Zscaler + Tidal Cyber

End-to-End Visibility, Threat Detection, and Remediation Empowered by XDR

JOINT SOLUTION BRIEF

INTEGRATION HIGHLIGHTS

- Enhanced Threat Intelligence and Defense
- Improved Threat Hunting, Test Prioritization, and Detection Engineering
- Defensive Stack Optimization and Visibility into Gaps

The Market Challenge

Organizations are facing increasing pressure to do more with less as budgets are cut and resource constraints grow, making it critical to maximize the value of existing security solutions and streamline decision-making.

Managing security tools and configurations to optimize defenses and budgets is a significant challenge. On top of that, understanding the true capabilities of a security stack while keeping track of tool configurations and coverage against threats is a time-intensive process that often leads to critical blind spots.

Identifying and addressing key solution gaps requires significant time and effort. What's more, understanding the holistic capabilities and value of your current toolset is challenging due to labor-intensive struggles with tracking and optimizing tool capabilities, configurations, and prioritizing new tools. This delays critical improvements and leads to underutilization.

The Solution

Together, Zscaler and Tidal Cyber unify to provide unprecedented visibility into your security threats and provide an understanding of how adversary tradecraft affects you. This integration delivers insight into how your entire security stack, with Zscaler as a cornerstone, is defending you. Tidal Cyber Enterprise Edition tracks and extends the MITRE ATT&CK® knowledge base with Tidal Cyber and CTI integrations, providing you with an up-to-date view of the threat landscape and the risks it poses. Tidal Cyber then allows you to track what Zscaler products and capabilities you have enabled to mitigate those risks, alongside key solutions like EDR, custom SIEM rules or firewall policies. With seamless integration between Zscaler and Tidal Cyber, security teams can minimize risk and block threats outright while also accelerating investigations and remediating threats faster. Security operation centers can triage, investigate, and remediate threats much more efficiently and with greater confidence, all while maximizing your Zscaler investment.

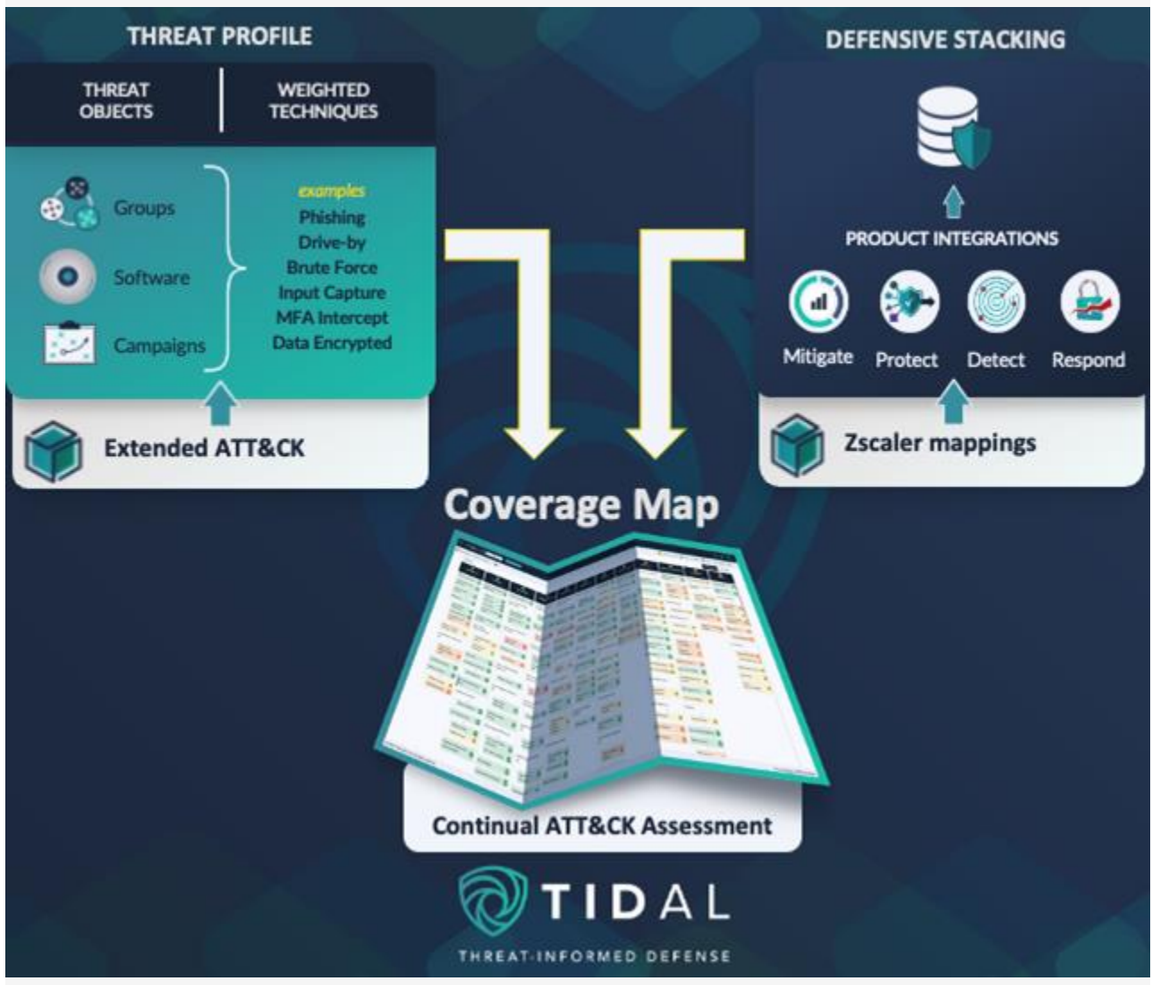
Together, Zscaler and Tidal Cyber delivers unparalleled visibility into adversary behaviors, putting security teams one step ahead of latest threats. Plus, you receive recommendations to better leverage your available security stack including Zscaler, improving your security posture.

