CrowdStrike White Paper

CROWDSTRIKE

STREAMLINE YOUR ZERO TRUST JOURNEY

Accelerate risk reduction with a standards-based, cloud-native solution

EXECUTIVE SUMMARY

Digital transformation has fundamentally changed how enterprises deliver and consume business applications and IT services. No longer confined to the office, today's employees work from any place, at any time, using a mix of legacy applications and cloud-based solutions. At the same time, adversaries have accelerated the speed and complexity of modern attacks — taking advantage of the challenges in defending complex IT environments and using machine learning (ML) techniques similar to those used for protecting them. Forward-looking enterprises are seeking new, actionable Zero Trust models to secure today's hybrid IT environments and cloud-first users against modern-day attacks.

A Zero Trust security model presumes every user and every device is a potential threat at all times. Zero Trust security solutions ensure users are authenticated, authorized and continually validated, protecting both on-premises and cloud-based resources against both internal and external threats.

This white paper reviews Zero Trust principles and architectural and implementation guidelines, and explains how CrowdStrike's frictionless Zero Trust approach can help make your Zero Trust journey effective and achievable so you can accelerate risk reduction and make the most of your existing technology investments.

THE NEED FOR A MODERN APPROACH TO SECURITY

Cloud transformation and the adoption of remote work create new opportunities for threat actors and new challenges for enterprise security, compliance and risk management professionals. Supply chain attacks like SUNBURST, ransomware exploits like Ryuk and GoldenEye, and vulnerabilities like Log4Shell demonstrate the futility of traditional perimeter-based defenses in the digital era.

External attackers and malicious insiders can exploit compromised credentials and other security vulnerabilities to penetrate networks (potentially within minutes), elevate privileges and rapidly move laterally to disrupt business-critical systems and steal confidential data. In fact, according to the **CrowdStrike 2022 Global Threat Report**, nearly 80% of cyberattacks leverage identity-based attacks to compromise legitimate credentials and use techniques like lateral movement to quickly evade detection.

Digital transformation requires a modern approach to security that adapts to modern threats while still enabling business productivity. A Zero Trust model discards outdated notions of a defendable network edge and assumes all users and applications must be authenticated, authorized and continuously validated.

When it comes to Zero Trust, not all vendors take the same approach. Some security vendors are simply repurposing their legacy virtual private network (VPN) solutions as Zero Trust Network Access (ZTNA) solutions.[1] Forward-thinking organizations are pursuing broader, standards-based Zero Trust solutions, built from the ground up to fully protect today's hybrid, multicloud environments and today's cloud-centric, hybrid workforces. The latter's approach

1. ZTNAs tunnel traffic just like a VPN. While VPNs give users access to all network resources and services, ZTNAs give users access to a defined set of resources and services.

takes into account evolving adversarial tactics and techniques to proactively protect the organization from modern attacks like ransomware and supply chain threats.

Best-of-breed Zero Trust solutions are easy to deploy, administer and extend, and provide comprehensive identity-based access controls and data protection functionality to defend against the supply chain attacks, ransomware and identity-driven exploits that dominate the modern threat landscape. The best Zero Trust solutions support adaptive, risk-based conditional access controls for people, applications and devices to positively identify users without impairing user experience or hampering worker productivity. And they employ cloud-based artificial intelligence and machine learning to detect advanced attacks and automate threat mitigation without on-premises equipment costs or threat-hunting operational hassles.

THE GOLD STANDARD SECURITY ARCHITECTURE FOR THE DIGITAL ERA

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 has emerged as the de facto standard Zero Trust architecture. U.S. government agencies and large and small enterprises worldwide are adopting it. The NIST Zero Trust architecture takes a vendor-neutral, end-to-end approach to security that focuses on continually validating identities, tightly restricting privileges and strictly controlling access to enterprise resources. A standards-based approach ensures enterprises need not re-architect their Zero Trust solution when changing vendors or business goals. The NIST architecture defends against both insider threats and external adversaries, limits privilege creep and lateral movement, and protects confidential data and critical infrastructure, regardless of location or deployment model.

