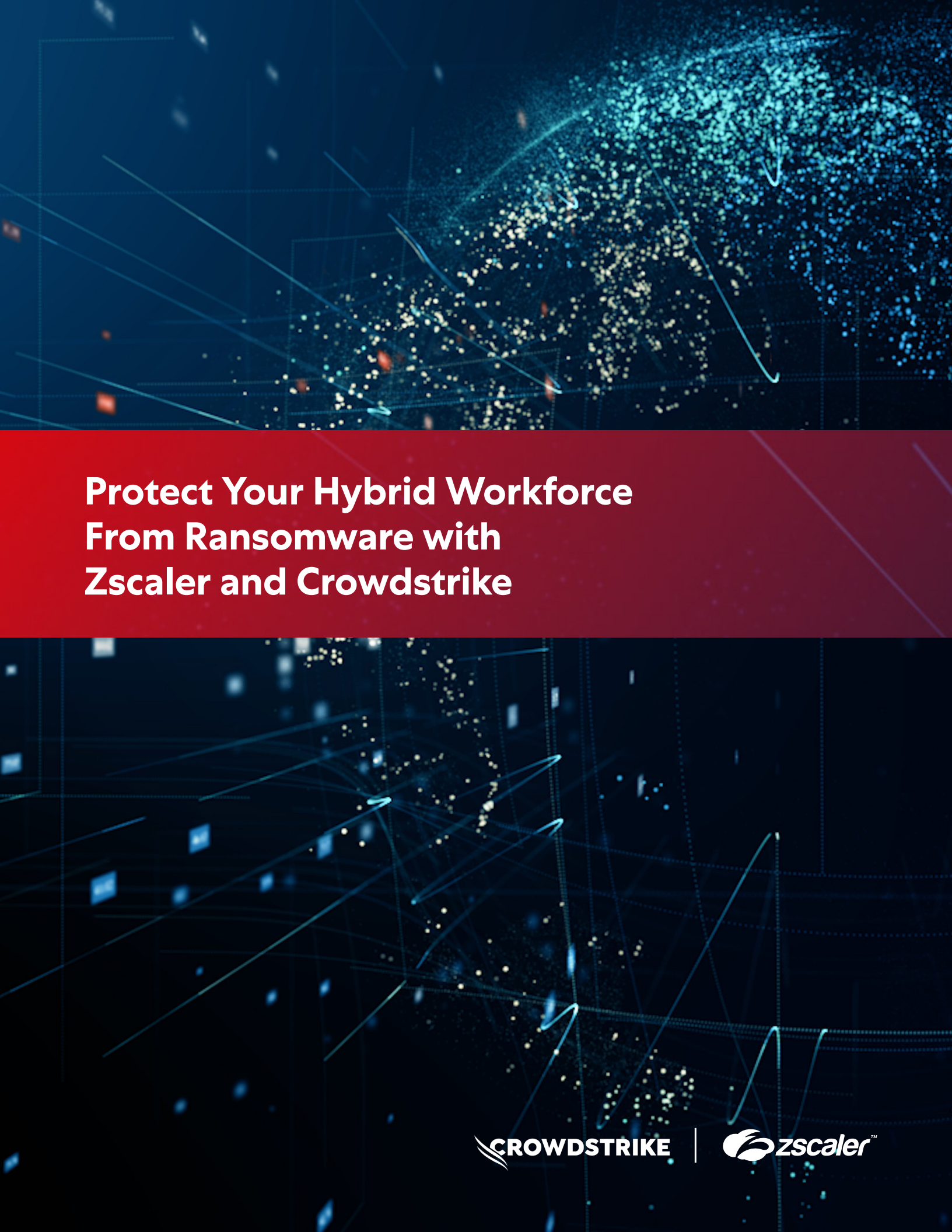


Protect Your Hybrid Workforce From Ransomware with Zscaler and Crowdstrike

CROWDSTRIKE | zscaler™

Ransomware attacks grew by 82% last year.*

*CrowdStrike 2022 Global Threat Report.

Hybrid work attracts sophisticated cyberthreats.

Shifting resources to the cloud in support of modern hybrid work adds agility and scalability. But for cybersecurity teams, an "anywhere, anytime, any device" workforce means a dramatically expanded attack surface. Threat actors, eager to take advantage, have redoubled their efforts to break through these expanding, hard-to-defend perimeters. Whether the attacks come from nation-states or dedicated criminal gangs, the highest-profile goal of this unauthorized access is ransomware: holding your own assets hostage for an easy payoff.

