INTRODUCTION

Organizations accelerating digital transformation initiatives while increasing the size of remote workforces experience a parallel increase in advanced attacks that leverage endpoints, user credentials and workloads. Enterprises understand that building a Zero Trust Architecture is a necessary strategy, but ask: “How do we start the journey and operationalize the framework?”

Zero Trust is not a one-stop solution. It is a security model built on the basic principle of explicitly verifying each and every access request that may originate from inside or outside the enterprise, and is not limited by vendors and platforms used in on-premises and cloud environments.

According to the NIST 800-207 publication, Zero Trust has been envisioned as trust none unless otherwise explicitly allowed — that is, user accounts, endpoints and other assets are stripped of the implicit trust that is tied to physical location or network location or that is based on whether they were managed or unmanaged by the enterprise.

TRADITIONAL ZERO TRUST IS HARD TO OPERATIONALIZE

Traditional Zero Trust solutions are built with several siloed security tools to protect user endpoints, workloads and user access to applications. Common challenges include:

- **Old architecture that doesn’t scale:** Perimeter-based solutions such as hardware firewalls, VPNs, NAC and VLANs are less effective today than over a decade ago in flat networks. Endpoints, users, applications, resources and data exist not only inside the enterprise perimeter, but also in multi-cloud environments.

- **Dynamic state of security defeats static policies:** Policies defined through firewall rules, VLAN ACLs and VPNs are rigid. With an explosion of remote and cloud users and applications, static policies slow the organization’s capability to rapidly adapt to change, where change is the new constant involving behavior, risks and analytics.

- **Hindered security visibility and posture:** Integrating siloed security tools across hybrid enterprises is a challenge, which can increase the blast radius in case of an attack. According to a recent IDG survey¹, despite increased IT security spending, almost 80% of IT leaders lack confidence in their enterprise’s security posture.

- **Negative impact on user experience (UX):** The impact on UX is not just for end users, but also for IT and security teams that are tasked with implementing digital transformation and protecting the enterprise from malicious actors.

- **Increase in operational complexity and costs:** The inter-connectedness and distribution of users, data, applications and devices means that enterprises face expensive investment in log management tools, hardware and software. IT and security teams therefore contend with cumbersome log analysis, manual threat correlations and rules, and complex policies to enforce Zero Trust.

¹ Cybersecurity at a Crossroads: The Insight 2021 Report
WHAT IS FRICTIONLESS ZERO TRUST?

When IT and security teams start a security project, friction arises from added costs and deployment and operational complexity. Budgetary constraints make it difficult for CISOs to meet security goals and ensure that the tool is adopted by users. If the security tool impacts the user experience, it decreases productivity and increases security compromises (e.g., a bad user experience from MFA fatigue could lead to a security compromise when a user inadvertently accepts the MFA challenge triggered by a malicious activity). Security teams not only must deal with an extra security tool, but may also have to manage alerts and log repositories, write correlation rules and deal with false positives.

CrowdStrike provides a frictionless Zero Trust approach for enterprises that reduces costs and operational complexity. CrowdStrike maximizes Zero Trust security coverage across hybrid environments and does all the heavy lifting for security teams to enforce frictionless policies with the industry leading CrowdStrike Security Cloud.

The CrowdStrike Zero Trust solution is built around:

1. The ability to stop breaches in real time for any endpoint, workload or identity and reduce the blast radius across on-premises and cloud data centers
2. High fidelity attack correlation and policy enforcement to realize frictionless Zero Trust journey for users, IT and security teams
3. A unified, cloud-native approach that removes the overhead of managing TBs of data, threat feeds, hardware and software, and ongoing personnel costs

THE FRICTIONLESS ZERO TRUST JOURNEY WITH CROWDSTRIKE

Zero Trust is not a one-stop solution for enterprises but a set of principles that aim to move security closer to the resources that are being protected (i.e., endpoints, workloads and identities).

Several well-defined Zero Trust frameworks exist in the industry. There is the Zero Trust eXtended (ZTX) ecosystem framework from Forrester, Gartner’s Continuous Adaptive Risk and Trust Assessment (CARTA) strategy and the NIST SP 800-207 framework. CrowdStrike most closely follows the NIST SP 800-207 framework, widely followed in the public and private sectors, to enable security in the cloud-first, work-from-anywhere environment.

---

2 National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture
KEY PRINCIPLES OF THE NIST ZERO TRUST FRAMEWORK

- **Understand Behavioral Data:** Use behavioral attributes to understand if the users are accessing the applications or resources they are supposed to access. Is there protocol misuse such as a regular user doing Remote Desktop Protocol (RDP) to a Domain Controller (DC)? Is there suspicious behavior using privileged credentials?

