Delinea

Delinea Platform: Seamlessly Extend Privileged Access Management

The cloud-native Delinea Platform provides just-in-time privileged access to authorized users with easy-to-use, adaptive controls that reduce risk while enabling growth, efficiency, and scalability.

The number of human and machine identities with privileged access is expanding. Most IT and security leaders employ a multitude of disparate security tools with little to no unified visibility across them all, making it challenging to manage fragmented privileged identity and access policies. Without a consistent, centralized way to manage privileges, IT and security teams waste valuable time, make mistakes, and leave security gaps that open the door to cyberattacks.

A comprehensive view of privileged access security in a centralized location is essential to save time, increase productivity, and reduce risk.

Secure privileged account credentials quickly

At the foundation of the Delinea Platform is the industryleading Privileged Access Management (PAM) vault, Secret Server, which ensures ease of use with enterprisegrade security in one centralized environment.

Secret Server seamlessly identifies, secures, manages, monitors, and audits shared credentials for service, application, root, and admin accounts across your enterprise.

Quickly secure access and monitor activity on mission-critical privileged accounts while driving the perfect balance between security, efficiency, and productivity across teams.

• Improve security Significantly tighten your attack surface with robust, granular controls on shared credentials for every privileged account.

o om roci		Al Secrets	All Se	All Secrets								
e ven		Q Dearch Falliers										
- 1451		O streets	a		Active v All Templates v	4					Create Seco	
h insigns	~	- C Peneral Notes									45 A	
Notifications	÷	D Tony Coulding	0		MANE	SECRET TEMPLATE	POLDER	HEARTBERT	OUT OF SING	CHECKOUT EMAILED	ROUBESARRON.	
Managence		C A.Mugir Accounts	> 0	9	1 Checkaut	Active Orectory Account	Use Case Drangies Secret Non-fovo	Success	N	795	140	
Administration		 C Address C Instantiane C Instantiane D Instantiane C Instantiane C Instantiane 	> 0	٠	1 Demandonin - Haden/festword	Arthe Greatbry Account	Use Case E. Joman John strators	Buccess	Ne	769	No	
y American			> 0	*	2.00mmr.40mn-um.07.5- 0	Active Orectory Account (La.	URCEREL, COMMONDINGUES	Success	N0	140	140	
			> 0	2	2 Voxfor - Srge Stap	Artise Orectory Account	Use-Case Examples/Secret Alph/lows	Buccess	NO	140	105	
			> 0	9	1 Vestor - Mail Stage	Active Orescipity Account	Use-Case Examples/Secret MarkTows	Buccess	No.	760	Yes	
			> 0	\$	A. Require Comment / Totat	Active Directory Account:	Use Geee Examples/Secret Markhows	Success	NO	NO	NO	
			> 0	\$	ADCProcyUser Rossent.	Unix Account (85H)	Platform Access RCMaCrime	Falled	Yes	780	740	
			> 0	\$	Ath Server Root Account	Unix Root Account (SSP)	Pathare Access RXMe7/re	Unknownéhor	NO	190	N0	
			> 0	\$	ALM Approver account	Tels Password	ALV Logn Accounts	District	Ne	790	740	
			> 0	\$	ALM Perguestar account.	THE Password	ALV LOGIN ACCOUNTS	District	N	NO.	740	
			> 0	\$	epi_uee1	Detreadens AN Grebertials	Use Gase Examples WPLAccounts	Doubled	No	No	No	
			> 0	ġ.	A3 +0C//Deries-C0EOCPR	Bri Delles Mainhame	Plothers Access R2400/Dysters I	Disekted	The later	Yes	794	
			> 0	\$	ANS/ANDonaule/User	Anazon/Mr.Conside Passer.	Use Geoe Exemples/Cloud AccoIA.	Owkied	No	190	100	
			> 0	\$	ANSUMISH	AnasoniMilley	Use-Cese Exemples/Coust RoosIA.	Falled	Yes	Thu	The later	
			> 0	\$	beckup	the deriva Mainhame	Plothers Access #0.40019ystam1	failed	79.0	no	no.	
			> 0	\$	velreaders.com/avc_spi	Active Directory Account	Use Gere Exemples/Dervice Accounts	0.com	Ne	19ap	Ne	
			> 0	٩	catheadons.comaxc_app	Active Directory Account	Use Case Examples/Dervice Accounts	Duccese .	74	No	744	
			> 0	\$	ceineadens.comiese_backup	Active Directory Account	Use Gase Examples/Service Accounts	0.0000	Ne	No	No	
			> 0	\$	celheadens.comasc_deeports	Active Directory Account	Use Case Examples/Dervice Accounts	Duccesa	The local data	The later	784	
			> 0	\$	celineadene.com/ave_pereilo	Active Directory Account	Use Case Examples/Service Accounts	0.0000	No	No	No	
	<		> 0	9	calmandama.comines_mine	Active Directory Account	Use Case Exemples/Denote Accounts	Delivers	har	The	Tex	

