INTRODUCTION

Privilege management and delegation is one of the central challenges for enterprise IT departments right now. Solutions for privilege management and delegation provide the tools to identify, discover and manage the privileged accounts and entitlements that provide access to an organization’s most valuable resources.

While the category is mature, the challenges are constantly evolving and, in many ways, proliferating. This makes it an ongoing challenge for IT departments to educate and assign resources to stay ahead of the curve and keep the enterprise safe and secure.

Security is top of mind for most organizations. A breach can have profound effects on many areas, including reputation, which can lead to financial loss, exfiltration of intellectual property and data, drops in stock price for public companies, problems attracting or retaining customers, and legal liability and compliance issues. The compromise of privileged accounts remains one of the most attractive targets for external attackers because the accounts provide access to the enterprise’s critical assets. These accounts allow attackers to do more within the compromised systems and they can also, paradoxically, be the lowest-hanging fruit in situations where organizations are unaware of the entitlements and which system accounts haven’t been properly managed. This can include even something as simple as changing default passwords.

A less-flashy—but often more dangerous—threat is administrators and other privileged insiders taking advantage of their status to intentionally cause damage to an organization. These insiders may be disgruntled over money, promotions or layoffs, be tempted by corporate espionage, or have other motivations. Not only can administrators intentionally cause harm, they can also unintentionally make simple but critical mistakes that negatively impact a company’s infrastructure and make it an easy target for attackers.

As today’s environments become more complicated to manage, administrators have new challenges. In addition to Microsoft Active Directory, organizations are also juggling user identities, and management of entitlements, from a multitude of other sources. As organizations take advantage of the cloud with services like Office 365, they introduce new administrative roles and entitlements to the mix and also begin managing users and resources with Azure Active Directory (Azure AD). Meanwhile, many enterprises are also managing identities and privileges in human resource systems or via an attached Lightweight Directory Access Protocol (LDAP) solution. At the same time, with the growth of Software-as-a-Service (SaaS) usage in enterprises, many organizations have been forced to deploy other identity solutions to manage user accounts across multiple services and applications.
Even as vendors across the industry focus on those “other identity” solutions, Active Directory retains its primary position in most organizations’ approach to managing their privileged accounts and resources. For example, Group Policy management remains a huge challenge, but fewer vendors are emphasizing it in their product development, which is ironic at a time when a policy-based approach to organizational control is gaining traction.

There are two other factors that are making the market more fragmented. One trend we’ve seen in the last few years has been for customers to look for and buy “silver bullet” solutions to individual security problems, say privilege management or delegated administration for a single directory type. Initially these “silver bullets” quickly and effectively address the single-focused problem that they’re intended to solve. Over time, however, it’s common for these point products to pile up, adding cost and complexity to the overall administration of the enterprise. They can also reduce agility and effectiveness of the operation, as even minor updates and product decisions can involve dozens of point products that interact in unexpected ways. The other factor adding to the complexity is having different products from a variety of different vendors for different problems can lead to a lot of confusion and task switching, as administrators turn from one tool to another to solve similar problems in different systems. Without robust and regularly updated internal documentation and processes for specific environments, it becomes common for administrative tasks to fall through the cracks of a burgeoning multi-vendor/multi-tool environment.

**SOLUTION**

One vendor offering a comprehensive solution for privilege management and delegation is Micro Focus, a U.K.-based enterprise software company with a focus on maximizing the value of existing software investments for customers while positioning and enabling them for the emerging hybrid IT environment via a broad product portfolio. The company has grown significantly through acquisitions and mergers in the last few years, including deals in 2014 to buy The Attachmate Group, in 2016 to acquire Serena Software and later in 2016 to acquire Hewlett Packard Enterprise’s software business unit.

Today, the company’s privilege management and delegation portfolio includes four major products—Privileged Account Manager, Directory and Resource Administrator, Group Policy Administrator, and Change Guardian. Together they offer a more complete approach to a common but related set of issues. That approach consists of treating privilege management and delegation as requiring three key abilities—to **discover** privileges, to **control** those privileges and to **monitor** the privileges on an ongoing basis.
Discover is primarily about determining which accounts have elevated privileges or entitlements to applications and services. This discovery function also allows an organization to create a comprehensive baseline for security, compliance and auditing purposes. That process drills down into delegated administration, discovering, for example, that in addition to the global Exchange administrator, there may be a regional Exchange expert who in turn manages country-level administrators. The discovery of dependencies also covers Group Policy, Microsoft’s powerful and intricate management technology that can often lead to unintended consequences, including security issues, as policies follow a complex inheritance model and propagate downward. The Micro Focus solution discovers non-essential and/or orphaned Group Policies among its many other discovery functions.

