SILVERFORT

Business Secure

Securing your business prosperity

Addressing the Telecommunication Security Framework Requirements for Privileged Accounts

WHITE PAPER

Table of Contents

Introduction

The need to place dedicated security controls over privileged user accounts is getting a lot of interest from those organisations who are embarking on the compliance journey with the Telecommunications Security Framework (TSF) which started with the Telecommunications Security Act in November 2021, and culminated in the Code of Practice that came into force during December 2022, with the first compliance milestone is scheduled for Q1 2024 for tier 1 providers and Q1 2025 for tier 2.

Traditionally, such security requirements are addressed with a Privileged Access Management (PAM) solution which vaults and rotates credentials. However, within both Silverfort and Business Secure we feel that there's a viable alternative/complementary approach that both addresses key challenges that PAM solutions struggle with regarding meeting TSF security requirements, as well as providing features which deliver a significantly more rapid and seamless deployment.

In this white paper Silverfort and Business Secure partner to bring our experience in the realms of delivering credential discovery and management solutions and governance programmes respectively:

- Provide a brief introduction to the TSF
- Highlight the key requirements for privileged access management
- Detail the key challenges to be addressed by providers
- Showcase how Silverfort can enable Telco providers to address those challenges.

What is the TSF?

The Telecommunications Security Framework (TSF) is a collection of different components:

- *The Telecommunications Security Act 2021* which is where the common term of TSA comes from. The TSA is the piece of legislation which defines the duties, roles and powers – including amending duties within sections 105A-D within the Communications Act 2003 and creating new duties within sections 105I-K of the Communications Act – this came into force on the 17th November 2021.
- *The Electronic Communications (Security Measures) Regulations 2022* define the specific security measures (also called 'the requirements') to be undertaken by providers of Public Electronic Communications Networks (PECN) and Public Electronic Communications Services (PECS) – this came into force on the 1st October 2022 (this date is very important as we shall discuss later on).
- *The Telecommunications Security Code of Practice (CoP)* provides detailed technical guidance to providers of PECN and PECS on the measures to be taken under sections 105A to 105D of the Communications Act, with the development, compliance and maintenance of the CoP being defined within sections 105E-I of the Communications Act – this came into force on the 1st December 2022.

Whilst the duties and specific security measures are deemed by section 105E(a) within the Communications Act as giving guidance as to the measures to be taken under sections 105A to 105D by the provider of a public electronic communications network or a public electronic communications service, it is important to understand how the code of practice is categorised. Figures 1 and 2 overleaf show the distribution of key activities from the code of practice for tier 1 and 2 providers of Public Electronic Communications Network (PECN) and Public Electronic Communications Service (PECS).

NB – it's important to understand that the key to compliance with the code of practice is to review everything within the document, and then detail where you are on the implementation journey for each requirement. Whilst the technical guidance measures are important, they are informed by the key concepts, and the Indicators of Good Practice (IGPs) in Annex C which are reference in technical guidance measure M5.01 – make sure you read all parts of the CoP.

For more detailed understanding of the issues, we recommend reading the 8-part series on the TSF that highlights the key areas at https://www.linkedin.com/pulse/making-sure-you-dont-cop-packet-demystifying-security-des-ward/

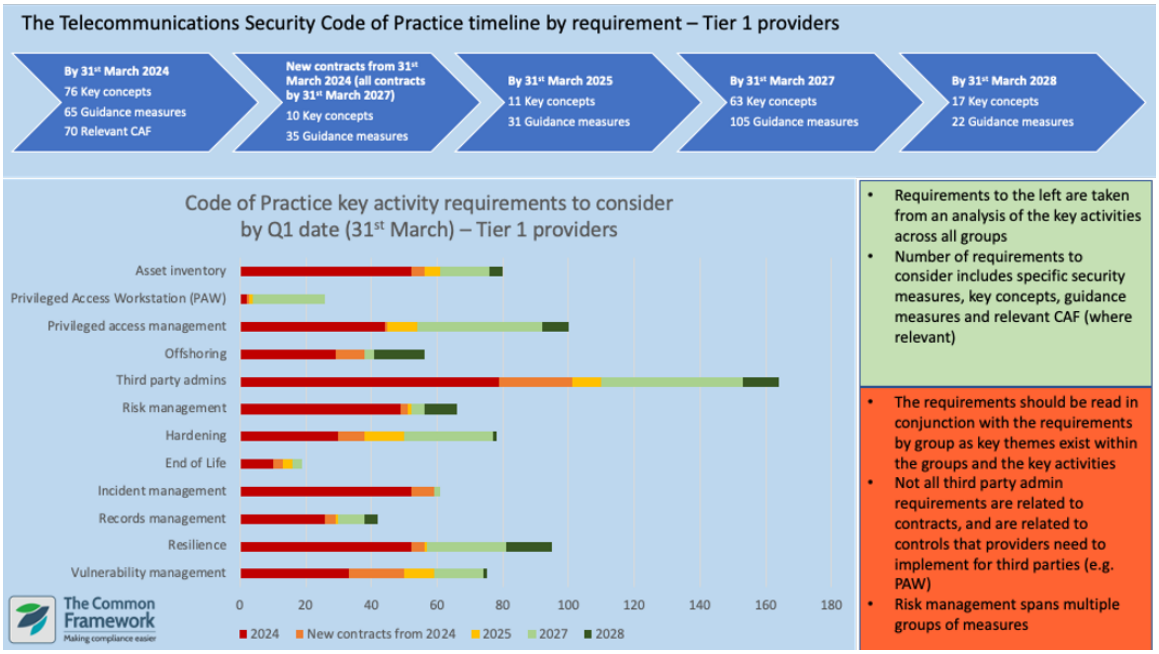


Figure 1 CoP key activities by Q1 date for Tier 1 providers © The Common Framework Limited