- Increase efficiency Intelligent automation automatically discovers orphaned or forgotten privileged accounts and rotates passwords while seamlessly testing with "Heartbeat."
- Fast time to value Easy deployment, implementation, and management ensures a lower total cost of ownership and a quick return on your investment.

Centralize authorization controls consistently across identities

Privilege Control for Servers enforces least privilege principles by centralizing authorization controls across identities to help IT and security teams meet compliance, improve productivity, and reduce risk.

Seamlessly build on your credentials vault by extending Privileged Access Management and layering security directly on your servers using enterprise identities.

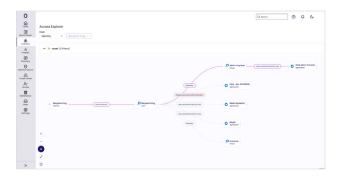
0				Q. Search th	Q. Search the Delinea Platform					
) Home	Inventory									
ecret Server	Manage Computers from this centraliz	ed location. Learn more 0	2							
& Inventory	Q Search									
ill Insights	26 items						Til ComputerName 🗱 🗄 🕻			
0	COMPUTER NAME 1	TYPE	DOMAIN	OPERATING SYSTEM	CLIENT VERSION	CREATED DATE	LAST MODIFIED			
Discovery	LS-RADIUS-01	Server	homelab.local	Unux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08 55 AM			
Policies	▲ LS-RH-03	Server	homelab3.local	Linux	6.0.1-375	9/6/2023 11-11 PM	1/4/202412-26 PM			
A.	∆ LS-RO-01	Server	homelab.local	Linux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08 55 AM			
2	∆ LS-RO-02	Server	homelab.local	Linux	6.0.0-151	8/17/2023 03:48 PM	9/26/2023 08:55 AM			
larketplace	∆ LS-UB-01	Server	homelab.local	Linux	6.0.1-359	8/17/2023 03:48 PM	10/25/2023 01:11 AM			
	ws-01	Server	homelab.local	Windows	6.0.0-115	8/17/2023 03:48 PM	9/26/2023 08:55 AM			
۲	ws-02	Server	homelab.local	Windows		8/17/2023 03:48 PM	8/17/2023 03:48 PM			
Settings	WS-04	Server	homelab.local	Windows	6.0.0-115	8/17/2023 03:48 PM	9/26/2023 08 55 AM			
	📕 W8-05	Server	homelab3.local	Windows	6.0.1-360	9/26/2023 08-55 AM	1/3/202412/11 PM			
	📕 WS-06	Server	homelab.local	Windows		9/6/202310/53 PM	9/6/2023 10:53 PM			
	S-07	Server	homelab3.local	Windows	6.0.1-362	1/22/2024 11:50 PM	1/22/2024 11:50 PM			

- Just-in-time (JIT) and Just Enough Privilege (JEP)
 Grant administrative rights and privileges only when they are required across Windows, Linux, and Unix in hybrid multi-cloud environments.
- Streamline privileged access Unify authorization across all identities with a full audit trail directly from the host.
- Security at depth Enforce Multi-Factor Authentication (MFA) at log-in and privilege elevation for additional identity assurance and to mitigate lateral movement risk.

