zscaler™

Zscaler Breach Predictor

Preemptive Detection and Response to identify today's attacks and anticipate tomorrow's.

Solution Brief

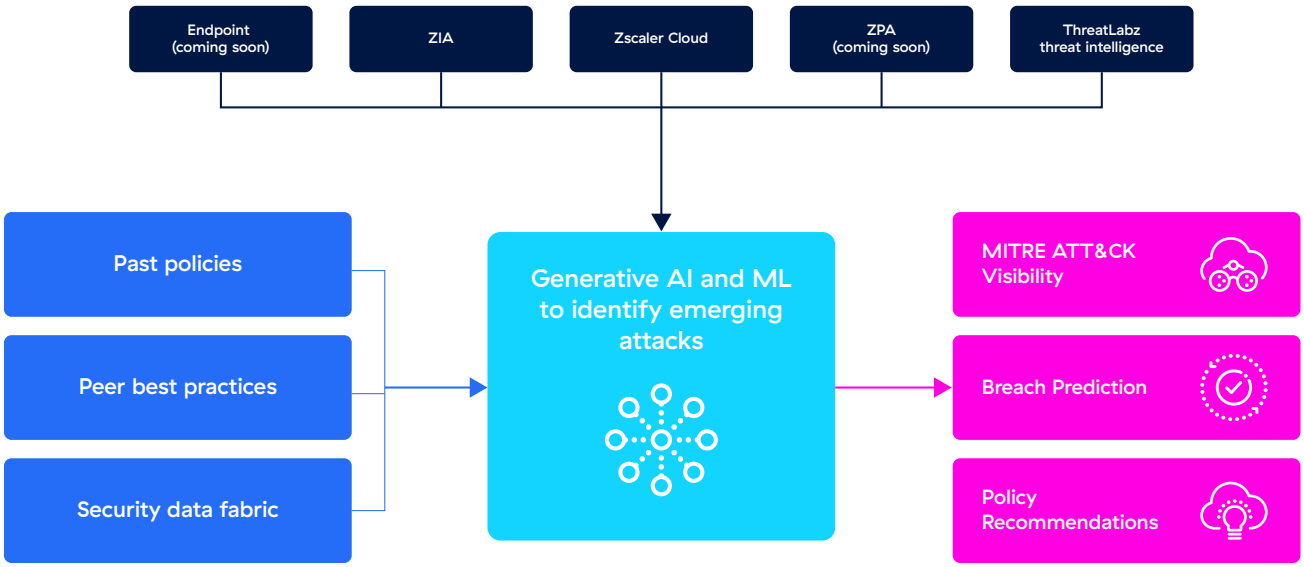
Enterprises continue to be plagued by ransomware, malware, and other threats, prompting advancements in tools like EDR, XDR, SOAR, often yielding better response automation. Yet attacks persist at concerning rates. Armed with generative AI, attackers are faster and more efficient at exploiting vulnerabilities, exploring attack surfaces, and manipulating users to breach defenses.

This heightened threat exacerbates challenges in SIEM-led triage, given unceasing attacks—not to mention false positives and overburdened teams. It is now crucial for organizations to consider more preemptive security.

Zscaler Breach Predictor is the first Preemptive Detection and Response (PreDR) solution that identifies attacks in progress and anticipates potential attacks to come. Breach Predictor visualizes attacker activity mapped to MITRE ATT&CK tactics, techniques, and procedures (TTPs), providing real-time insights on affected users and helping to understand and stop attacks underway. Utilizing advanced AI/ML, it empowers organizations to predict potential security breaches and preemptively strengthen security before exploitation occurs, ultimately simplifying security operations.

Breach Predictor benefits:

- **Enhanced threat visibility:** Get attack path visualization and real-time insights into attacker activity mapped to MITRE TTPs.
- **Predict and prevent potential breaches:** Leverage AI-powered breach probability scoring and policy recommendations to preemptively eliminate likely attack paths, lowering your overall risk.
- **Improved SOC efficiency:** Ease burdens on SOC workflows by decreasing overall number of security events while enhancing attack investigation ability.