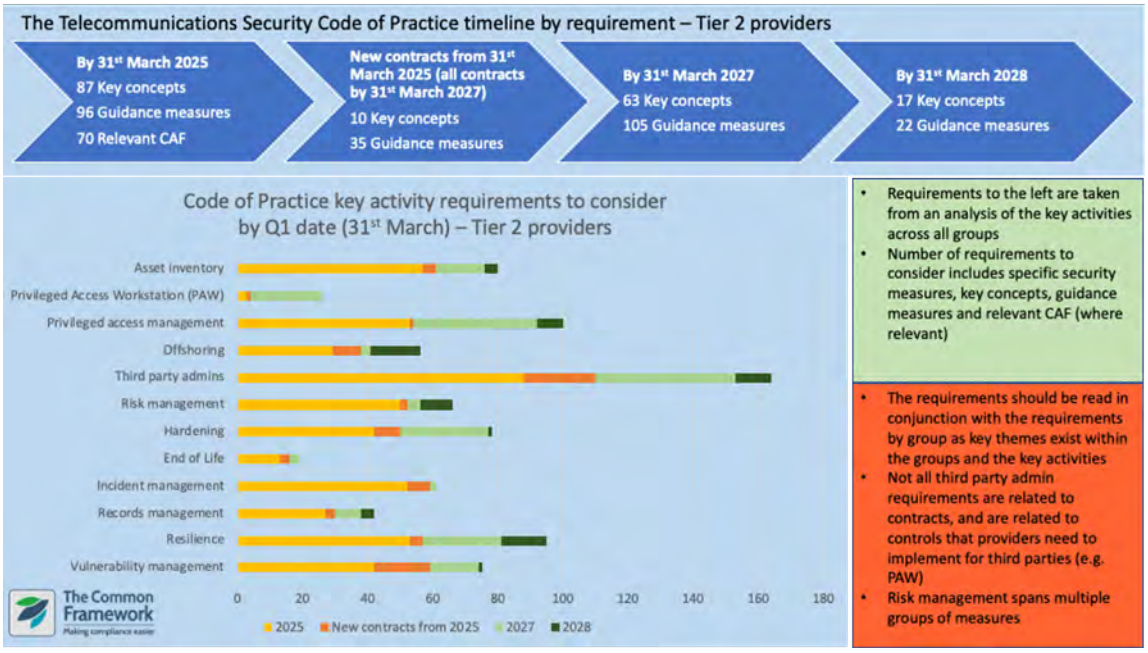


Figure 2 CoP key activities by Q1 date for Tier 2 providers © The Common Framework Limited

As you can see, managing privileged access is one of the most significant key activities alongside third party administrator management.

As we look at the breakdown of the activity groups for privileged access in figures 3 and 4 overleaf, we can see there are a range of activities that must be undertaken for compliance with the requirements of the CoP, and it is these that we will summarise within the remainder of this document.

Whilst there is a wide range of activities that must be assessed for compliance by the first compliance milestone (Q1 2024 for tier 1 providers and Q1 2025 for tier 2), we will concentrate on the most important ones for consideration.

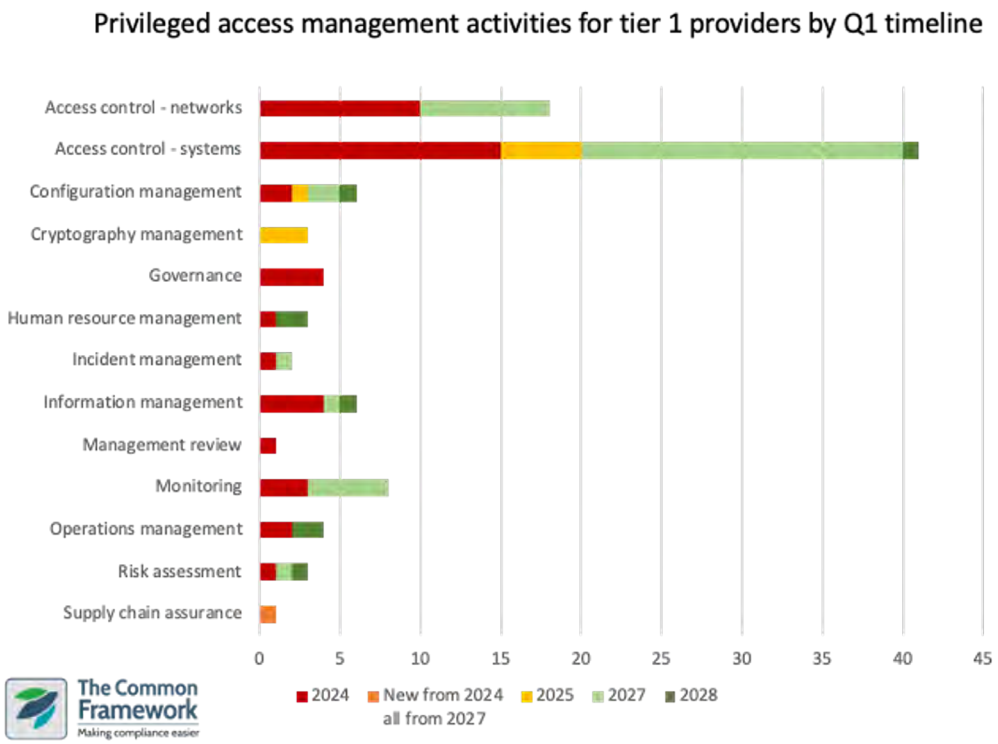


Figure 3 Privileged access management activities for tier 1 providers © The Common Framework Limited