Next is control, which involves an organization reducing its risk by delegating those discovered privileges logically across the hybrid enterprise. This is the phase where the critical security concept of least-privilege delegation comes into play. Another essential control feature is the Enterprise Credential Vault, where Micro Focus stores encrypted passwords for systems, applications and databases that can be controlled through a simple check-out/checked-back function. The control function also allows administrators to encompass multi-factor authentication (MFA), adaptive attribute provisioning, session management, Group Policy management, hybrid directory management, Linux and Unix root delegation, and workflow automation.

Finally, the ongoing monitoring of privileges and delegation includes tools that monitor for unauthorized changes, privilege misuse and other threats and, where appropriate, are able to automatically shut down access, even mid-session. It also includes the logging and reporting of any problematic or risky changes. A key element of the solution is the ability to demonstrate to auditors the administrator’s control and visibility into the system, to not only be able to answer specific compliance questions, but to show the ability to quickly address future concerns through the toolset.
PRODUCTS IN THE SOLUTION
As part of its broad enterprise software portfolio, Micro Focus offers a host of products that also incorporate aspects of identity, including Identity Manager, Self-Service Password Reset, Access Manager, Secure Login, Advanced Authentication, Exchange Administrator, Identity Governance, ArcSight, Voltage and Vertica.

While the privilege management and delegated administration solution has tight connections to many of those other Micro Focus identity-related offerings, we will discuss the core solution, which at its basic construct consists of four products.

Privileged Account Manager
Privileged Account Manager is the flagship product of the Micro Focus privilege management and delegation solution. As a first step in privilege management, the product includes a component that handles privilege discovery. Primarily, the product allows IT administrators to work on applications, databases, cloud services and virtual servers, plus Windows, Unix and Linux systems without exposing administrator or supervisor passwords or root-account credentials. The Privileged Account Manager architecture consists of a server-based management framework, agent software, a centralized rules engine and the Enterprise Credential Vault. When a user tries to execute a command on, say, a Windows Server, the agent captures the command, and submits it to the management software. There the command gets checked against the rules database. If the user, the hosts, and the day and time check out with existing rules in the database, the command is executed on the target host, with logging and, optionally, session capturing, which records all the data transferred between the administrator and the target host.

While the Enterprise Credential Vault itself could be an attractive target for attack, Micro Focus secures the embedded database with two levels of encryption. The first level covers individual passwords by encrypting them with AES 256-bit keys. The second level encrypts the entire database with an AES 256-bit key. The product also includes a risk-analysis engine that analyzes commands as they are typed and assigns a risk level. Depending on organizational preference, when the risk crosses a certain threshold, Privileged Account Manager can be set to flag an event, send an alert or even disconnect the session and revoke a user’s ability to access any privileged accounts.

Directory and Resource Administrator
Microsoft Active Directory, Office 365 and Microsoft Exchange all have their own, native administration tools and are designed to support administrative scripting. Directory and Resource Administrator centralizes these functions logically in a single interface and adds significant capabilities not included in the native tools. Allowing for discreet delegation
and audited, policy-oriented administration of multi-domain, multiple-organization and hybrid environments. With logical groupings of roles and entitlements and providing hundreds of extended capabilities, Directory and Resource Administrator allows organizations to model and exercise the principle of least privilege, delegating only the precise entitlements users need to accomplish the targeted administrative tasks assigned specifically to them. As an example, the tool includes the ability to transfer appropriate user and mailbox management functions to the help desk or to create some simple self-service functions to save on administrative overhead and processing.

**Group Policy Administrator**

One of the most powerful technologies in any Microsoft-focused enterprise toolkit is Group Policy. Yet changes to Group Policy Objects (GPOs) can have unintended consequences and potentially damaging effects on an enterprise. Group Policy Administrator significantly reduces the risk of making changes to GPOs in Active Directory by allowing administrators to model and test the changes, offline, before rolling them into production. Similar to other products in the solution, Group Policy Administrator includes delegation and workflow tools, ensuring that the right people can make changes at the appropriate times and that key managers approve these changes before they actually take effect in a production environment. The tool also includes detailed logging of Group Policy changes for auditing and compliance purposes.