- **Limit the Attack Surface with Segmentation:** Limit the scope of what applications can do; control where regular users, third-party contractors and privileged users can go; and limit what service accounts can access with segmentation. Apply the principles of least privilege and dynamic risk assessment to reduce the attack surface.

- **Automate Security Tied to Context:** Use signals from users, devices, networks and workloads to gain unified visibility, improve analytics, enforce policies and automate security — all tied to context to improve the fidelity of alerts and incident response.

- **Continuously Verify Access with the Least Friction:** Verify every access to applications, resources and workloads with deep knowledge of the risks and deviations, and not based on trust or access time-outs (i.e., continuously monitor what’s happening even after granting access to a resource). The key is to verify access continuously without degrading the user experience or affecting business productivity.

CROWDSTRIKE ZERO TRUST MATURITY JOURNEY

Most enterprises that want to adopt Zero Trust or are in different stages in the Zero Trust journey want to accomplish maximum protection of a major portion of their hybrid enterprise. At the same time, enterprises want to accomplish Zero Trust with reduced complexity and costs and the least disruption to business productivity.

CrowdStrike's frictionless Zero Trust solution aligns with the key principles described above to realize maximum coverage across hybrid enterprises by protecting endpoints, identities, and applications and workloads.
The CrowdStrike Zero Trust journey involves just two components: the **CrowdStrike Falcon® sensor/agent** and the **CrowdStrike Security Cloud**.

- Falcon sensors/agents can be deployed at scale and in hours, not days.
- The CrowdStrike Security Cloud provides security automation and analytics to intelligently enforce policies with the least friction for users, IT and security teams.
- With the industry-leading sets of endpoint, workload, container and identity telemetry, threat intelligence and AI-powered analytics, security teams can automatically predict and prevent modern threats in real time.
- CrowdStrike’s cloud-native approach is the only solution that empowers security teams to achieve Zero Trust protection without the combined overhead of managing terabytes of data, threat feeds, hardware and software, and related ongoing personnel management costs.

**NIST Mapping with CrowdStrike Components: Sensor/Agent and Security Cloud**

- **Control Plane**
  - Policy Engine
  - Policy Administrator

- **Security Cloud**
  - Policy Enforcement

- **Data Plane**
  - Untrusted
  - Trusted

- **Control Plane**
  - Endpoint Agent/Sensor
  - Workload Agent/Sensor

- **Data Plane**
  - Enterprise Resource

- **Adoption**
  - Discover endpoints, identities, applications
  - Protect endpoints, identities, workloads in real-time with behavioral & real-time analytics
  - Automatically segment identities
  - Enrich telemetry with threat context & intel

- **Protection**
  - Enhance UX with intelligent conditional access
  - Extend MFA to improve security coverage
  - Assess and share endpoint security posture
  - Unlock the full potential of frictionless Zero Trust with CrowdStrike Zero Trust Ecosystem partners

- **Mitigate**
  - Discover endpoints, identities, applications
  - Protect endpoints, identities, workloads in real-time with behavioral & real-time analytics
  - Automatically segment identities
  - Enrich telemetry with threat context & intel

- **Visualize**
  - Discover endpoints, identities, applications
  - Visualize attack paths
  - Discover & assess multi-cloud workloads

- **Optimize**
  - Enhance UX with intelligent conditional access
  - Extend MFA to improve security coverage
  - Assess and share endpoint security posture
  - Unlock the full potential of frictionless Zero Trust with CrowdStrike Zero Trust Ecosystem partners

_The CrowdStrike Zero Trust Journey_
Visualize

With an increase in remote workstyles, employees are accessing internal resources, workloads and applications from outside the enterprise security infrastructure and from their own devices — which may not be managed by the enterprise. Without unified visibility, IT and security leaders have no way of seeing the gaps resulting from remote users and service accounts spread across multi-directory environments (e.g., Microsoft AD, Azure AD or an SSO such as Okta) and logging in from managed or unmanaged endpoints to access multi-workloads and applications.

At any time, IT security teams should know who their users are, if they are privileged, whether service accounts are performing interactive logins, why a particular endpoint is exhibiting suspicious behavior, and so on. Most vendors provide visibility on specific areas such as endpoints, identities or multi-clouds. However, getting that visibility in a central dashboard across all of these entities is hard, but essential to Zero Trust.

One of the core values of a Zero Trust solution is to provide visibility of all possible attack paths across the hybrid enterprise. Such visibility should cover critical workloads and applications as well as identities — such as office users, remote users, and service and privileged accounts across multiple identity stores — that are accessing the workloads and applications using endpoints including unmanaged devices.