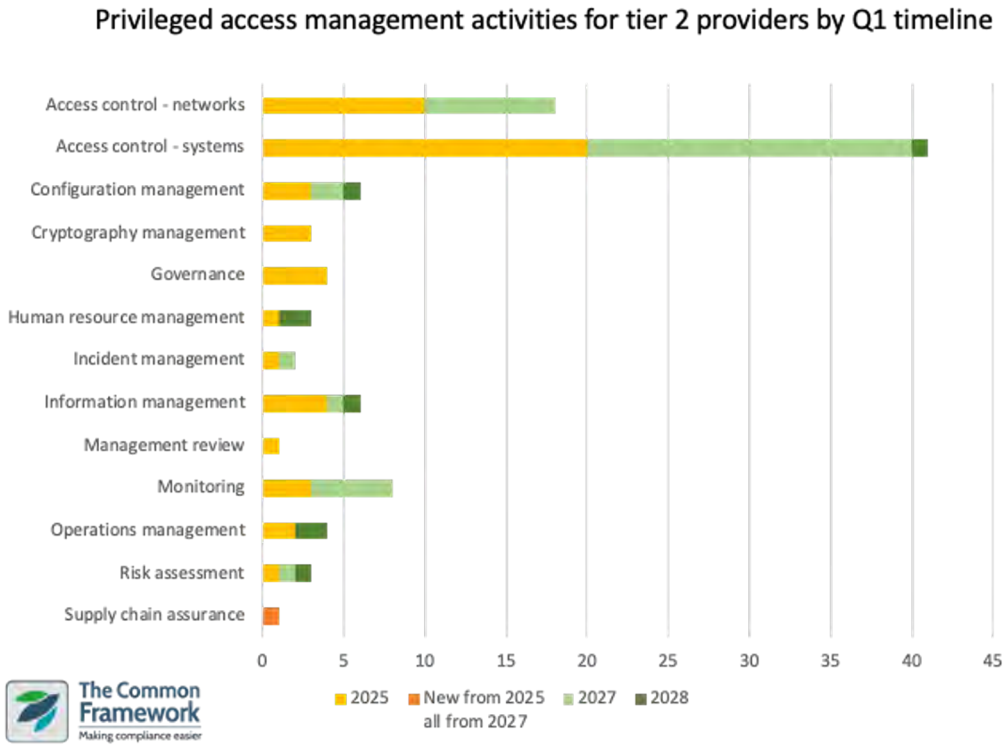


Figure 4 Privileged access management activities for tier 2 providers © The Common Framework Limited

When you analyse the 100 activities across the code of practice, as shown above, it's clear that whilst access control for functions and networks are the largest groups, the requirement for sound governance and monitoring are the next largest.

What are the key privileged access management challenges?

The TSF ultimately requires that we implement AAA in daily operation (authentication, authorisation and accounting) to deliver the mantra of "never trust, always verify" from zero trust approaches; but this requires that we understand the access paths in place in order to maintain the balance between managing known credentials used by individuals and services with the needs of vendors to support systems during emergency situations (often using generic accounts).

As shown in figure 5 below, the reality of what needs to be managed is often complex and requires careful consideration.

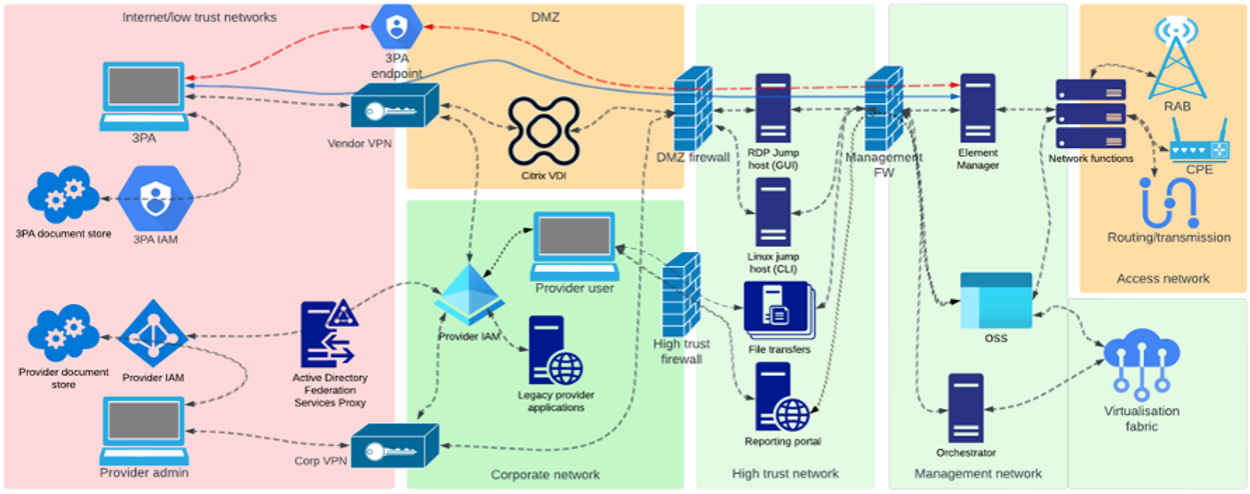


Figure 5 the operational reality of privileged access paths

The compliance debt from poor management of both user and system assets, especially in networks built for ease of support, now requires addressing to effectively meet the challenges. This challenge isn't just in legacy environments, but also within the myriad of open-source components within Cloud native or Vendor-virtualised application architectures which are built for interoperability first and security second.

The credential boundaries implemented using Privileged Access Management (PAM) solutions work very well for defined access paths but are often not able to manage (often proprietary) shadow access paths used by global support organisations, out of band access where the PAM solution might not be reachable, or to adapt quickly to scaling the existing defined access to maintain control In Cloud computing deployments or even emergency situations.

Looking at the requirements for authentication, authorisation and accounting alongside the challenges posed will provide a basis to detail how to address the challenges and where Silverfort can help you.

