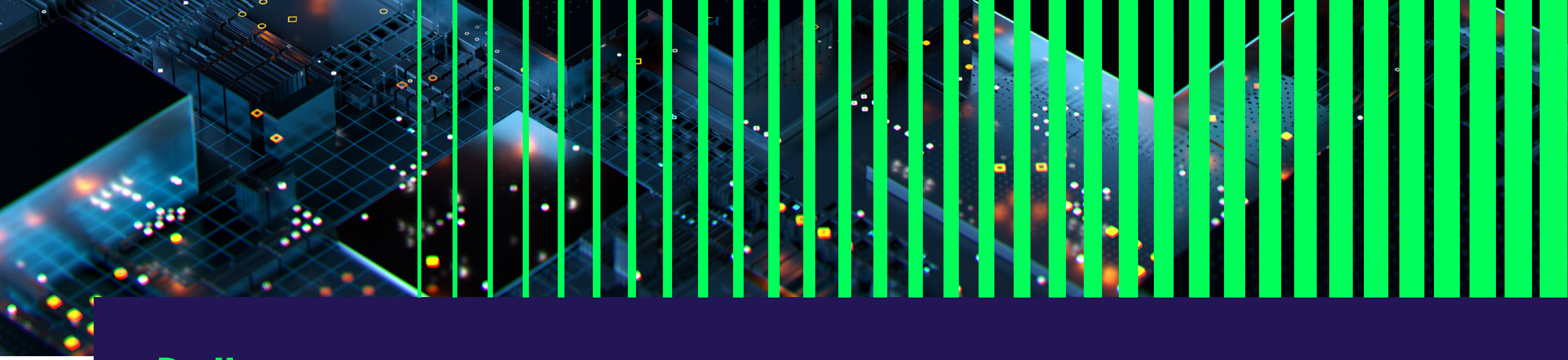

Stronger Privileged Access Security

Secret Server + Privilege Manager

Typically, an attacker's goal is to gain access to a company's sensitive data without being detected, to potentially either expose a company for something, use the information for other malicious purposes, or to sell the data on the underground market.

For an attacker to do this, they must obtain access to where the data is being stored and export that data without detection. The longer they can "own" a device that stores data, the more data they can pull out over time. The more data they have, the greater the reward.

Research has shown, in nearly all major data breaches, that access to the sensitive data happened with a compromised endpoint and compromised privileged credentials. Therefore, to protect an organization's sensitive data, they must protect both their endpoints and their privileged credentials.

Delinea prevents cyberattacks by securing passwords, protecting endpoints, and controlling access.

Every product we offer helps contribute to this with our two flagship products, Secret Server and Privilege Manager, leading the way.

Privileged access security

Secret Server and Privilege Manager work in tandem to provide privilege access security and tighten the attack surface. To ensure security for those accessing Privilege Manager, admins can use Secret Server as the authentication source for Privilege Manager to provide two-factor authentication (2FA) options.

In addition, the local credentials managed by Privilege Manager can be stored in Secret Server. Secret Server's RBAC and workflow options can be used to access the credentials as Secrets in Secret Server making that access more secure.

Just-in-time access and least privilege

Delinea offers various methods of just-in-time privilege to allow users to automatically get approved elevation.

Within Secret Server, Check Out Hooks allows administrators to configure PowerShell, SSH, and SQL scripts to run pre- and post-check out and check in. Common use cases for these scripts involve temporary elevation of an account and temporarily enabling an administrator or root level account. This is available for any system compatible with PowerShell, SSH, and SQL. With Check Out Hooks, administrators can provide time-based privileged elevation. Using the Request for Access feature, this process can be further secured with multiple approvers and ticket system validation.

At times end users may need elevated privileges to update critical applications or perform simple tasks, such as installing a local printer. Most least privilege policies fail because removing administrator rights negatively impacts users and creates more work for IT support teams.

Privilege Manager uses policy-based controls to elevate applications users need without requiring administrator credentials or requesting IT support. It automatically adds trusted applications to an allow list, checks the latest threat intelligence from tools, such as VirusTotal and Blackberry Protect (formerly Cylance), to create block lists, and adds execution rules for unknown applications in a restrict list.

IT teams decide how their policies will impact their end users. For example, administrators can choose to sandbox an unknown application, so they don't have access to system controls or operating system configurations. Alternatively, administrators can choose to require approval before unknown applications are executed or choose to provide access to that application for a limited period of time.

Because Privilege Manager elevates applications and not the user, it never leaves a window open for cyber criminals.

About Privilege Manager

Privilege Manager is the most comprehensive endpoint privilege elevation and application control solution for workstations that operates at cloud speed and scale. With Privilege Manager, you can prevent malware from exploiting applications by removing local administrative rights from endpoints without causing any end user friction that slows productivity. Enterprises and fast-growing teams can manage hundreds of thousands of machines through Privilege Manager, with built-in application control, real-time threat intelligence, and actionable reporting that demonstrates compliance with least privilege policies to executives and auditors.

About Secret Server

Secret Server is a fully featured PAM solution available both on premise and in the cloud. It empowers security and IT operations teams to secure and manage all types of privileged accounts and offers the fastest time to value of any PAM solution. Get up and running fast with solutions for privileged account discovery, turnkey installation, and out-of-the-box auditing and reporting. Delinea is doing things differently from the traditional complex, disconnected security tools.

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**