Mitigate

As the world learned with Sunburst in December 2020, a seemingly normal software update can be a vector for a malicious payload, which can move laterally to critical resources in your enterprise by leveraging valid user credentials and endpoints. To detect this lateral movement, security analysts usually have to rely on time-consuming and cumbersome log analysis — that is, if they see indicators of compromise (IOCs) and know what they are hunting for in the first place. In hybrid enterprises, the security tools that work for on-premises may not work in the cloud, allowing lateral movement attacks to go undetected until it’s too late. Sophisticated hackers using valid user credentials often remain undetected, and then successfully exfiltrate critical data back to their command and control servers.

Malware and ransomware adversaries pose a silent yet significant threat to enterprises using sophisticated tactics, techniques and procedures (TTPs). Hackers and state-sponsored bad actors leverage the gaps in security, integration challenges and the lack of a single source of truth to deploy malware and ransomware exploits to disrupt business critical applications or to steal intellectual property (IP) information.

Upon getting visibility into the possible attack paths with CrowdStrike Zero Trust, security teams put controls in place to prevent the attacks in real time, and also to comply with regulatory standards. Automating analytics based on hundreds of behavior signals, user risks, device risk posture and the overall Active Directory and endpoint hygiene improves the fidelity of the data. Security analysts can consume the accuracy of correlations to create simple policies for enforcement and to maintain the risk posture of the enterprise.
Automatic segmentation, as noted above in the key principles, limits the attack surface and the number of policies required to enforce security (as opposed to network micro-segmentation techniques). Old school network segmentation requires multiple internal firewalls (physical or virtual) and tends to, at best, wrangle IP lists or all or none traffic choices. Microsegmentation by user groups is often time-consuming if done manually, or at worst unachievable with traditional network tools. When discussing tying security automation to user context, security teams should not only be able to export contextual data to a preferred security information and event management (SIEM) or security orchestration, automation and response (SOAR) solution, but also consume data from them, if necessary, to improve the fidelity of the incident information for effective real-time response.

**Optimize**

Limiting users’ access to applications using VPNs and firewalls will affect the overall productivity and UX, while being ineffective at protecting the enterprise from sophisticated threats. For example, if to prevent lateral movement threats security teams challenge users by triggering identity verification (e.g., MFA) every time they try to access a resource, workforce productivity will diminish. (Note that this will not necessarily stop the lateral movement attack, for a user that just passed the MFA challenge may still download a malicious email attachment and set off the lateral movement process).

The ability to collect and correlate behavior and risks in real time — from identities, multi-directory identity stores such as Microsoft AD/Azure AD, multi-cloud workloads, and managed or unmanaged endpoints — as a single source of truth using massive databases, siloed log repositories and threat intelligence can increase costs and complexity. The CrowdStrike Security Cloud enables security teams to visualize and stop breaches in real time and tied to context. CrowdStrike’s adaptive conditional access helps enterprises realize proactive security and confidently move away from reactive techniques. Adaptive conditional access is based on risk and deterministic signals. For example, to prevent lateral movement threats, users are challenged only when there’s suspicious behavior or deviation from their baselines, and from signals from compromised endpoints. As opposed to the traditional approach of triggering MFA every time, the CrowdStrike approach, with high-fidelity incident data and policy automation, ensures secure access to critical resources without degrading users’ experience. CrowdStrike protects workloads and on-premises/SaaS applications distributed across hybrid enterprise with continuous identity verification when accessed by regular, privileged and service accounts.

CrowdStrike Zero Trust extends coverage for enterprises to reduce risk through API and pre-integrations. This includes addressing risk factors such as legacy systems, deprecated authentication protocol use, proprietary applications and SaaS apps, as well as unmanaged devices used by third-party vendors and contractors. With broad API support, security teams can integrate their favorite security tools such as SIEM and SOAR solutions. In addition to APIs, CrowdStrike Zero Trust Assessment (ZTA) provides pre-integrations with the CrowdStrike Zero Trust ecosystem partners including Zscaler, Okta, Proofpoint and Netskope.
WHY CROWDSTRIKE ZERO TRUST?

The CrowdStrike Security Cloud does the heavy-lifting to reduce the complexity of the Zero Trust journey. By eliminating the need to rip and replace existing IT infrastructure and security tools, enterprises can save money and provide a frictionless experience for users, IT and security teams.