NB – Whilst we discuss timescales for evidencing that requirements have been met in the following sections, it should be remembered that all the requirements we discuss are part of the assessment baseline for any PECN/PECS brought into service after the 1st October 2022 (the date when the regulations came into force).

Managing Authentication — Key Requirements

Authentication involves a user providing information about who they are, and within the TSF the following are key requirements:

Ensure that default credentials are managed

The TSF requires that the passwords are changed from default on these accounts initially, with the accounts themselves being disabled from 2025 onwards.

One of the greatest challenges within telecommunications is the amount of applications, systems and network devices with default generic accounts which provide administrative access. It's a challenge that doesn't just blight legacy environments, but also impacts a range of Cloud-native applications and virtual network functions providing operational support to PECN and PECS – many of which will be built dynamically.

This challenge increases when you consider that vendors may also have default accounts that are not known to the provider which allow them to maintain the service being provided.

Ensure that access is linked to individuals

It is expected that all access is linked to individual users by 2025, with unique accounts created which use multi-factor authentication. Break-glass access is expected to be configured by 2025, with all access to network functions is expected to use unique accounts from 2027.

Notwithstanding the challenges regarding default accounts, a lack of centralised authentication results in the prolific use of local user accounts, often with generic accounts for different types of access. This can pose a problem within telecommunications as most systems and network functions are Linux-based and even virtualised functions contain Linux-daemons within them.

A further issue is the use of accounts for non-interactive sessions, these service accounts can either use generic accounts or sometimes user accounts for this purpose.

Finally, MFA can be difficult to operate without exposing the network to services outside the trusted zone – something especially of note within Cloud-native platforms.

Ensure that credentials are managed

By 2025, it is expected that all user accounts that are in regular use will be stored in a centralised location; static credentials (such as break glass usernames/passwords and certificates or other secrets) are to be stored in hardware-backed storage by 2027.

When local accounts are used on Linux-based systems and network devices, bringing them into centralised control can pose a real challenge due to offline access requirements in the event that the host is unable to reach the centralised location.

Managing Authorisation — Key Requirements

Authorisation involves an authenticated user being granted the access they are supposed to have, and within the TSF the following are key requirements:

Ensure that the access of privileged users is defined and implemented

Initially, it is expected that all access for privileged access is formally defined and reviewed, including roles and responsibilities. This requirement includes definition of the access that third-party administrators (3PAs) are expected to have, including to network/user data and information. By 2027, it is expected that all privileged access is shown to be defined from formal templates; management access to network oversight functions and virtualised functions/workloads is expected to be limited to those who require it by then as well.

The greatest challenge regarding understanding what access people should have and who should have it is the explosion of applications, systems and network devices that provide, maintain and support PECN and PECS.

Until you understand the operational reality of what is being accessed by users and how those users are accessing functions you will be unable to define the roles and responsibilities to effectively control access.

Ensure that break-glass access is managed

Whilst break-glass accounts are expected on all applications, systems and network devices that require them from 2025, the management of break glass is expected to be evidenced by 2027. This management is expected to include controlling access to the accounts themselves, ensuring that alerts are raised when they are used and that they are reset after use. It is also expected that processes to allow for the temporary suspension of existing privileged access controls, including alerting and reset of the controls, is evidenced by this time.

The approach taken by many providers to implement technical solutions for privileged access management works well when all the connections between the solution and the assets it manages are functioning. However, in emergency situations it is more difficult to react when connections are compromised and out-of-band access paths are utilised.

Providers should consider what happens to maintain a baseline level of control, regardless of whether the primary control is operational, and how to reset controls used.

Ensure that technical architectures are used to control access

The initial expectation is for providers to prevent direct access from 3PAs into their applications, systems and network devices using meditation points, with providers expected to separate 3PAs by 2027. All direct access to these devices is expected to evidenced as mediated with 'browse-down' architectures by 2027 as well.

The most common issue with current PAM solutions is that unless careful consideration has been given then there is a real danger of lateral movement from hosts that users have been given access to onwards to other hosts.

Providers should consider if all access to applications, systems and network devices is managed or if there are other downstream access paths.

Managing Accounting — Key Requirements

Accounting involves recording what activities authenticated users undertake, within the TSF the following are key requirements:

Ensure that the activities of privileged users are recorded

Initially, all privileged access to key applications, systems and network devices used to provide/support/maintain the PECN/PECS is to be logged.

By 2027, access to all applications, systems and network devices is to be logged with activity recorded and linked to operational changes and incidents.

Whilst it is becoming common to use PAM solutions to capture screen recording of activities conducted, what is required is to ensure that we record all access.

Would lateral access to other systems or at different times than usual log an event? Can access be granted based on a temporary basis based on an incident that requires resolution?

Ensure that the activities of privileged users are monitored

By 2027, it is expected that all unauthorised privileged access to key applications, systems and network devices used to provide/support/maintain the PECN/PECS is to be monitored and events raised when it happens.

A challenge within complex networks is not only when an event is logged as exceeding the permission, but also when the access is unusual.

Logs can easily be generated in the event that access is authorised/unauthorised but corealltion would be required to identify that the event was abnormal and required a reaction.

Providers should consider their ability to detect anomalous access relating to privileged access.