SP 800-207 explains the basic tenets of a Zero Trust framework, defines the logical components that make up the architecture, reviews typical deployment scenarios and provides guidance for migrating to a Zero Trust model. As shown in Figure 1, the SP 800-207 reference architecture includes a policy enforcement point (PEP) that controls access to enterprise resources based on dynamic business rules maintained in a policy decision point (PDP). The core PEP and PDP components leverage external data sources such as continuous diagnostics and mitigation (CDM) systems, threat intelligence databases, identity management solutions, and security information and event management (SIEM) systems to assess risks and manage access.

The Zero Trust system authenticates and authorizes subjects (users and applications) in real time when they try to access enterprise resources (e.g., endpoints, data, applications). It uses behavioral data and contextual information (e.g., device characteristics, geo location data, historical user behavior) to strengthen access security and defend against fast-moving attacks such as identity-driven exploits like credential theft and impersonation.

By enforcing policies close to enterprise resources and continuously validating users and applications, the SP 800-207 architecture shrinks implicit trust zones, limits unauthorized access and minimizes the blast radius across on-premises and cloud data centers.

In May 2021, the Biden administration issued an **Executive Order on Improving the Nation's Cybersecurity** that mandated U.S. federal agencies adhere to NIST SP 800-207 and recommended that **private-sector organizations follow suit**. The Executive Order has increased awareness of the NIST framework and accelerated its adoption.

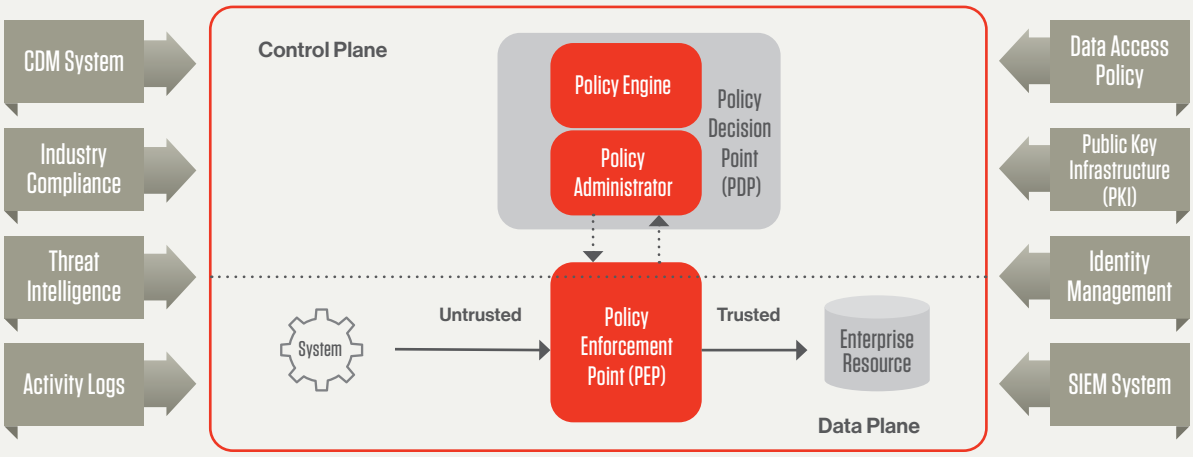

Figure 1. *NIST SP 800-207 core Zero Trust logical components*

MIGRATING TO A NIST SP 800-207 ZERO TRUST MODEL

Implementing a Zero Trust architecture is a process, not an event. By introducing Zero Trust constructs and elements gradually, in stages, enterprises can protect their highest-value and most vulnerable assets as quickly as possible and introduce additional protections and coverage over time. The phased approach helps minimize disruptions and protect and extend previous investments.

A typical Zero Trust journey begins by improving visibility into identity, endpoints, users, applications and data and associated risks across the hybrid, multicloud environment. The goal of this stage is to discover all endpoints and all human and non-human identities scattered across the entire extended enterprise, understand their roles and behaviors, assess threats, and identify security gaps and potential attack paths for threat actors.

