateral movement (PowerShell, Pass the Hash (PtH), Golden Ticket, RDP), NTLM relay attacks and others throughout the MITRE ATT&CK framework.

Phase 3

Identity store enforcement, the full power of Falcon Zero Trust is now available to enterprises. When there is a suspicious or malicious activity, Falcon Zero Trust holds the access request. Depending on the adaptive policy, the user can be challenged via a variety of real-time mechanisms on any network resource (including PowerShell, RDP, folders, etc.) with MFA, Email, SMS, or even block, or just alert. Falcon Zero Trust supports a dozen commercial MFA solutions, including but not limited to Duo, Azure MFA, RSA SecurID, CA, Symantec, Okta, and more, with various authentication methods from Fast Identity Online (FIDO) tokens, through phone calls, interactive OTP, and up to the common push method.

CONCLUSION

Falcon Identity Protection supports the frictionless Zero Trust initiative, which in the end benefits all stakeholders in the system – employees, support teams, and other shareholders in the identity store. Focusing on identity-centric security supports mission-critical functions and fulfills the security business requirements without disrupting the core competencies of the enterprise.

Zero Trust success can be measured in three ways:

- The workforce experience – Providing consistent or improved user experience across all channels and touchpoints in the organization
- Operational efficiency – The drive to streamline operations, reduce risk, and lower overhead in time, human resources, and money
- Reduction in risk immediate and over time – Whether measured by domain, organization, or individuals, it's important to track improvement in your risk scores. Whether by having fewer incidents or a lower score, or simply tracking fewer support tickets and incidents, Zero Trust is about reducing risk and helping you get back to your core business.

No network starts out to be complex. Security stacks grow as the business grows – but need a serious architectural review when considering Zero Trust initiatives. As organizations change through; growth, absorbing other companies and groups, migrating all or partially to the cloud, business

transformation, streamlining legacy systems, or embracing new automation; a strategy of Zero Trust, Zero Friction is consistent across any board initiative. Falcon Identity Protection can help your security transformation match your Zero Trust initiatives, with less hassle to your workforce.

Falcon Identity Protection can help your security transformation match your Zero Trust initiatives, with the least friction to your workforce.

SOURCE:

1. https://www.ibm.com/security/data-breach

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.

https://www.crowdstrike.com/products/identity-protection