DATASHEET

Lead the Way in Identity Threat Detection with Zaperon

Cyber attackers are employing increasingly advanced methods to target identities and identity systems. As identity-based attacks continue to proliferate, businesses today require robust detection capabilities to identify when attackers exploit, misuse, or steal enterprise identities. These threats often involve unauthorized access to user accounts through tactics such as stolen or weak credentials, phishing attacks etc. resulting in data breaches and financial losses to enterprises. Traditional threat detection techniques and legacy identity systems are frequently ineffective against these modern threats.

Zaperon **Identity Threat Detection & Response (ITDR)** addresses these challenges by mitigating the risks associated with cyber threats targeting identities and identity infrastructure.

86%

of data breaches are due to compromised credentials

Source: Verizon Data Breach Investigation Report 2023

328

Number of days it took to identify and contain data breaches resulting from stolen credentials

Source: IBM Cost of Data Breach Report 2023

74%

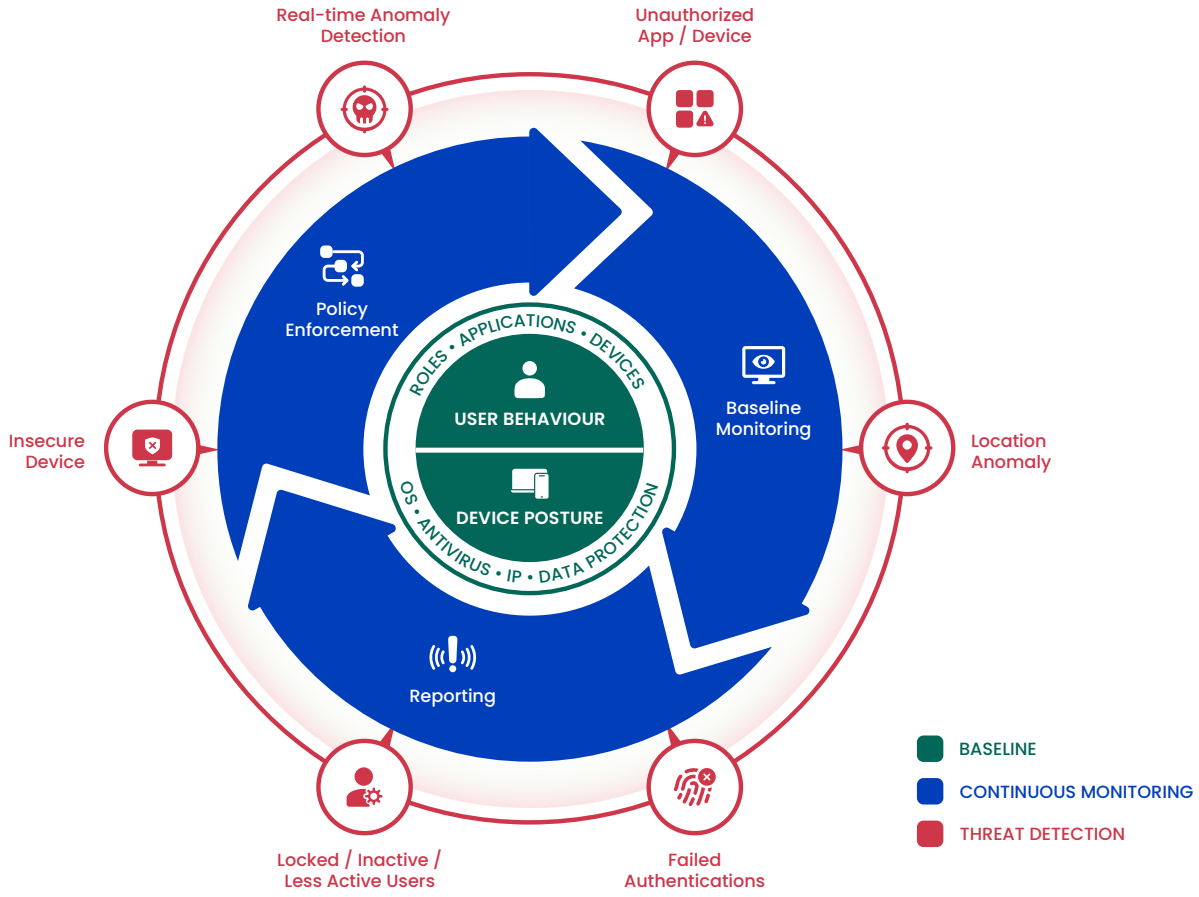
of data breaches involve human element

Source: Verizon Data Breach Investigation Report 2023

How Zaperon ITDR Works

Zaperon streamlines identity complexities in a hybrid work environment by offering essential components of an identity fabric, addressing the most pressing identity threat detection and response challenges today. Zaperon can integrate seamlessly with your existing identity systems and enhance your identity protection capabilities across various applications without incurring substantial integration costs.