The next phase involves detecting and stopping threats against high-value targets in real time. This stage introduces threat intelligence and risk assessment technology to automatically identify and mitigate malicious attacks. It also employs **identity segmentation** techniques to tightly control access to resources and prevent common breach techniques such as privilege abuse and lateral movement, with minimal operational overhead.

The final stage extends the Zero Trust protection model to additional enterprise resources and introduces adaptive multifactor authentication (MFA) methods to strengthen security and improve user experiences. This phase also incorporates external systems such as identity security solutions, continuous diagnostics and mitigation (CDM) platforms and SIEM.

Figure 2. *A typical Zero Trust journey*

ACCELERATING RISK REDUCTION WITH CROWDSTRIKE'S CLOUD-NATIVE SOLUTION

The **CrowdStrike Zero Trust solution** is built from the ground up to secure the modern enterprise by stopping breaches in real time on endpoints, workloads, data and identities, independent of location or network. The CrowdStrike solution includes a flexible policy engine to enforce risk-based, conditional access to on-premises and cloud-based resources. It employs world-class artificial intelligence (AI) and creates actionable data through the CrowdStrike Security Cloud. The solution identifies shifts in adversarial tactics, mapping tradecraft in the patented CrowdStrike Threat Graph®, automatically preventing threats in real time across CrowdStrike's global customer base.

The CrowdStrike solution follows the NIST SP 800-207 framework, radically simplifying Zero Trust deployment and dramatically accelerating time-to-value by delivering PDP and PEP functionality in the cloud (see Figure 3). Customers can deploy and gradually evolve the CrowdStrike solution to address new use cases without making changes to their network. Purpose-built in the cloud, with a single lightweight-agent architecture, the CrowdStrike solution minimizes operational expense and complexity; takes full advantage of cloud scalability, agility and economics; and frees up technical staff to focus on core business tasks.

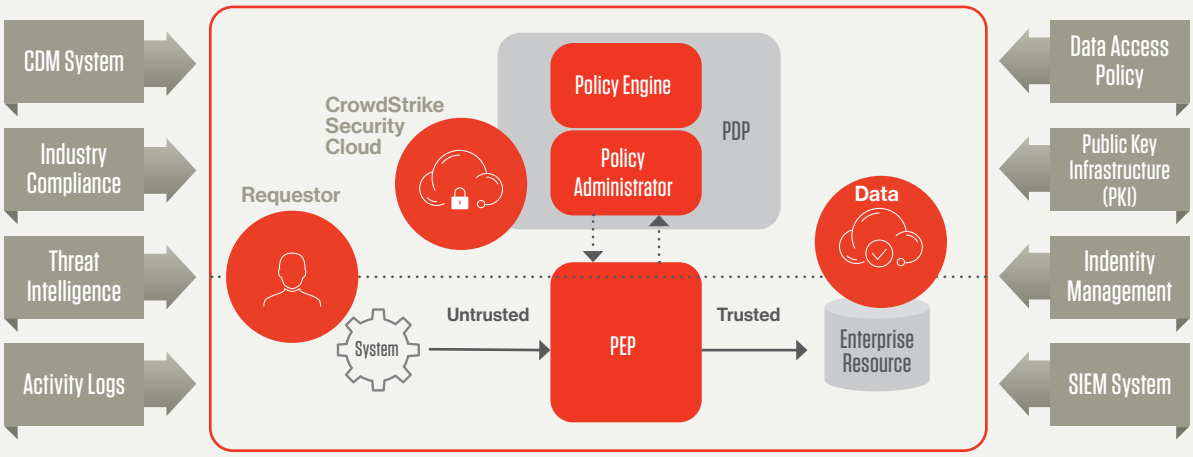

Figure 3. *CrowdStrike solution delivers NIST SP 800-207 PDP/PEP functionality in the cloud*

The CrowdStrike Zero Trust solution adheres to the key tenets of the NIST framework by:

- Using behavioral data and endpoint environmental attributes to validate identities and tightly control access to enterprise resources.
- Segmenting accounts and identities, and enforcing the principle of least privilege to limit an attack's blast radius.
- Seamlessly integrating with external systems for authenticating, authorizing and continuously validating requestors, without impairing the user experience or burdening security operations teams.
- Analyzing hundreds of signals from users, devices, networks, data and workloads in real time to gather security intelligence, improve the fidelity of alerts, automate remediation actions and accelerate mitigation efforts.