Enforce least standing privilege across public clouds

Privilege Control for Cloud Entitlements provides cloud security leaders with deep context into cloud and identity usage to discover excess privilege and limit authorization across multi-cloud infrastructure to reduce risk.

Integrate cloud entitlements as part of your central authorization policies across all identities by discovering and visualizing all identities, accounts, and their access across Google, Amazon, and Microsoft clouds to identify anomalous behavior and refactor privileges.



- Continuous discovery Single click launcher with robust controls gets you going fast.
- Enforce least privilege Agentless deployment eliminates additional software and management time.
- Identify risky identities Session recording for every remote session gives you oversight.





Proactively detect and address identity-related threats

Identity Threat Protection builds context across the identity layer to discover and remediate threats in real-time, delivering high-quality insights that help Security Operations leaders limit the impact of identity-related threats.

Proactively reduce risk by identifying anomalous behavior, understanding the most vulnerable identities, determining the potential impact if compromised, and taking appropriate actions.

Apps Over	rview							Q Search	0	ф с
9, Search		40	p Type Al	*						
🛹 ANS Acc	ount 071186405907	39×	🛹 AMS Account 57659307626	a 51%	Microsoft	t Active Directory - A.,	52×	Ping ident/	ty environment - A	a. 1
62 Accounts		iO2 Neto	36 25 Accounts Groups	568 Assets	5,340 Accounts		,225 10053	18 Accounts	6 Oroups	20 Assets
25 Attin	Active		23 Active Onexis • High (2) • Medium (6) • Low (5)		12 Active Checks • Medium (4) • Low (1)			11 4 Failed Checks Checks • Medium (k)		
Pingidor	tity environment- W.,	68%	Ping identity environment - e	en. 68%	O Okta - de	N-52038398		Ping Ident/	ty Organization - t	n. 10
14 Accounts	16 40 Groups Asi	HTS	90 20 Accounts Groups	36 Assets	46 Accounts	10 2 Groups A	6 Inets	0 Accounts	0 Groups	2 Assets
11 Attive	5 Faled Checks Medium (3)	_	11 Active Checks • Medium (3)		12 Active	Failed Checks	-	11 0 Active Checks	FaledChecks	
A Microsof	A Microsoft Azure - Authomize									
95 Accounts		005								

- Continual detection Discover identity misconfigurations and anomalous behavior across federated and local identities.
- Continual detection Visualize identity access pathways across identity systems, SaaS applications, the cloud, and traditional infrastructure.
- Remediate threats Take recommended actions or automate responses to reduce the impact of an attack.

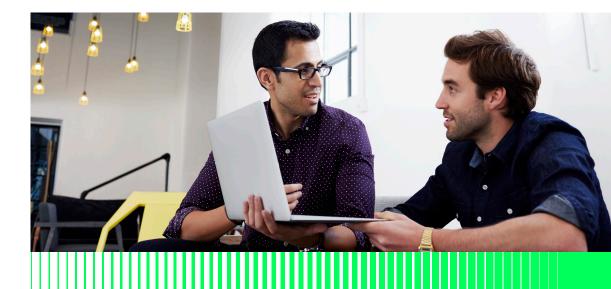
Simplify secure access for privileged users outside your network.

Privileged Remote Access on the Delinea Platform provides browser-based, VPN-less sessions with least privilege controls to help IT & Security leaders minimize risks and inefficiencies associated with remote access.

Privileged remote access can be provided to any user outside the network. As part of the cloud-native Delinea Platform, centralize authorization for remote sessions with credential injection to eliminate the exposure of privileged credentials on the endpoint while enabling users to seamlessly connect to target resources.