Solution Components Deep Dive

Tidal Cyber Enterprise customers define what threats they care about, whether through Tidal-curated threat profiles, cyber threat intelligence integrations, or their own creation. This defines the ATT&CK techniques they care about, as well as how much risk they pose.

The Tidal Cyber customer then creates a Defensive Stack, containing their Zscaler products, alongside any other defensive solutions they want to get credit for. Whether manually or via cyber defense intelligence integrations, they set their tools to the configuration they have deployed.

The Tidal Cyber platform continually collates the user's threat profile and defensive stack against each other, so as the threat landscape changes or your defenses evolve, you are seeing the up-to-date risk posture of your organization as it relates to ATT&CK. Any non-enabled configuration options for your defenses turn into recommendations, with a risk reduction displayed to ensure the next thing you do, whether reconfiguration, hunt or detection is the most impactful.



KEY USE CASES

Maximize the Value of Threat Insights

Manage threat intelligence at scale and turn it into actionable insights by quickly sifting through large amounts of intelligence to pinpoint threats and behaviors that are both relevant and urgent. Tidal Cyber's comprehensive approach ensures a continually updated comprehensive view of threats correlated against existing defensive coverage, allowing organizations to stay ahead of fast-evolving adversaries.

Optimize Defenses While Reducing Gaps

A centralized approach manages security tools and configurations in a single platform, enabling a clear understanding of tool configurations and how existing tools can be fully utilized. Gaps in defenses can be quickly and easily identified and mitigated with data-driven guidance to optimize the defensive stack through configuration changes or new investments.

In a recent use case, a threat analyst was struggling with fragmented threat intelligence, a lack of context, and a volume of threats that made any assessment unmanageable. Tidal Cyber provided a centralized, structured approach to threat research, profiling, and prioritization, which enabled the analyst to handle three times the workload compared to before.

"We were able to leverage Tidal Cyber to accelerate our early-stage threat program maturity by two years!"

Threat Analyst, Insurance Company

Zscaler + Tidal Cyber Benefits

ACTION	DESCRIPTION
SOC Assessment and Prioritization	Unify Cyberthreat Intelligence and Cyber Defensive Intelligence to define MITRE ATT&CK coverage, understand the risk of threats, how you are utilizing your defenses, and get data-driven recommendations for improvement.
Defensive Stack Optimization	Understand the Defensive Value your solutions are providing including what ATT&CK techniques they leverage, what D3FEND countermeasures they provide, how well you are utilizing the solutions you own, and how you can improve your Defensive Stack.
Threat Profiling	Research and prioritize your threat intel, powered by continual updates from Tidal Cyber. As your threats evolve, your threat profile expands, your coverage map recalculates, and your understanding of your defenses evolves, too.
Threat Hunt Prioritization	Ensure your next hunt is the most impactful. Guide your hunt based on your biggest risks, then articulate the work you have done hunting—even if you haven't found a threat.
Detection Coverage Measurement	Correlate your custom rules against your vendors and the community to understand what you have as well as what should be done next in the greater context of all the other mitigations, protections, etc., that you have in place.

Conclusion

Deliver better business results with Zscaler and Tidal Cyber

Zscaler + Tidal Cyber unify to provide unprecedented visibility into your security threats and give you an understanding of how adversary tradecraft affects you so you can know how your entire security stack is defending you. Together, Zscaler and Tidal Cyber deliver visibility into adversary behaviors, giving you strong defense against the latest threats and providing recommendations on how to better leverage Zscaler and the tools you currently own to further reduce the risk these threats pose.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | Zero Trust Everywhere

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 in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.