In the past, simple ransomware attacks that locked down a user's computer or files could often be reversed by a trained professional. Today's ransomware attacks are much more complex and premeditated, and victims often have little choice but to pay the ransom. In a typical modern attack, hackers breach your security and exfiltrate sensitive data, then encrypt it and offer to provide a decryption key in exchange for a payment (usually in untraceable cryptocurrency).

Even if you were foresighted enough to backup your data, you're not off the hook. Threat actors can leak that private data—which can include partner data, customer credit cards, or patients' personally identifiable information—unless you pay up. This is known as "double-extortion," and it's just one example of the ever-evolving details of ransomware attacks. With hybrid work clearly here to stay, organizations are struggling with how to provide the seamless access remote and on-premises workforces need while safeguarding enterprise data from cyberthreats.

Solution: A Zero Trust security posture that provides end to end security.

Supporting modern hybrid work without putting enterprise assets at risk requires a fundamentally different, comprehensive approach to cloud security. Defending today's work-from-anywhere environment requires a scalable zero trust security posture and extended detection and response (XDR) tools to better arm security teams to protect users, applications, and sensitive data from inbound threats, regardless of where users are connected or what devices they're using.

Zscaler and CrowdStrike provide best-of-breed, cloud-delivered, end-to-end security solutions that let organizations safely support hybrid work while hardening defenses against ransomware and other cyberthreats. Spanning workloads, endpoints, applications, and users, the platforms share telemetry and threat intel to enable zero-day malware detection and quick remediation. **The Zscaler Zero Trust Exchange** keeps your users and apps invisible: Authenticated users connect directly to the applications they need, never to the network, minimizing the ability of intruders to move laterally. **Crowdstrike's Falcon Platform** intelligently synthesizes telemetry data from endpoints, producing realtime device posture scores and working with Zscaler to inform access decisions with user context and device health.

The two solutions work together to inspect all inbound and outbound traffic, whether or not it's encrypted. Admins gain real-time, contextualized insights into the threat landscape, and can modify access policies dynamically based on the context of the user and device security posture. Enterprises get new tools to safely automate access policy enforcement, block malicious IP and domains inline, and ensure that only currently-compliant devices can access highly sensitive data and private apps.

Together, Zscaler and CrowdStrike provide ransomware prevention, protection and remediation.

1. Supply conditional access based on device posture for private and SaaS apps

CrowdStrike Falcon collects telemetry from endpoint devices trying to access private apps, and calculates a Zero Trust Assessment (ZTA) score. Any changes in device settings triggers a recalculation, allowing CrowdStrike to dynamically assess the health of all user devices. After confirming the CrowdStrike sensor is running on the endpoint device, Zscaler Zero Trust Exchange compares the device's ZTA score against the defined policy threshold, granting or revoking access to the internet, SaaS and private apps. Access thresholds can be easily adjusted on the Zscaler dashboard.

2. Support zero-day detection and remediation on ransomware files

The Zscaler Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. When malicious or suspicious files are discovered, the file hash is correlated with the endpoint data from CrowdStrike, tying the threat to the endpoint data. The correlation automatically identifies the impacted endpoints across the environment; administrators can pivot from the Zscaler Insight Log to the CrowdStrike Falcon Console with automatically populated data for quick endpoint investigation and remediations like quarantine.

3. Block ransomware threats inline with shared cross-platform intelligence

Using CrowdStrike APIs, Zscaler integrates global threat feeds with CrowdStrike's threat intelligence covering each customer environment. These threats are compiled as high-confidence Indicators of Compromise (IOCs) in a custom block list. ZIA can then automatically block these identified threats, based on a deeply integrated, continuous update of IOCs across cloud applications and endpoints.

4. Identify ransomware issues in real time as CrowdStrike Humio Log Management ingests Zscaler logs

The Zscaler Internet Access (ZIA) & Humio package was designed specifically to receive data directly from Zscaler's cloud services, particularly the Nanolog Streaming Service. This package for Zscaler's ZIA CASB, Cloud Firewall, Web Traffic and Quick Look includes parsers and dashboards for each of the different logs, as well as saved searches to enable customers to action data immediately upon receipt from the cloud. Administrators receive richer context by combining Falcon detection with Zscaler telemetry through a single database.