The Zscaler Breach Predictor Difference

AI-powered by 500 trillion daily signals
Harness the power of the world's largest security cloud and data fabric for security. Zscaler's AI/ML engines are trained by threat intelligence and insights harvested from more than 500 trillion daily signatures that flow through the Zero Trust Exchange.

Breach Predictor uses AI and ML models to analyze data from various sources—including past policies, best practices, security data fabric context, IoCs and threat intelligence, and data from ZIA, ZPA, our cloud sandbox, and endpoints. Analyzing this data together allows us to model breach probabilities and recommend preemptive policies against potential attacks.

The result: Preempt attackers by eliminating likely attack paths they intend to exploit and reduce your risk of breaches over time.

Preemptive security

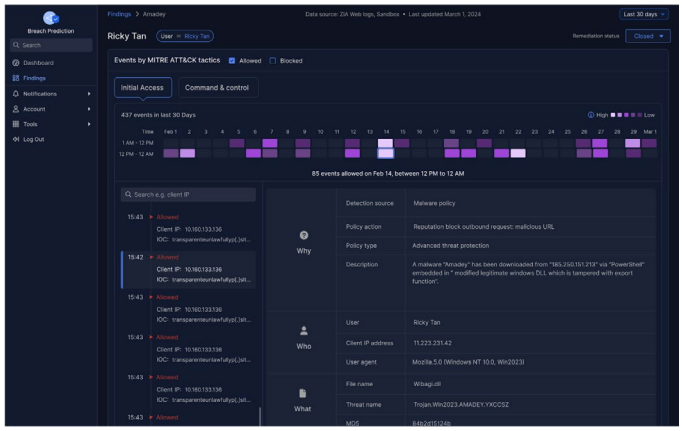
AI-powered breach probability scoring: Utilize breach probability scores to assess the likelihood of potential breaches, enabling proactive risk mitigation and reducing the burden on your SOC team's response efforts.

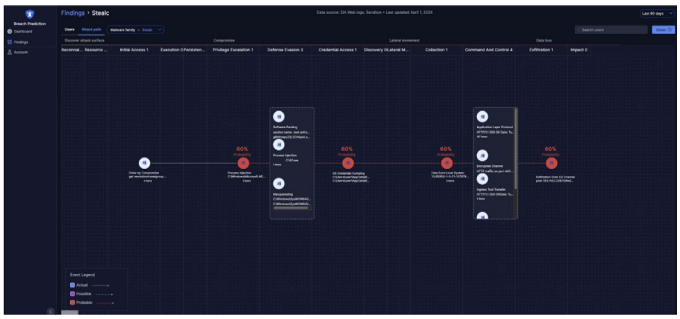
Attack path visualizations mapped to attack stages: Visualize potential attack paths mapped to the four stages of an attack to understand likely attack pathways before exploitation.

Analysis of potential attacker activity: Get detailed descriptions of popular attacker behaviors to proactively prepare and fortify security against the most imminent threats.

Preemptive policy recommendations and alerting: Receive accurate real-time alerts and tailored policy recommendations to close off attack paths preemptively, reducing security events and SOC response pressures.

COMING SOON





Key Capabilities:

FULL ATTACK VISIBILITY

- **Attack activity tracking:** Identify and trace malware activity associated with the most prevalent malware families and categories across stages of an attack, enabling targeted threat mitigation and prevention efforts.
- **Malware IOC mapping to MITRE TTPs:** Correlate observed indicators of compromise (IOCs) with MITRE ATT&CK framework TTPs, enhancing threat understanding and response strategies.
- **Granular findings on compromised users:** Visualize attack patterns and see their impact on users for faster remediation.
- **Dashboard drilldowns for attack path details:** Easily drill down into attacks for more specific findings on attack paths with related malware activities and TTPs. Also included is the forecasted probability of future attack activity.

zscaler™ | Experience your world, secured.™

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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com