Požadavky na funkční a nefunkční vlastnosti systému PAM/PIM

Oblast	ID		Požadavek	Požadovaná vlastnost?
A		Oblast	Funkční požadavky	
	A.1	Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.	Požadované
	A.2	Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat. Systém jako celek musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivaletní certifikaci.	Požadované
	A.3	Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.	Požadované
	A.4	Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v nástroji typu ServiceDesk apod.	Požadované
	A.5	Správa řešení pomocí RestAPI	Řešení je možné spravovat pomocí RestAPI a to minimálně na úrovni: vytváření uživatelů a účtů, nastavení oprávnění, změny politik, system health monitoring, schvalování požadavků, autentizace atp.	Požadované
	A.6	Integrace s ticketing nástroji	Řešení musí umožňovat integraci s ticketing nástroji třetích stran - žádost o schválení přístupu, přístup na základě existujícího ticektu, atp.	Požadované
	A.7	Podpora MS Active Directory	Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD.	Požadované
	A.8	Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes MS Active Directory/LDAP s vícefaktorovým ověřením (minimálně MS Authenticator, PKI čipové karty, RSA ID, Radius server,...).	Požadované
	A.9	Jednotná centrální správa	Správá řešení je umožněna pomocí jednotné centrální správy. Řešení musí umožňovat konfiguraci systému pomocí RestAPI - správa uživatelů, zakládání a editace účtů, změny přihlašovacíxh údajů, terminace spojení atp.	Požadované
	A.10	Šifrování a zabezpečení dat	Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-3096. Řešení umožňuje splnit compliance požadavky pro ZoKB/VoKB, GDPR, PCI-DSS, SOX, HIPAA, atd. Šifrovací standardy musí splňovat doporučení NÚKIB "MInimální požadfavky na kryptografické algoritmy v2.0" ze dne 08.06.2022	Požadované
	A.11	Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + další oeřovací faktor (MS Authenticxator, RADIUS, PKI, certifikát, atp...). Řešení musí umožit integraci s MFA nástroji třetích stran.	Požadované
	A.12	Jednorázové povýšení oprávnění	Nástroj umožňuje povýšení oprávnění běžných (neprivilegovaných) uživatelů na koncových systémech bez nutnosti instalace agentského řešení. Řešení umožňuje povyšování oprávnění na základě požadavku, příslušnosti do AD skupiny, případně na časově omezené období.	Požadované
B		Oblast	Password Management	
	B.1	Vyhledávání a přidávání privilegovaných účtů	Řešení umožňuje vyhledávat privilegované účty v operačních systémech/Active Directory/LDAP a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí (např. AWS).	Požadované
	B.2	Ověřování hesel	Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.	Požadované
	B.3	Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bez nutnosti instalace agentů. Řešení musí podporovat změnu přihlašovacích údajů minimálně pro definované typy systémů *(viz. bod "Podpora řízení hesel a bezpečné přístupy pro systémy")* , zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele.	Požadované
	B.4	Řízení servisních účtů	Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object,...). Při přidávání účtú na návaznosti upozorňuje nebo automaticky integruje do systému. Při vynucení změny hesla je heslo propsáno i do navázných služeb.	Požadované
	B.5	Customizace Password Management	Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.	Požadované
	B.6	Vyhledání tzv. backdoor účtů a automatický onboarding	Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla.	Požadované
	B.7	Řízení hesel na Windows endpointech	Nástroj umožňuje automatickou výměnu hesel privilegovaných účtů i na koncových systémech s OS MS Windows, které nejsou standardně připojeny do korporátní sítě. Rotace hesel je vynucena lokálně v pravidelných intervalech dle bezpečnostní politiky.	Volitelné
C		Oblast	Auditing a reporting	
	C.1	Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.	Požadované
	C.2	Audit administrátorských akcí	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.	Požadované
