CYBERARK®

DATA SHEET

Identity Security Intelligence

The Challenge

More identities than ever before require secure access to corporate data. If once, only IT admins were considered to have privileged access, this notion has changed. Trends like remote work and digital transformation have greatly expanded the number of identities who can access sensitive data stored in web applications, internal files, or databases and servers hosted on-premises and in the public cloud.

Centralized identity threat detection and prevention can help protect these identities. While many organizations may have threat analytics functionalities in existing access management and privileged access management solutions, analyzing distinct data can create siloes that interfere with security and compliance outcomes.

Organizations need consistent, centralized processes to detect risky access for workforce and privileged users. Otherwise, they could face gaps in context and coverage that could cause them to miss, mishandle or respond too slowly to security events that signal compromised access

The Solution

Identity Security Intelligence – one of the CyberArk Identity Security Platform Shared Services – automatically detects multi-contextual anomalous user behavior and privileged access misuse. Detections cover both web apps and privileged accounts for all employees, allowing data correlation. The service provides real-time alerts and recommends actions to accelerate identification, analysis, and response to high-risk events.

Through a highly customizable, centralized user interface, Identity Security Intelligence allows organizations to solve common challenges in assessing and responding to identity-related risks. The service helps reduce risk across a wide variety of user sessions by allowing organizations to apply intelligent privilege controls in-line with the risk of access.

In the average organization:

52%

of workforce identities can access sensitive data

The average staff member accesses more than 30 applications and accounts

Credential access remains the top reported sense of risk

Source: CyberArk Identity Security Threat Landscape report, 2022

How it Works:

For all identity types, Identity Security Intelligence centrally gathers user behavior analytics data such as login date/time, device, location, and use of privileged accounts. The service then applies artificial intelligence to establish behavioral baselines for all users across their access to web apps, resources and privileged accounts.

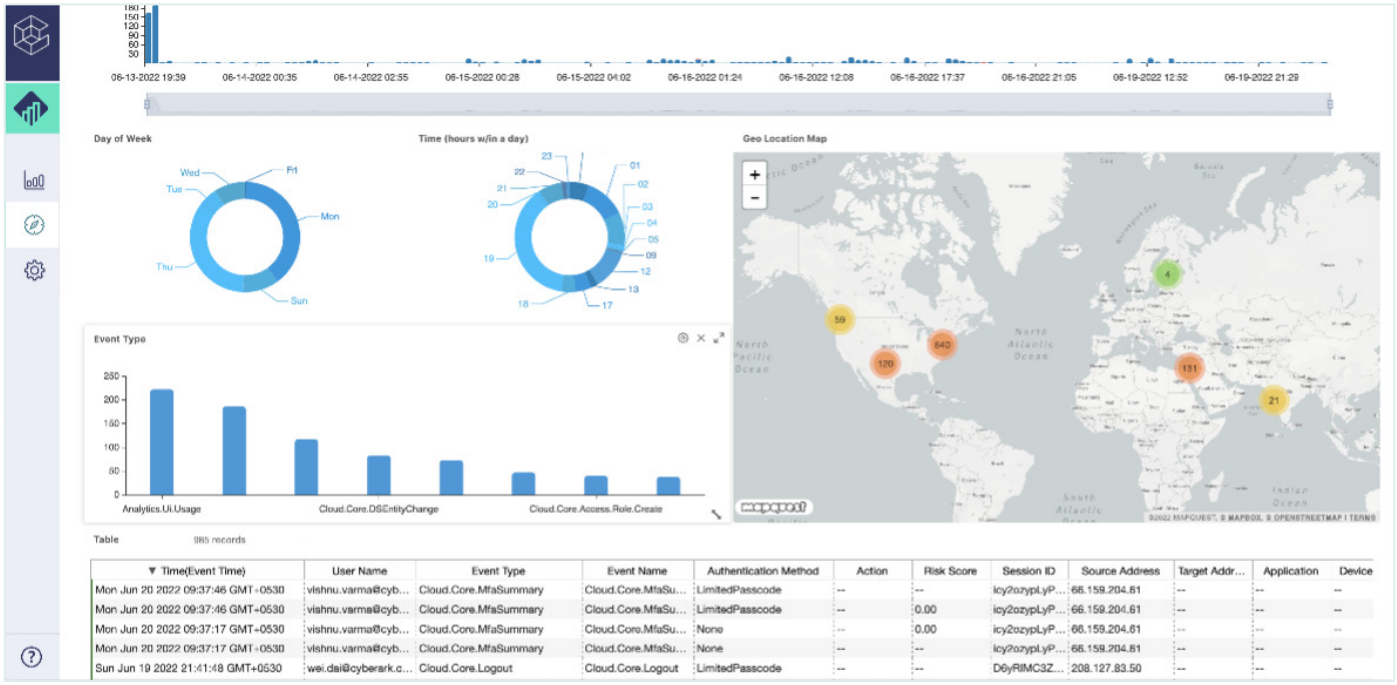
Once behavioral baselines have been established, Identity Security Intelligence can detect anomalous behavior and suspicious access attempts. The service provides risk scores to help evaluate the likelihood of Identity compromise. These risk scores are highly customizable to help define risk based on organizational context.