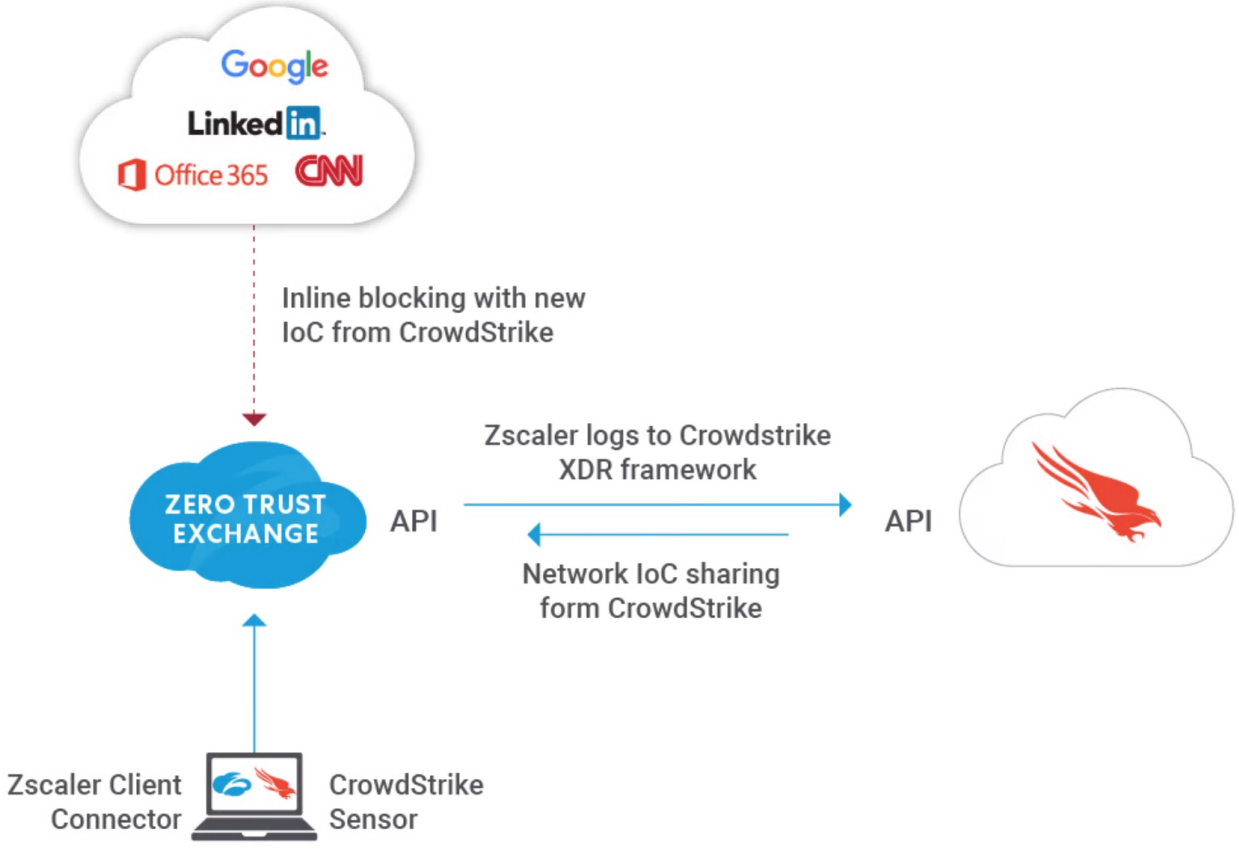
5. Minimize the threat of insider attacks with Zscaler and CrowdStrike integrated together