Ensure that the activities of 3PA users are recorded and monitored

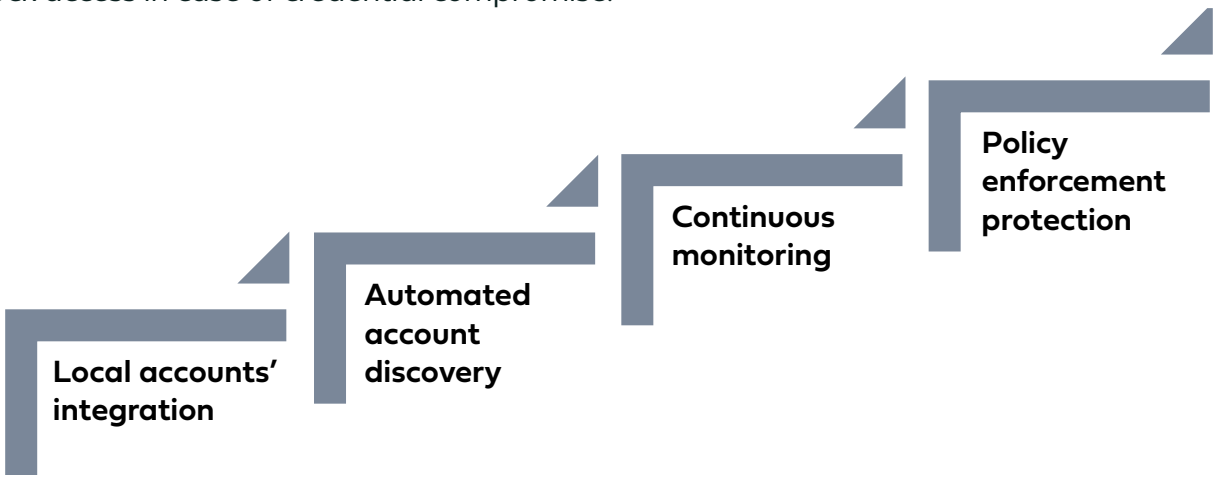
Initially, it is expected that all 3PA access to key applications, systems and network devices used to provide/support/maintain the PECN/PECS is defined in terms of who can access, what they can access and what they are allowed to do.

When have already identified that use of generic accounts is common, alongside a gap of understanding what access is required, it is important for providers to discover what type of access is required, where it is required and what is unusual behaviour to monitor.

Silverfort's Protection for Privileged Accounts per the TSF requirements?

Overview

Silverfort can help with the challenges identified to meet the requirements in a four-step process: AD integration of local Linux accounts, discovery and mapping of all domain accounts, continuous monitoring of accounts' activity, and enforcement of access policies to block access in case of credential compromise.



Let's explore these stages in detail.

Integrate Local Linux Accounts

Note: this stage is performed independently of Silverfort, and its purpose is to include privileged local Linux account in the continuous monitoring, risk analysis and access policy enforcement that Silverfort provides.

Whilst the concept of joining windows computers (servers & desktops) to Microsoft Active Directory is a standard practice for enterprise customers, allowing the centralisation of authentications for human/non-human users on Linux platforms is occasionally overlooked.

Fortunately, there are several options to provide active LDAP\directory-based authentications for Linux. Annex 1 provides a detailed description of how such an integration can take place using open-source tools.

Benefits

Bridging local Linux accounts to AD provides the following benefits:

- Consolidate identities into one source of truth (AD) allowing users to log into multiple servers vs. a local account on every server. This reduces the attack service by leveraging AD (Kerberos) for strong authentication.
- Improve IT productivity is through centralised AD administration verses the need to maintain, create/delete local accounts on each Linux server.
- Reduced overhead due to helpdesk/IT staff not having to consider resetting local account passwords across several Linux servers (as the ID & credentials are based upon AD).
- Role based access. Introduce roles and rights and their management along departmental boundaries such as HR, Finance, and Sales. Use AD to delegate administration rights according to AD group member for those department administrators.

Once integrated into AD, local Linux accounts can be subject to Silverfort's protection, which well now explore in detail.

Discovery and Visibility of Directory-Managed Accounts

Initial Discovery

Silverfort provides automated discovery for all accounts that authenticate to AD, or any other cloud or on-prem directory it connects to, as well as map their behaviours, dependencies and privilege level.

These capabilities apply equally to both native Windows domain accounts as well as to Linux accounts that were bridged to AD

Classification to privileged human and service accounts

In addition, Silverfort automates the discovery and classification of machine-to-machine service accounts. This is done by analysing accounts' behaviour and identifying the ones that feature the repetitive and pattern-like behaviour of service accounts. Following classification, all service accounts are the displayed in a dedicated screen, for easy analysis and operation.

Learning privileged users' behaviour

Silverfort learns the activities of each user account and establishes a behavioural baseline that captures the standard login activity for this user. This is extremely valuable for privileged accounts as it's the basis to spot abnormalities that indicate a potential compromise.

Continuous Monitoring and Risk Analysis

Every account authentication is monitored and analysed to disclose any potential risk it might introduce. Such risks can be either exposure to attacks such as use of insecure protocols, existence of shadow admins, etc., or attempted attack such as pass-the-hashm brute force, Kerberoasting, and others. Silverfort assigns to each authentication a risk score bases on this analysis, that can be either 'Low', 'Medium', 'High', or 'Critical'.

Account Information Display

Gathered information is displayed in three ways:

- **Log screen:** visibility into each authentication with mutliple filters such as source\ destination, username, authentication protocol, risk score, and many others.
- **Insights screen:** aggregation of all inventory and exposed attack surface risks, enabling users to easily locate and resolve them.
- **Identity Threat Detection screen:** aggregating all active threats that were detected in the monitored environment.

Export data to SIEM

Silverfort can export logs and alerts to any SIEM platform using Syslog. All the data in the logs, including customized filters can be exported.

For Splunk users, there is an enhanced output delivered by an integration app, available in the Splunk app store.

Enforcement of Access Policies

Silverfort enables its users to enforce an access policy to either alert, block, or require to step-up authentication with MFA. Silverfort architecture enables it to apply this protection to every user, resource, and access method in the AD-managed environment, even if the underlying protocol doesn't support it. In that manner, Silverfort can extend MFA to command line access, file shares and other resources that couldn't have been protected with MFA previously.

Privileged account protection: human users

Policies are configured by the users that assigns the users they apply to as well as the protected authentication's sources and destinations.

Static rule-based policies: these are policies that are triggered whenever a set of conditions is met. For example, a user or a user group accessing a certain resource.