When Identity Security Intelligence detects anomalous or risky activity, it sends automatic alerts to prompt investigation in a centralized user interface. The Identity Security Intelligence user interface collects data into custom threat feeds for all identities, helping organizations comprehensively visualize and analyze risk.

Identity Security Intelligence also provides recommended response actions to mitigate potential identity compromise, such as locking of user accounts when risky commands are entered. The service forwards notifications to SIEM solutions to integrate with existing incident response processes.

BENEFITS

- **Deliver measurable cyber-risk reduction:** Identity Security Intelligence arms organizations with the insights needed to respond to identity-related threats. Automated security alerts and recommended actions allow organizations to quickly analyze and mitigate potential compromise.
- **Enable operational efficiencies:** Identity Security Intelligence unifies threat detection for both workforce and privileged identities. With this holistic approach and context, organizations can eliminate duplicate processes, improve detection accuracy, and more efficiently respond to security incidents.
- **Satisfy audit and compliance:** All web app and privileged sessions are assigned risk scores to streamline review. This helps auditors know exactly where to look for potential compliance risks, reducing manual review.



Time(Event Time)	User Name	Event Type	Event Name	Authentication Method	Action	Risk Score	Session ID	Source Address	Target Addr...	Application	Device
Mon Jun 20 2022 09:37:46 GMT+0530	vishnu.varma@cyb...	Cloud.Core.MfaSummary	Cloud.Core.MfaSu...	LimitedPasscode	--	--	icy2ozypLyP...	66.159.204.61	--	--	--
Mon Jun 20 2022 09:37:46 GMT+0530	vishnu.varma@cyb...	Cloud.Core.MfaSummary	Cloud.Core.MfaSu...	LimitedPasscode	--	0.00	icy2ozypLyP...	66.159.204.61	--	--	--
Mon Jun 20 2022 09:37:17 GMT+0530	vishnu.varma@cyb...	Cloud.Core.MfaSummary	Cloud.Core.MfaSu...	None	--	0.00	icy2ozypLyP...	66.159.204.61	--	--	--
Mon Jun 20 2022 09:37:17 GMT+0530	vishnu.varma@cyb...	Cloud.Core.MfaSummary	Cloud.Core.MfaSu...	None	--	--	icy2ozypLyP...	66.159.204.61	--	--	--
Sun Jun 19 2022 21:41:48 GMT+0530	wei.dai@cyberark.c...	Cloud.Core.Logout	Cloud.Core.Logout	LimitedPasscode	--	--	D6yRIMC3Z...	208.127.83.50	--	--	--

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®