	C.3	Přístup k reportům	Řešení musí umožnit nastavení přístupu k reportům pouze pro vybrané uživatele.	Požadované
	C.4	Export auditních dat	Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports atp.	Požadované
	C.5	Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.	Požadované
	C.6	Zabezpečení auditních záznamů	Řešení musí zajistit nesmazatelnost logů po dobu minimáně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.	Požadované
	C.7	Monitoring pomocí RestAPI	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI (pro budoucí integraci s monitoring systémy zadavatele)	Požadované
D		Oblast	Řízení vzdálených relací	
	D.1	Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace...např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace.	Požadované
	D.2	Izolace SSH relací	Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřený svými přihlašovacími údaji (možno spárovat s MS Active Directory) a bude připojen zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s AD/LDAP, RADIUS, či autentizace pomocí SSH klíče).	Požadované
	D.3	Vzdálené připojení pomocí prohlížeče	Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS (není tedy například nutné otevírat z klientské stanice např. RDP/SSH/ apod. protokoly); mezi uživatelem a jump serverem bude vždy otevřený pouze bezpečný WebSocket protokol (typicky port 443).	Požadované
	D.4	Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu pomocí tzv. Webové proxy. Řešení umožní uživateli přihlášení do vybrané webové aplikace pomocí standardního (neprivilegovaného) účtu, webová proxy následně zprostředkuje přihlášení do koncové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.	Požadované
	D.5	Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat: minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.	Požadované
	D.6	Automatické označení podezřelých aktivit v nahrávkách	Systém poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp.	Požadované
	D.7	Pozastavení/terminace relací	Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat - typ události, uživatelé (možnost nastavení výjimke na úrovni skupin v AD) a typ reakce.	Požadované
	D.8	Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).	Požadované
	D.9	Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. Volitelná je možnost označovat nahrávky relací pomocí skóre podle spuštěných aplikací, akcí a příkazů v dané relaci.	Požadované
	D.10	Analýza a detekce potenciálně	Součástí řešení je nástroj umožňující provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování - uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy, atp...	Požadované
	D.11	Detekce a blokování podezřelý	Systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření - alerting, změna přihlašovacích údajů, terminace/pozastavení relací.	Požadované

E		**Oblast**	**Architektura systému**	
	E.1	Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.	Požadované
	E.2	Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů nebo jiných bezpečných údajů.	Požadované
	E.3	Automatická instalace	Veškeré komponenty řešení musí umožňovat automatickou instalaci v cloud i on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci. Automatickou instalaci je možné řešit například pomocí Ansible roles.	Požadované
F		**Oblast**	**Podpora řízení hesel a bezpečné přístupy pro systémy**	
	F.1	Podpora systémů zadavatele	Windows 7 a vyšší (7, 8, 8.1, 10, 11), Windows Server 2008, 2012, 2016, 2019, 2022 Active Directory, HP iLO, Dell DRAC, IBM Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+ VMWare, Red Hat, Unix, AIX MS SQL, MySQL, PostreSQL, Oracle, Checkpoint, Fortinet, Cisco, Juniper, F5, Office 365, Microsoft Azure Application Keys	Požadované
G		**Oblast**	**Podpora výrobce**	
	G.1	Podpora systémů zadavatele	Systém musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů (*minimálně v rozsahu viz. bod: "Podpora řízení hesel a bezpečné přístupy pro systémy")* . Případně poskytuje možnost konfigurace a vývoje vlastních konektorů pro změnu hesel a vzdálených přístupů.	Požadované