Zaperon's ITDR works through a multi-step process designed to enhance security by monitoring and managing user identities and behaviors.



BASELINE CREATION

On Zaperon cloud controller, you can create a baseline of normal user behavior, device posture and zero trust access policies to identify any deviations. Baseline includes following information:

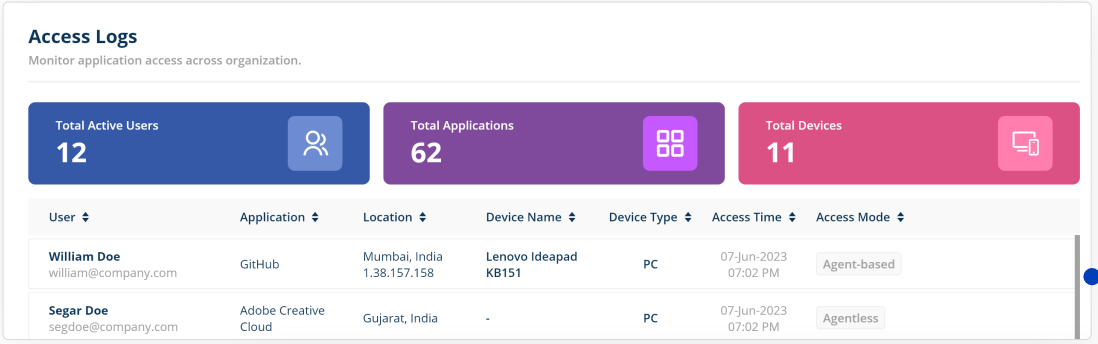
1. **Desired User Behavior:** Users' access permissions to applications are determined by their organizational roles. For instance, a finance manager might be granted access to financial reporting tools while being restricted from accessing marketing analytics applications. Additionally, administrators can configure access privileges based on authorized devices, enforce geo-location restrictions, set specific access times, and enhance security through measures like multi-factor authentication (MFA). Permissions can also be defined for users to restrict data transfer from their endpoints via USB ports, Bluetooth and Airdrop and to prevent access to files on cloud storage applications such as Google Drive, OneDrive and Sharepoint.

2. **Desired Device Posture:** These are a set of security criteria that devices must meet to be considered compliant and secure for accessing resources.

- **Operating System Version:** Specify the required operating system versions that devices must be running. Zaperon supports all major platforms including Windows, Mac and Linux.
- **Anti-virus / Anti-malware Protection:** Require devices to have active and up-to-date anti-malware software installed.
- **Patch Level:** Ensure that operating systems of the devices are up-to-date with the latest security patches and updates.
- **IP Address:** Range of whitelist and blacklist IPs can be defined.