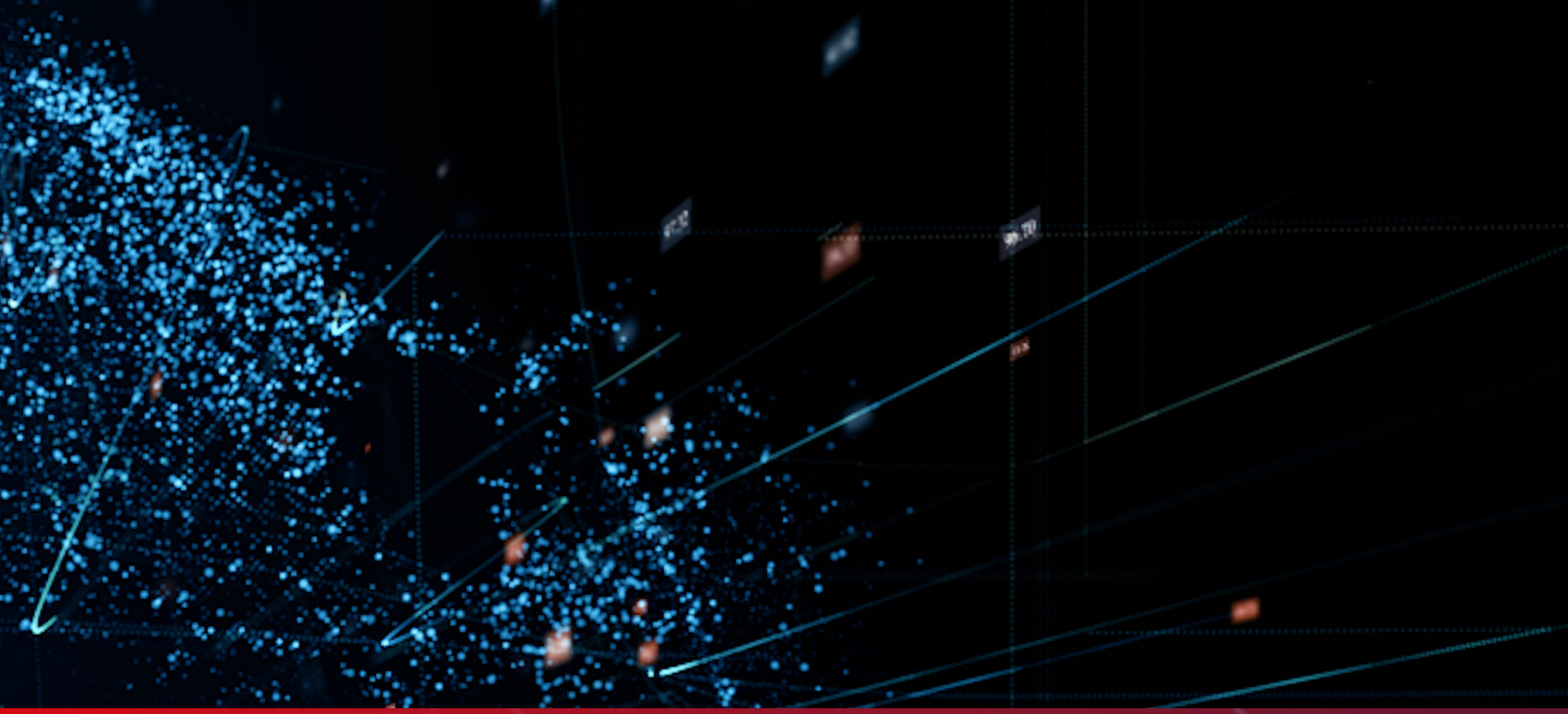
The CrowdStrike-Zscaler Intel Bridge uses APIs to transfer high-confidence malicious indicators from CrowdStrike's FalconX Intelligence Module to the Zscaler platform. Within this easy-to-use platform, Falcon administrators can create custom rules to block users from interacting with known malicious websites. Sharing threat intelligence through the CrowdStrike-Zscaler integration allows organizations to push mitigations to the network layer, and proactively prevent threats before they ever reach the endpoint.

End-to-end visibility enables conditional Zero Trust access.

Zscaler and CrowdStrike: Ransomware Protection for a Changing World

Zscaler and CrowdStrike provide a comprehensive, end-to-end security solution that provides modern enterprises with a reliable Zero Trust foundation, so they can safely permit the hybrid work today's dynamic global teams need. Spanning managed and unmanaged devices, servers, public cloud, and cloud apps, this comprehensive collaboration delivers all key security controls as an edge service—close to every end user, branch, or enterprise headquarters. Shared threat intelligence minimizes the risk of lateral movement by threat actors, prevents data loss, and delivers quick time-to-detection and prompt remediation. Together, the platforms provide secure access to essential business applications for a workforce on the go, while protecting these hybrid workforces from new, sophisticated ransomware tactics.





Zscaler and CrowdStrike: Safely enable hybrid work and protect against ransomware with a unified solution that scales.

About CrowdStrike: Crowdstrike Holdings, Inc. (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.

Learn more at **www.crowdstrike.com**.

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on **Twitter @zscaler**.

CROWDSTRIKE | zscaler™