	G.2	Seznam podporovaných systémů	Výrobce musí poskytovat veřejně dostupný seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM, atp.	Požadované
	G.3	MFA - multi factor autentizace	Řešení musí podporovat integraci s nástroji třetích stran pro vynucení multi factor autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA, atp.	Požadované
	G.4	SIEM integrace	Systém musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamův čase blízkém reálnému pomocí Syslog.	Požadované
	G.5	HSM integrace	Systém musí umožňovat integraci s nástroji HSM - uložení šifrovacích klíčů k databázi řešení.	Požadované
H		**Oblast**	**Podpora výrobce**	
	H.1	Konzultační služby	Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele.	Požadované
	H.2	Implementační služby	Výrobce poskytuje vlastní implementační služby v rámci projektů implementace PAM řešení na lokálním trhu.	Volitelné
	H.3	Síť certifikovaných partnerů na lokálním trhu	Výrobce garantuje síť certifikovaných partnerů na lokálním trhu, kde je zaručena technická znalost řešení, zkušenosti s implementací a řízením projektů PAM.	Požadované
	H.4	PAS Assessment tool	Výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí zadavatele, vzhledem k předem definovaným rizikům. Celý koncept PAS Assessment nástroje umožňuje zákazníkům postupné povyšování bezpečnosti a případné porovnání aktuálního stavu s anonynmním údaji tisíců zákazníků po celém světě.	Požadované
	H.5	Program zabezpečení privilegovaných účtů	Výrobce poskytuje metodiku postupného zabezpečení privilegovaných účtů, včetně osobních konzultací na lokálním trhu. Metodika popisuje základní témata a rizika svázaná s oblastí privilegovaných přístupů do IT infrastruktury a zároveň navrhuje patřičná nápravná opatření.	Požadované
	H.6	Discovery tool	Výrobce poskytuje zdarma nástroj na vyhledání privilegovaných účtů v prostředí zadavatele a s nimi svázaných zranitelností. Zároveň poskytuje vlastní konzultační služby pro vyhodnocení a před-implementační podporu.	Volitelné
I		**Oblast**	**Licenční model**	
	I.1	Druh licence	Řešení musí být dimenzované minimálně pro 300 administrátorů s možností rozšíření licence. Licence není omezena na počet koncových zařízení nebo řízených účtů. Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (active-active) s dodatečnou místní redundancí v druhé geolokaci.	Požadované
	I.2	Testovací prostředí	Licence zároveň pokrývá možnost instalace separátního trvalého testovacího prostředí s plnou funkčností a v rozsahu minimálně 10% licencovaného produklčního prostředí. HW pro testova,cí prostředí není součástí dodávky. Veškeré ostatní SW komponenty musí být součástí nabízeného řešení.	Požadované
	I.3	Licence podle druhu použití	Licencování umožňuje rozdělit uživatele na více úrovní podle typu prístupu. Minimálně typy - uživatel s plným přístupem (využívá veškeré funkce řešení); externí uživatel (využívá pouze funkce vzdáleného přístupu).	Požadované
J		**Oblast**	**Bezpečný vzdálený přístup**	
	J.1	Vícefaktorová autentizace	Řešení vynucuje bezpečnou autentizaci uživatelů s využitím vícefaktorové autentizace.	Požadované
	J.2	Šifrované spojení	Spojení mezi externím uživatelem, prostředím zákazníka a cílovým systémem musí být plně šifrované. Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem - je využit princip bezpečného 'jump' serveru.	Požadované
	J.3	Řešení bez SW agentů	Pro plnou funkcionalitu řešení není nutné instalovat agentské řešení na stanice uživatelů, ani na cílové systémy. Externí uživatelé tedy mohou bezpečně přistupovat z libovolného koncového zařízení, které podporuje spuštění webového prohlížeče. Uživatelům není vynucováno připojení pomocí VPN.	Požadované
K		**Oblast**	**Detekce a prevence útoků**	
	K.1	Vynucení nápravy probíhajícího útoku	Řešení musí umožňovat vynucení nápravy na probíhající útoky na zneužití privilegovaných účtů a přihlašovacích údajů v reálném čase (například změna přihlašovacích údajů, zaslání alertu na SIEM, atp...).	Požadované
L		**Oblast**	**Aplikační účty (řešení musí umožňovat tyto funkcionality označené jako "Požadované", licence nemusí být součástí nabídky)**	