Dynamic risk-based policies: these are policies that are triggered based on the authentication's risk score, or per the detection of specific threats.

Both types of policies support either block access, notify, or trigger MFA as a protective action.

Silverfort users can either use Silverfort's MFA app or integrated Silverfort with their existing MFA solution. These are the MFA solutions that support such integration:

- Azure MFA
- PING
- Yubico
- RSA
- Okta Verify
- DUO
- HYPR
- FIDO2

Azure AD Bridging

Silverfort also supports the management and policy configuration of AD managed accounts in Azure AD. When this feature is enabled, users can configure Conditional Access policies in Azure AD and apply them to the AD environment.

Privileged account protection: service accounts

These policies are automatically created for each account that was classified as a service account, and they reflect the account's standard behaviour. A policy can be created to either a single account or group of accounts.

Any deviation from this behaviour such as logging from or to new machines can trigger either alert or block access altogether. All the user needs to do is to choose the protective action and enable the policy.

How Do Customers Use What Is Presented?

Customers use the information gathered by using Silverfort discovery capabilities to enhance their identity secure posture by:

- **Extending MFA to all non-cloud-based applications that historically have not support MFA previously**
- **Identify any weakness in the identity attack surface that expose it to attacks, such as the use of NTLMv1 protocol, shadow admins, stale users and many more.**
- **Identify and prevent attacks that make use of compromised credentials for malicious access.**
- **Apply Virtual Fences to privileged users and services account, restricting risky user activity and stopping attackers laterally moving through the network.**

Table: Mapping Silverfort and PAM Controls for TSF Requirements

Managing authentication – Authentication involves a user providing information about who they are			
TSF references	**Key requirement**	**Silverfort**	**PAM solutions**
Specific security measures 8(2)(d) and 8(2)(e) Key concepts 2.23 and 3.37 Technical guidance measures M2.05, M6.05 and M10.48	**Ensure that default credentials are managed** The TSF requires that the passwords are changed from default on these accounts initially, with the accounts themselves being disabled from 2025 onwards.	Silverfort can discover the privileged user accounts that are used within centralised directory services, based on their privilege and activity, and enforce MFA and access based on conditions presented within the portal.	PAM solutions can scan the local devices (Windows and Linux) and the Cloud hosts (AWS, Azure and GCP) to determine the local privileged accounts on those hosts. PAM solutions can take ownership of the local and centralised privileged user accounts on hosts it manages and will usually change the passwords to ensure that you must go through the PAM solution, rotating the password on a defined basis.
Specific security measures 3(1)(c), 8(2)(b), 8(2)(g) and 8(5)(b) Key concepts 2.22-23, 2.27, 3.37, 4.7 and 6.10 Technical guidance measures M2.01-03, M2.05, M6.01-05, M10.10, M10.20, M10.48, M11.02, M11.05-07, M11.09, M11-12, M11.20, M11.35 M17.01 and M19.05-06 Cyber Assessment Framework v3.1 Indicator of Good Practice a.1.b	**Ensure that access is linked to individuals** It is expected that all access is linked to individual users by 2025, with unique accounts created which use multi-factor authentication. Break-glass access is expected to be configured by 2025, with all access to network functions is expected to use unique accounts from 2027.	Silverfort can manage all access types (including lateral movement, emergency and out-of-band access) and implement conditional MFA for the privileged user accounts that are used.	PAM solutions can take ownership of the local and centralised privileged user accounts on hosts it manages and will usually change the passwords to ensure that you must go through the PAM solution, rotating the password on a defined basis, but access is only single factor on the managed node (which is mitigated on the rotation of password). PAM solutions do not enforce MFA on the hosts themselves but rely on password rotation as a mitigation for MFA being solely applied at the solution itself.

Managing authentication – Authentication involves a user providing information about who they are			
TSF references	**Key requirement**	**Silverfort**	**PAM solutions**
Specific security measure 8(5)(a) Key concepts 2.27, 2.47 and 4.7 Technical guidance measures M2.01, M2.03, M6.01-02, M6.04, M11.02, M11.05-07, M11.09, M11.11-12, M17.01 and M19.01 Cyber Assessment Framework v3.1 Indicator of Good Practice a.1.b	**Ensure that credentials are managed** By 2025, it is expected that all user accounts that are in regular use will be stored in a centralised location; static credentials (such as break glass usernames/passwords and certificates or other secrets) are to be stored in hardware-backed storage by 2027.	Silverfort can integrate with any centralised directory service in mainstream use, both on-premise and in-Cloud, to provide conditional access wherever the privileged users attempt access (both in and out of band). Silverfort ensures that the use of privileged users for emergency access can be constantly managed, with conditional access approved where any node is capable of using a central directory without losing control.	PAM solutions can provide a centralised directory for in-band BAU access but do not manage out-of-band emergency access for privileged user access without a network path. In the event that the managed node isn't able to access the PAM solution, then another path would have to be used for access or the credential can be checked out from the PAM solution to gain access when network is unavailable.