Delinea	armen Disertem	AlSecre	ra						0 6 3
B 1									-
h mayor -	di semanan - 1 desemblemen								
2 ·	The Association of Street of Streeto			and the second	10.000				-
	C AND ADDRESS OF	* 25 *					-	-	-
			Construction of the Owner, Name	And in case of the local division of the loc	carbonic designations.	-	-	-	-
	in the second second		The Party name and address of the Party name	Spinster, Spinst	Included States Industry,	Statute of Lot o	-	-	-
			Select Laund			100	-	-	-
			This becaut has multiple banchers, which are would you file to use!				-	-	-
							-	-	-
		* 8 *					-	-	-
							-	-	100
		> E *	Connwith Remote Acce	and a	-		-		
							-	-	-
					Clamics		-	-	-
			And in case of the local division of the loc	State of the local division of the local div	Station Sciences in Survey	and the local division of the local division	-	-	-
			And in case of the local division of the loc	stranger dark some frages.	the Designation of the Party of	Support of the local division of the local d	144	-	-
			and shows	designer disclore	cardanitargaritagence at	times.	-	-	-
			tering .	Management of the Owner, where the owner	Station Income Street Station		-	-	-
			And and a second se	And an international Advanced in	the local designs for the local is	Manufacture 1	-	-	-
			and the second s	Street Station, Square,	Interland statements for the Automatical	-	-	-	-
			And and a subscription of the local diversity	Sector Sector Sector	the local series for the local series	Second Co.	-	-	-
			designation of the Amperia	And in Frank Street of Concession, Name of Street of Str	the local parameter design of the local distance in	Sec.	-	-	-
			derivative provide	And in case of the Owner, Spinster,	the local design of the local distance in	Second Second	-	-	-
							-	-	

- Privileged remote access Secure remote access with privilege controls applied.
- Seamless management Agentless deployment
 eliminates additional software and management time.
- Compliance controls Session recording and Al driven
 auditing for every remote session



Extensible integration ecosystem for centralized access to vendors and solutions

With the **Marketplace** in the Delinea Platform, you can **view**, **try**, **buy**, and access third-party integrations in one view.

Working with multiple, siloed security solutions increases costs and takes time as you try to match up data and information. We eliminate that cumbersome inefficiency with a unified view of your Privileged Access Management landscape in one unified experience.

Oelinea		0	5 8
Ω Home ™ Wuit "II Heights ~ Ω Notifications ~	Marketplace weare to format, which invergings figures at bonnes working protone, C2. Insert Michaelmann At Companya		
Marketplace	Discover Applications Integrations		
Administration ~	INTERVIENCE HINDREAL COOSS SERVICE HINDREAL COOSS SERVICE MININGER AND		>
	Featured Integrations Wee	All Integ	ations -

- Unified experience Connect to all parts of your IT operations and workflow, security reporting, incident response, and more.
- Improve effectiveness Increase adoption by embedding PAM, CIEM, and ITDR in the everyday workflow of IT, security, developers, and business users.
- Increase productivity Accelerate digital transformation with easy-to-access and download third-party solutions.



Simplify privileged access administration

Shared capabilities on the Delinea Platform simplify Privileged Access Management with integrated functionality that streamlines and simplifies deployment and administration.

Siloed Privileged Access Management capabilities and the growing number of identities with access to business-critical assets are becoming increasingly difficult to manage. Shared capabilities eliminate cumbersome processes for privileged access administration.

- Streamline Administration Shared capabilities improve operational efficiency and productivity as you adopt and mature your PAM controls.
- Reduce complexity Using discovery, auditing, analytics, monitoring, and MFA enforcement services complexity and simplifies management.
- Unified view Clear line of sight across privileged activities and access controls across your environment helps mitigate risk, prove compliance, and increase productivity.

Organizations are evaluating their privileged account security and discovering that their expectations and needs have changed. Designed to enable growth while enhancing privileged access and identity security with unified visibility, improved efficiency and security, streamlined management, and increased productivity, the Delinea Platform meets you where you are with everything you need when you need it.

Learn more about the Delinea Platform.





Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available. Learn more about Delinea on LinkedIn, Twitter, and YouTube.