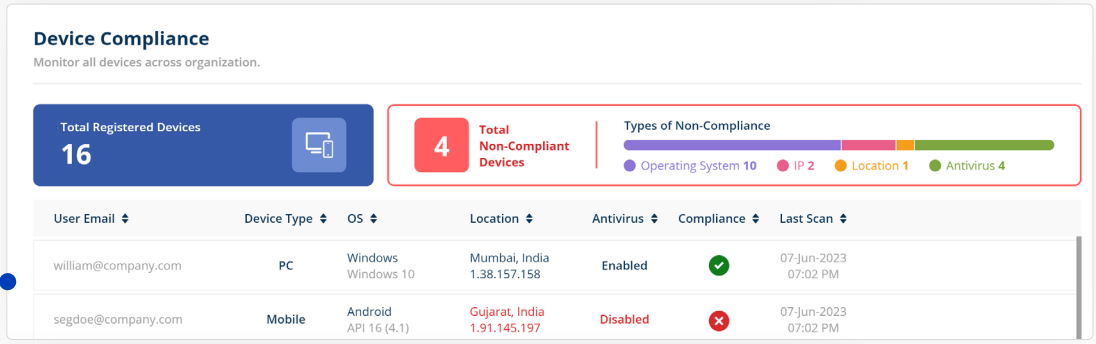
POLICY ENFORCEMENT

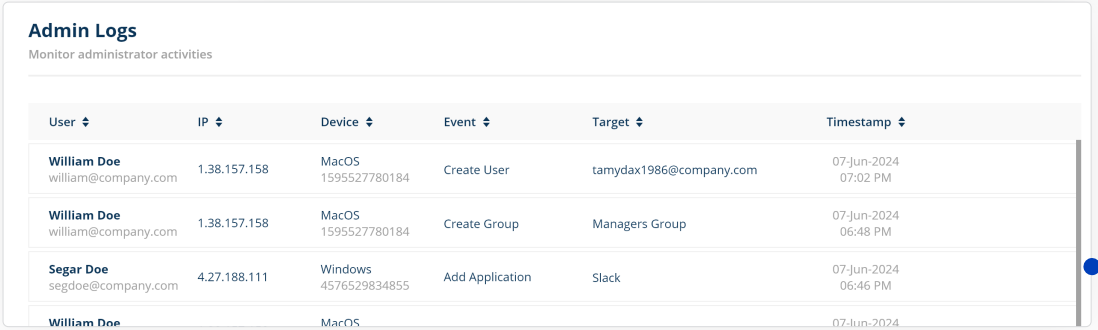
- **Policy Enforcement:** Once the policies are created, they are enforced by a Zaperon agent on the user device that ensures compliance.
- **Continuous Monitoring:** Agent conducts real-time checks every minute on all the baseline parameters of user behaviour and device posture.
- **Logging:** Along with monitoring, logs are created to capture the changes in user behaviour and device posture. All the activities performed by admin users are also logged to ensure there is no misuse of privileges and to track privilege escalation changes. Additionally, visual dashboards display real-time security status and ongoing activities for comprehensive oversight.



Application access logs for all the users

Real-time device posture check on all user devices





Log of all the admin users activities

ANOMALY DETECTION

Zaperon ITDR significantly enhances enterprise security by swiftly detecting identity-based attacks through proactive anomaly detection.



1. **Unauthorized Access Prevention:** Zaperon immediately blocks user access to applications not authorized for their use or from unassigned devices, ensuring strict least privilege access control and preventing lateral movement.
2. **Device Security Monitoring:** Zaperon monitors events indicating changes in device security configurations (e.g., antivirus deactivation, outdated firmware, network changes) to proactively block access from insecure devices.
3. **Location Anomaly Detection:** Leveraging historical geo-location data, Zaperon identifies anomalies in user locations and alerts the security team. Users geo-fenced by Zaperon policies are promptly denied access from unauthorized locations.
4. **Identification of Locked or Inactive Users:** Zaperon monitors user activity status, flagging locked accounts or those showing minimal activity (e.g., no recent application access). Security teams can investigate these flagged users to mitigate potential risks promptly.
5. **Failed Authentication Detection:** Zaperon continuously detects inappropriate login attempts across its portal and enterprise resources, promptly flagging such incidents and identifying potentially compromised user IDs.

Key Use Cases of Zaperon ITDR for Modern Enterprises



ADVANCED THREAT DETECTION

Identify sophisticated identity-based threats in real-time with proactive detection of anomalies and potential breaches within enterprise systems.



AUTOMATED INCIDENT RESPONSE

Automate the response to detected threats by blocking unauthorized access to enterprise resources and flagging suspicious accounts, minimizing the time between detection and remediation, thus reducing the impact of security incidents on business operations.



USER BEHAVIOR ANALYTICS

Monitor and analyze user behavior patterns to detect deviations that might indicate insider threats or compromised accounts, helping in proactive threat mitigation.



ENDPOINT PROTECTION

Secure endpoints by continuously monitoring and assessing their security posture, ensuring that devices are protected against vulnerabilities and malware.



INTEGRATION WITH SIEM SYSTEMS

Seamlessly integrate with Security Information and Event Management (SIEM) systems to enhance the correlation and analysis of security events, improving overall security visibility.

Zaperon is an Identity Protection 2.0 platform that secures organizations from credential attacks. It features PKI-based passwordless access, phishing-resistant multi-factor authentication, continuous zero trust policy enforcement based on user behavior and device posture, and proactive identity threat detection and response, ensuring comprehensive security for users, devices, applications, and cloud infrastructure.


+1 202 600 5234


+91 8800 170387

sales@zaperon.com

www.zaperon.com

© 2024 Zaperon, Inc.
All Rights Reserved.