Managing authorisation – Authorisation involves an authenticated user being granted the access they are supposed to have			
TSF references	**Key requirement**	**Silverfort**	**PAM solutions**
Specific security measures 4(1)(a), 4(2)(a), 7(1), 8(4), 8(5)(a), 10(4) and 11(b) Key concepts 2.21, 2.26-28, 2.43, 2.47, 2.87, 3.11-12, 3.29, 4.7-08, 5.12, 5.15-16, 5.41, 6.10-11, 69-11, 6.17-19, 6.36 and 12.4 Technical guidance measures M2.01, M2.03, M4.01, M6.01-04, M10.02-03, M10.05-06, M10.08, M10.10, M10.18, M10.20-35, M11.02, M11.04-07, M11.08-09, M11.11-12, M11.15, M11.35, M13.09, M13.24, M13.26, M15.06-08, M15.10, M16.01, M16.06-07, M16.12, M17.01 and M21.02 Cyber Assessment Framework v3.1 Indicators of Good Practices a.1.b and a.2.a	**Ensure that the access of privileged users is defined and implemented** Initially, it is expected that all access for privileged access is formally defined and reviewed, including roles and responsibilities. This requirement includes definition of the access that third-party administrators (3PAs) are expected to have, including to network/user data and information. By 2027, it is expected that all privileged access is shown to be defined from formal templates; management access to network oversight functions and virtualised functions/workloads is expected to be limited to those who require it by then as well.	Silverfort can discover the privileged user accounts that are used, and how they are used. Silverfort can not only define a baseline for privileged and service accounts but also identify user accounts that are being used a service accounts. These baselines can be used to easily the define not only the roles, but also the conditions that apply to privileged/service users both in terms of MFA but also time and host-based. Silverfort therefore lends itself to managing dynamic 3PA access as well, reacting to emergency access requirements for break glass accounts within the control envelope of the organisation.	PAM solutions are primarily reliant on the knowledge presented to them regarding the privileged and service accounts within the organisations. Whilst local privileged accounts can be discovered, PAM solutions will implement the roles and responsibilities for access to privileged accounts that are defined from discovery exercises. Some PAM solutions can interrogate mainstream SIEM solutions for successful logins, using the account names to determine if privileged access has been used outside of the PAM solutions control (or if the PAM solution is not managing hosts) and report back to the SIEM as an event.

Managing authorisation – Authorisation involves an authenticated user being granted the access they are supposed to have			
TSF references	**Key requirement**	**Silverfort**	**PAM solutions**
Technical guidance measures M11.02, M11.10-12	**Ensure that break-glass access is managed** Whilst break-glass accounts are expected on all applications, systems and network devices that require them from 2025, the management of break glass is expected to be evidenced by 2027. This management is expected to include controlling access to the accounts themselves, ensuring that alerts are raised when they are used and that they are reset after use. It is also expected that processes to allow for the temporary suspension of existing privileged access controls, including alerting and reset of the controls, is evidenced by this time.	Silverfort can integrate with any centralised directory service in mainstream use, both on-premise and in-Cloud, to provide conditional access wherever the privileged users attempt access (both in and out of band). Silverfort ensures that the use of privileged users for emergency access can be constantly managed, with conditional access approved where any node is capable of using a central directory without losing control.	PAM solutions can provide a centralised directory for in-band BAU access but do not manage out-of-band emergency access for privileged user access without a network path. In the event that the managed node isn't able to access the PAM solution, then another path would have to be used for access or the credential can be checked out from the PAM solution to gain access when network is unavailable. Some PAM solutions can automatically reset the passwords of the accounts that have been checked out once the host reconnects to the solution.
Specific security measures 3(3)(d), 8(6)(a)/(b) and 7(4)(b) Key concepts 2.16-17, 2.21, 2.23-28 2.49, 4.3-5, 5.12, 6.9-11, 6.17-19 and 12.4 Technical guidance measures M2.01, M2.05, M6.01, M6.04-05, M10.05-06, M10.08, M10.10-13, M10.17-18, M10.20-35, M11.02-04, M11.08-09, M11.12, M11.14-15, M11.17, M11.25, M15.06, M15.09, M21.01 and M21.04 Cyber Assessment Framework v3.1 Indicator of Good Practice a.1.b	**Ensure that technical architectures are used to control access** The initial expectation is for providers to prevent direct access from 3PAs into their applications, systems and network devices using meditation points, with providers expected to separate 3PAs by 2027. All direct access to these devices is expected to evidenced as mediated with 'browse-down' architectures by 2027 as well.	Silverfort can manage all access types (including lateral movement, emergency and out-of-band access) and implement conditional MFA for the privileged user accounts that are used.	PAM solutions can only control the activity of privileged users on the hosts that they manage access to, with the access managed according to defined architectural principles. Lateral/onward movement to unmanaged hosts is a risk to be managed.

Managing accounting – Accounting involves recording what activities authenticated users undertake			
TSF references	**Key requirement**	**Silverfort**	**PAM solutions**
Specific security measure 6(3)(a) Key concepts 5.7 and 5.20 Technical guidance measures M2.02, M8.07, M11.13, M16.14 and M16.20	**Ensure that the activities of privileged users are recorded** Initially, all privileged access to key applications, systems and network devices used to provide/support/ maintain the PECN/PECS is to be logged. By 2027, access to all applications, systems and network devices is to be logged with activity recorded and linked to operational changes and incidents.	Silverfort provides the context surrounding the activities surrounding the activities of privileged and service user accounts, including where access is abnormal in terms of time and destination. The conditional access implemented by Silverfort can lend itself to control of access in emergency situations being managed, without breaching the control envelope.	PAM solutions are strong at recording activities within defined use of privileged users on configured hosts to monitor. In the event that privileged/service user access is undertaken beyond the credential boundaries implemented by PAM solutions, the ability of the solution to record the activity is compromised as it breaches the control envelope.
Specific security measure 6(3)(b) Key concepts 5.12, 5.14, 5.19-21, 5.37-39 and 5.42 Technical guidance measures M2.02, M10.32, M11.11, M11.13, M15.11, M16.02, M16.09, M16.13-14, M16.20-22, M19.07 and M20.01	**Ensure that the activities of privileged users are monitored** By 2027, it is expected that all unauthorised privileged access to key applications, systems and network devices used to provide/support/ maintain the PECN/PECS is to be monitored and events raised when it happens.	Silverfort natively supports the ability to maintain visibility of the activities of privileged/service users if their access is via centralised accounts, with dedicated interfaces for popular SIEM tools allowing context to be presented to monitoring teams of risky behaviour. Silverfort can reduce the time to detecting monitored activities that need further investigation.	PAM solutions can present traditional monitoring events to SIEMs, but do not monitor access outside of the control of the PAM solution. Some PAM solutions can interrogate mainstream SIEM solutions for successful logins, using the account names to determine if privileged access has been used outside of the PAM solutions control (or if the PAM solution is not managing hosts) and report back to the SIEM as an event.
Specific security measures 6(3)(a, 6(3)(b) and 7(1) Key concepts 2.26-28, 5.7, 5.12, 5.14, 5.19-21, 5.37-39 and 5.42 Technical guidance measures M2.02, M8.07, M10.06, M10.08, M10.18, M10.20, M10.22, M10.32, M11.11, M11.13, M15.11, M16.02, M16.09, M16.13-14, M16.20-22, M19.07 and M20.01	**Ensure that the activities of 3PA users are recorded and monitored** Initially, it is expected that all 3PA access to key applications, systems and network devices used to provide/support/ maintain the PECN/PECS is defined in terms of who can access, what they can access and what they are allowed to do.	Silverfort can discover the privileged user accounts that are used within centralised directory services, based on their privilege and activity, and enforce MFA and access based on conditions presented within the portal.	PAM solutions can scan the local devices (Windows and Linux) and the Cloud hosts (AWS, Azure and GCP) to determine the local privileged accounts on those hosts. PAM solutions cannot define which users will access the local privileged accounts. PAM solutions can take ownership of the local and centralised privileged user accounts on hosts it manages and will usually change the passwords to ensure that you have to go through the PAM solution, rotating the password on a defined basis, but access is only single factor on the managed node (which is mitigated on the rotation of password).