KEY BENEFITS

<table>
<thead>
<tr>
<th>Industry’s Only Real-time, Cloud-native Zero Trust Solution</th>
<th>Industry’s Highest-fidelity Attack Correlation and Frictionless Policy Enforcement</th>
<th>Reduced Costs and Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrowdStrike Zero Trust’s fast detection and response is powered by industry’s largest Security Cloud built around machine learning (ML) models fed by over five trillion events per week. The cloud-delivered Zero Trust model increases visibility and coverage across hybrid enterprise infrastructure. This enables seamless scaling up as the Security Cloud data, analytics and integration grows through technology partners and APIs.</td>
<td>CrowdStrike Threat Graph™ database automatically collects petabytes of data with the most effective, automated detection and prevention in real time, driven by the largest TTPs and IOCs database, alongside hundreds of behavioral, deterministic and identity analytics. Continuous identity verification is through the adaptive conditional access approach ensuring easy user experience that translates to increased security adoption and decreased security operations center (SOC) costs.</td>
<td>CrowdStrike Zero Trust solution reduces the overhead for security teams as it requires only two components: the Security Cloud and the sensor. The enterprise can reduce traditional Zero Trust security investments in managing massive log repositories, external threat feeds, and hardware, storage and software costs. With identity-based segmentation combined with the real-time data and ML models, the enterprise benefits from easy policy deployment for all IT assets.</td>
</tr>
</tbody>
</table>

COMMON USE CASES

CrowdStrike enables enterprises to adopt Zero Trust with a clear understanding of who is trying to access what and why they should be given access. This is possible with CrowdStrike Security Cloud doing the heavy lifting, by combining signals and contextual information from the entities in hybrid environments.

The CrowdStrike Zero Trust solution can protect enterprises against a variety of sophisticated threats. The following highlights some common use cases.
MITIGATING SOFTWARE SUPPLY CHAIN ATTACKS

**Breach:** A threat actor can compromise a vendor’s software update package to gain entry into an enterprise’s IT environment. The threat actor then uses the compromised service account that is used to run the software update package to move laterally and identify privileged users. These privileged user accounts can be used by the threat actor to gain access to critical resources in the enterprise and exfiltrate data to the command and control server.

**Response:** The CrowdStrike Zero Trust solution will detect this activity early using identity segmentation along with risk-based behavior analytics and granular visibility into identity-related lateral movement threats such as Pass the Hash (PtH) and persistence methods such as Golden Ticket attacks. Upon detecting this anomalous behavior, the threat actor will be challenged with forced identity verification.

PREVENTING RANSOMWARE THREATS

**Breach:** Ransomware threats such as Maze can infect an unsuspecting employee’s endpoint through a malicious payload via email. If the user of this endpoint has logged into the enterprise’s IT and support systems, PtH can be used to harvest credentials from the Local Security Authority Subsystem Service (LSASS). PtH is an effective technique and is very hard to detect and prevent.

**Response:** The CrowdStrike Zero Trust solution protects enterprises from ransomware attacks in several ways. When the email with the malicious payload is opened by the employee, one of CrowdStrike’s Zero Trust ecosystem partners — Proofpoint — can detect this threat. If the malware or ransomware gets executed on the endpoint CrowdStrike’s powerful endpoint protection will detect and prevent this breach in real time. If this malware tries to move laterally in the network, CrowdStrike Falcon Identity Protection detects this as a suspicious movement, even with valid credentials, because the account is trying to do an action that’s outside established baselines (e.g., logging in to a DC from a new or different endpoint) and with an increased risk score. The account will be challenged with an MFA or simply blocked, effectively stopping the attack.

STOPPING WORMABLE EXPLOITS

**Breach:** By potentially compromising non-monitored service accounts (i.e., programmatic accounts), wormable exploits such as EternalBlue compromises Microsoft Windows systems and moves machine to machine across the enterprise.

**Response:** The CrowdStrike Zero Trust solution proactively protects the enterprise from wormable exploits by detecting and mitigating lateral movement through segmentation or monitoring credential behavior to determine the access deviations and the change in risk. CrowdStrike Zero Trust enables simple policies to be defined to prevent service accounts from logging on to DCs using RDP, trigger MFA for stale human and service accounts and extend MFA to legacy applications.
NEXT STEPS

The quest for a Zero Trust architecture cannot be satisfied by a single product or a one-stop solution. It’s a security model that offers enterprises the appropriate controls to assess security gaps and proactively detect and prevent threats in real time, with improved UX for users, IT and security teams. A Zero Trust journey need not involve complex technologies, heavy capital investment or “rip and replace” projects.

For more information on getting started with the CrowdStrike Zero Trust maturity journey, visit [www.crowdstrike.com/zero-trust/](http://www.crowdstrike.com/zero-trust/).

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There’s only one thing to remember about CrowdStrike: **We stop breaches.**

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)

© 2021 CrowdStrike, Inc. All rights reserved.