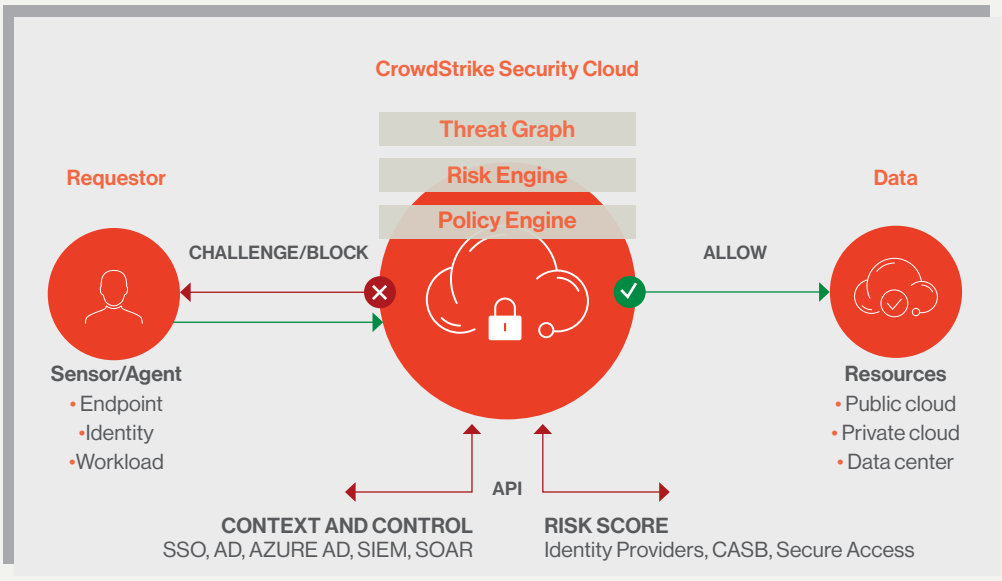

Figure 4. *The CrowdStrike Zero Trust solution combines universal sensor agents with cloud intelligence*

CrowdStrike's frictionless approach to Zero Trust includes two cloud-delivered components: the CrowdStrike Security Cloud and the CrowdStrike Falcon® sensor. The Falcon sensor is a universal lightweight agent that runs on a variety of endpoints, operating systems and identity stores including workstations, servers, virtual machines and virtual desktops, containers, mobile devices, Internet-of-Things (IoT) endpoints and directory services like Microsoft Active Directory. Designed for today's cloud-centric digital businesses, the Falcon agent requires no enterprise network or VPN connectivity, and supports traditional devices like PCs and bare-metal servers as well as virtual endpoints instantiated in private or public clouds.

The CrowdStrike Security Cloud combines a massively scalable threat intelligence database with AI-powered analytics to help detect, prevent, predict and mitigate advanced attacks and zero-day exploits. CrowdStrike's pioneering Threat Graph database, the brains behind the CrowdStrike Security Cloud, continuously ingests massive volumes of live telemetry data from Falcon sensors and other sources — at scale — enriched with contextual information to identify and stop threats. The CrowdStrike Security Cloud processes and correlates trillions of events, enabling high-fidelity attack correlation and real-time threat analytics and response. The CrowdStrike Security Cloud also includes an extensible policy engine that lets organizations control access to enterprise resources based on business rules and contextual factors.

The CrowdStrike Security Cloud provides application programming interfaces (APIs) for integrating third-party security solutions and homegrown security tools. Customers can use the APIs to incorporate contextual data or control information from external systems such as SIEM solutions, directory services platforms, and security orchestration, automation and response (SOAR) solutions. They can also use the APIs to gather risk assessment data from identity providers, cloud access security brokers (CASBs) and other external sources.

CrowdStrike offers off-the-shelf Security Cloud integrations with a variety of third-party solutions through the **CrowdStrike Store** and enables organizations to expand security coverage to areas like email security, your existing SIEM tools for log storage and compliance, and many more.