Annex #1: Bridging Linux Accounts to AD

Whilst there are commercial solutions available, we will be focusing on open source for this whitepaper and something that has been proven within project in the banks sector.

System Security Services Daemon For LINUX https://sssd.io/ is an Open Source Client for Enterprise Identity Management and the subject of our discussion today.

NOTE: UNIX Operating Systems such as Solaris 11 or AIX do not support talking to Microsoft Active Directory without a commercial solution. Vendor specific implementations allow these operating systems to use SSSD via an alternative directory known as FreeIPA.

- *FreeIPA is an integrated security information management system combining Linux, a Directory Server (LDAP), Kerberos, NTP, and DNS. It's a system that can be loosely compared to Active Directory in what it attempts to solve for UNIX. It is not an active directory and introduces another "source of truth" which is not sustainable at an enterprise level due to overheads/support as well as a large increase in effort to maintain and replicate IDs from AD to FreeIPA.*

For these operating systems in a production/enterprise environment, market research into commercial AD bridging solution is recommended.

System Security Services Daemon - Overview

The introduction of AD Bridging for Linux (SSSD) helps remove the challenges of multiple identity silos. For example: local Linux host-based authentication versus leveraging Active Directory as the source of truth.

SSSD allows Linux systems to handoff authentication for both human and 'service accounts' back to Active Directory. An additional benefit is the ability to present AD groups back to the OS allowing fundamentals such as role-based access control including centralised protection for Linux privilege elevation functions.

Annex #2: Human Users and Service Accounts – Technical Presentation of System Security Services Daemon

Authentication before SSSD

In a traditional Linux environment, non-human (and human) users are maintained and configured locally on each machine and are authenticated using the operating system local database and pluggable authentication modules (*PAM).

**NOTE: Not to be confused with Privilege Access Management*

Pluggable Authentication Modules (PAM)

PAM comprises a suite of shared libraries enabling local system administrators to choose how various applications can authenticate users. For example, a dedicated program will answer the call when a user connects to an endpoint network during login. In modern Linux based distributions, the operating system (Secure Shell Service - SSH) will answer calls involving network connections. Once SSH answer's a call, it will start a login program. It will log request a username and a password for verification against the credentials in the /etc/shadow file. PAM often creates a layer of protection between an application and the actual authentication protocol.

Privilege Elevation with *sudo (super user do)*

In addition to controlling who can login, PAM may also be configured at the OS layer to provide the ability for users or members of local Linux groups to have the ability to temporarily run specific commands in the context of an administrator.

Authentication after SSSD

Once the System Security Services Daemon has been configured, the need to maintain local users and local groups at the host level is removed. Authentication and group membership is handled by Active Directory. In combination with the configuration of the PAM service on the LINUX platform login & privilege elevation rights are centrally managed removing the need to maintain the local operating system database of users and groups.

Secure Shell Service – SSH

It is common for organisations with Linux environments to extend local authentication capabilities using the concept of SSH KEYS

A SSH key can be shared in the concept of public keys and authorized keys. EG A public key may be generated for a LINUX service account (where it is stored in the home/.ssh folder). Such keys may be distributed to other Linux Servers allowing for Service Accounts (or other users) to authenticate between local database authentication servers without additional authentication.

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could not have been protected in this way before, such as homegrown/ legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort automates the discovery of all accounts within the environment, continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

For more information, visit **silverfort.com**

About Business Secure

In an increasingly regulated world, it is tempting to look toward technology for a 'quick fix' of compliance until the next time.

Business Secure is focussed on delivering effective information governance for its customers using over almost 30 years of cumulative experience from its consultants to create effective approaches which manage exposure to the myriad of obligation risks that organisations need to address. Business Secure isn't focussed on providing jargon-filled shelfware or purely technical solutions, but using proven techniques to create evidence-based baselines with clearly understood improvement plans allied to innovative technical solutions which enhance existing spend to which allow its customers to show they are in control.

Consultants within Business Secure have over 12 years of experience of delivering compliance within Telecommunications Providers to a range of industry compliance requirements; ranging from N3, through CAS(T)/HSCN and more recently the TSR and TSF.

For more information, visit **business-secure.com**

For more information, visit **silverfort.com**