**Change Guardian**

The previous three products primarily cover discovery and control aspects of privilege management and delegation, although all of them perform their own sophisticated logging. Change Guardian supports the other solutions by monitoring the activities of privileged users and accounts on an ongoing basis. Providing real-time monitoring of files, systems and applications, Change Guardian is designed to detect and notify on any unauthorized activity by privileged users. Information it provides includes who, what, where, when, and origin of the change and its capabilities are also especially geared for compliance and auditing scenarios. With simple, human-readable event language to describe its monitoring policies, Change Guardian is also designed to integrate well with security information and event management (SIEM) solutions, making it an effective information source for security teams. Main features include change detection, real-time alerts, flexible reporting, and support for Windows, Active Directory, Azure AD, Linux, Unix and NetApp.
SYNERGIES
Because these products hail from the NetIQ business unit that Micro Focus acquired as part of The Attachmate Group, integrations are deep, giving users visibility across the products into the entire privileged identity lifecycle.

As a design goal, the group of products also emphasizes simple drag-and-drop and click-through solutions over complex, custom scripting (although scripting is possible and robustly supported). Many IT administrators currently in the field, with deep experience in Windows administration, are less comfortable working in a command-line interface than previous generations of Unix-based admins, and the Micro Focus solution is built to allow those more graphically oriented admins full capabilities for building workflows and other processes in a familiar, visual fashion.

The breadth of the Micro Focus solution, meanwhile, offers many other opportunities for organizations licensing other Micro Focus products to get additional value out of the...
privilege management and delegation solution. Some common “better together” scenarios occur with Advanced Authentication, for multi-factor authentication; Arc Sight, for security operations integration; Vertica, for unified analytics; and Voltage, for data encryption.

CORE USE CASES
There are several core use cases for which the Micro Focus privilege management and delegation solution, usually involving two or more of the individual products, are commonly used by enterprise customers.

- **Hybrid Management**: As organizations adopt Office 365 and Azure AD, they’re finding functionality gaps in the native tools from Microsoft. The Micro Focus solution automates Office 365 license provisioning, helps with hybrid directory management, and simplifies administration and reporting.

- **Least Privilege Provisioning**: One of the key principles in security is giving administrators the absolute minimum amount of privilege necessary to do their jobs. The Micro Focus solution helps organizations meet this key security requirement by discovering privileged identities for review and provisioning access at a more granular level than native tools allow and, optionally, for a limited amount of time.

- **Threat and Incident Prevention**: Privileged accounts are the most attractive targets for external attackers. The Micro Focus solution helps prevent compromise through isolation and credential vaulting, adaptive access provisioning, and real-time threat alerting and remediation.

- **Governance and Compliance**: Failing an audit or struggling with achieving and maintaining compliance is a major reason for organizations to seek out a privilege management and delegation solution. The Micro Focus solution helps by balancing administrative control with administrator productivity, enforcing security policies, providing tamper-evident logs and reports, and simplifying the certification and attestation process for IT teams.

- **Privilege Tracking**: Being able to tell what privileged identity holders, such as administrators, are doing is beyond the capabilities of many IT departments. The Micro Focus solution allows privileged sessions to be recorded for command-by-command playback, identifying unapproved changes or misuse and for integration with SIEM products.
CONCLUSION
Privilege management and delegation sits at the intersection of several top enterprise priorities, including security, compliance and hybrid computing management.

The products included in the solution build on one another and on the long experience and deep expertise of Micro Focus with managing Microsoft-centric, but still heterogeneous, infrastructure. Privileged Account Manager handles privilege discovery, credential vaulting, and rules management across various platforms and applications. Directory and Resource Administrator virtualizes and greatly expands the granularity of permissions within essential Microsoft products, including Active Directory, Office 365 and Exchange, allowing for more flexible and business-oriented delegation. Group Policy Administrator helps organizations manage Active Directory Group Policy and delegate privileges in a policy-based fashion while avoiding pitfalls common to native management of GPOs. Change Guardian provides the real-time monitoring and auditing to ensure that users are using their privileges responsibly and simplifies, abstracts and centralizes the auditing and compliance capability of the entire solution to a higher level.

While many organizations struggle to get a handle on managing their privilege management and delegation issues with native tools and multiple point products, Micro Focus brings together a broad base of essential capabilities under a single portfolio.

Scott Bekker is a senior analyst with Redmond Intelligence and editorial director of Converge360. He has been reviewing, analyzing and covering Microsoft-related technologies for more than 20 years.

ABOUT REDMOND INTELLIGENCE
Redmond Intelligence provides independent and objective research and advisory services to technology buyers and vendors in the Microsoft ecosystem. Written by technical subject matter experts, Redmond Intelligence reports dive into the details of the Microsoft stack to provide actionable insights and concrete guidance. Projects range in scope from Solution Spotlights covering products in the Microsoft ecosystem to survey-based research reports to custom papers. For more information, visit redmondintelligence.com.