STREAMLINING YOUR ZERO TRUST JOURNEY WITH CROWDSTRIKE

CrowdStrike's cloud-native Zero Trust solution is incredibly easy to deploy, extend and scale. The solution includes only two components: the CrowdStrike Falcon sensor and the CrowdStrike Security Cloud.

CrowdStrike's cloud-delivered Falcon sensor agents are simple and non-disruptive to install, with no reboot required. Customers can deploy the Falcon sensor in minutes, easily onboarding tens of thousands of endpoints per day.

The CrowdStrike Security Cloud eliminates security infrastructure cost and complexity, with no on-premises technology to buy, operate, manage or scale.

With CrowdStrike, customers can introduce security controls in phases, on their own terms, to address their specific priorities, requirements and timelines. CrowdStrike delivers new capabilities and software updates to customers directly in the cloud for ultimate speed, flexibility and simplicity.

CrowdStrike's cloud-delivered solution streamlines the Zero Trust journey, making it easy to extend protection and expand coverage over time to tightly align investments with potential risk reduction benefits.

Stage 1: Visualize	Stage 2: Mitigate	Stage 3: Optimize
Discover all endpoints, identities, data and applications including managed and unmanaged endpoints, identity systems and human and programmatic credentials.	Protect endpoints, identities, data and workloads against ransomware, malware, fileless attacks and credential abuse.	Enhance the user experience with intelligent, risk-based conditional access based on contextual information, authentication patterns, behavior baselines, risk scores and other business rules.
Get full attack visibility across endpoints, identity stores, data, workloads and container environments. Unravel an entire attack happening across endpoints with an intuitive process tree.	Automatically detect and mitigate reconnaissance tactics, lateral movement, privilege escalation and other malicious activity.	Extend MFA and other controls to legacy systems, tools and applications to reduce attack surface.
Discover and assess multicloud workloads including context-rich metadata about system size and configuration, networking, and security group information for AWS, Azure and Google Cloud Platform.	Use a massively scalable AI/ML-powered threat intelligence database to improve fidelity and stop threats in real time.	Leverage APIs and prebuilt integrations to incorporate third-party security solutions and internally developed security tools.

Table 1. *CrowdStrike's three-stage Zero Trust journey*

KEY USE CASES

1. **Ransomware:** Ransomware threats such as Maze can infect an unsuspecting employee's endpoint through a malicious payload via email. Pass-the-hash (PtH) can be used to harvest credentials from the Local Security Authority Subsystem Service (LSASS) to enable attack progression. PtH is an effective technique and is very hard to detect and prevent.

   The CrowdStrike Zero Trust solution uses behavioral attributes, device posture, identity segmentation, security automation and risk-based conditional access to detect and stop malicious payload execution as well as lateral movement and attack progression using compromised credentials.

2. **Supply chain threats:** An adversary can compromise a vendor's software update package to gain entry into an enterprise's IT environment, or leverage compromised credentials from a vendor or third-party endpoint and enter the network.

The CrowdStrike Zero Trust solution provides visibility into endpoints, identities, data and cloud workloads, and the security context tied to these entities, and detects endpoint changes and the associated user behavior deviations and risk. Without requiring complex, manual log analysis and correlations, it helps your SOC teams detect adversary activity early using identity segmentation and prevents access to a vendor's software update package with risk-based MFA.

3. **Cyber insurance:** Adversaries can reduce an organization's insurability by increasing its risk exposure and response time to mitigate threats, resulting in monetary losses, lawsuits and damaged brand reputation.

   The CrowdStrike Zero Trust solution does the heavy lifting for security teams to assess and minimize ransomware risks in real time, and to improve the security posture for the enterprise. With industry-leading sets of endpoint, workload, data, container and identity telemetry, combined with threat intelligence and AI-powered analytics, security teams can automatically predict and prevent modern threats in real time, improving cyber insurability.

NEXT STEPS

To learn more about how CrowdStrike's standards-based, cloud-native solution can help you streamline your Zero Trust journey and accelerate risk reduction, visit **crowdstrike.com/zero-trust**.

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**