	L.1	Bezpečná autentizace aplikací	Řešení musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů a to minimálně na úrovni - hostname/IP adresa aplikačního serveru, certifikátu, uživatele pod kterým je aplikace/skript spuštěna, cesty k aplikaci, případně vhodný hash	Požadované
	L.2	Řízení aplikačních účtů	Řešení poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Řešení umožňujě odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. Systém musí obsahovat dokmumentované API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty.	Požadované
	L.3	Lokální cache	Systém umožňuje poskytování přihlašovacích údajů aplikacím a skriptům pomocí agentského řešení, které obsahuje možnost bezpečné cache. V případě síťového výpadku bude aplikace/skript mít stále k dispozici přihlašovací údaje k privilegovanému účtu.	Požadované
	L.4	Rest API	Pro méně kritické aplikace a skripty systém umožňuje vyzvednutí přihlašovacích údajů pomocí webového volání přes RestAPI. Webový server musí umožňovat vynucení silné autentizace minimálně na úrovni hostname/IP adresa aplikačního serveru a certifikátu.	Požadované
	L.5	Vulnerability Scanners – RPA - Orchestration/Response	Řešení musí umožňovat integraci s nástroji typu Vulnerability Management, nebo RPA pro automatické a bezpečné vyzvedávání secrets pomocí API rozhraní.	Požadované
	L.6	Popis SDK	Výrobce musí poskytovat popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací.	Požadované
M		**Oblast**	**Zabezpečení koncových bodů (řešení musí umožňovat tyto funkcionality označené jako "Požadované", licence nemusí být součástí nabídky)**	
	M.1	Řízení privilegií na koncovém bodu	Řešení umožňuje řízení oprávnění uživatelů na koncových systémech (OS platformy Windows, MacOS a UX), tak aby bylo možné granulárně definovat, který příkaz, aplikaci a akci je uživatel schopný spustit a pod jakými oprávněními.	Požadované
	M.2	Schvalování privilegovaných činností	Řešení je schopné vynutit autorizaci (zadání důvodu, schvalování) pro každý úkon, který vyžaduje vyšší oprávnění, jako je spuštění aplikace vyžadující vyšší oprávnění, konfigurace systému, editace systémových nastavení atp.	Požadované
	M.3	Odstranění práv local administrator	Řešení umožňuje aby uživatel na koncovém zařízení, ať se jedná o uživatelské pracovní stanice, notebooky nebo servery, mohl pracovat pouze pod standardním neprivilegovaným uživatelským oprávněním. Veškeré požadavky na vyšší oprávnění jsou řízeny podle bezpečnostní politiky. Oprávnění jsou následně povyšována jednorázově pro vybrané aktivity.	Volitelné
	M.4	Přidělení oprávnění pro vybrané aplikace	Správce řešení může centrálně definovat, jaké aplikace budou spuštěny se standardním oprávněním, a které se budou spouštět s vyšším oprávněním. Díky této funkci je možné umožnit uživatelům bezproblémovou práci se standardními prostředky a zároveň zajistit maximální bezpečnost systému.	Požadované
	M.5	Monitoring spuštěných aplikací	Systém dokáže monitorovat spuštěné aplikace na koncových systémech a na základě monitoringu vytvářet politiky, které aplikace následně systém umožní na koncových bodech spustit a které nikoliv.	Volitelné
	M.6	Omezení oprávnění neznámých aplikací	Systém umožňuje spuštění neznámých aplikací na koncových bodech, ale v omezeném režimu (tzn. omezení práv pod kterými je aplikace spuštěna, omezení přístupu ke korporátním datům, omezení přístupu na internet). Umožňuje tedy prevenci škod způsobených neznámým malware, nikoliv závislým na detekci škodlivého kódu, ale omezením přístupů neznámé aplikace.	Volitelné
	M.7	Zabezpečení přihlašovacích údajů na koncovém bodu	Řešení umožňuje detekci a blokování aktivit, které vedou ke zcizení přihlašovaích údajů uživatelů na koncových bodech. Systém poskytuje zabezpečení minimálně na úrovni ochrany Windows credentials (SAM, LSASS, LSA, NTDS.dit,...), přihlašovacích údajů uložených v cache prohlížečů (IE, Edge, Chrome, Firefox), přihlašovacích údajů uložených v různých nástrojích pro vzdálenou správu (WinSCP, VNC, Putty,...) a případně dalších standardních nástrojích (Git, Total Commander,...).	Požadované
	M.8	Rotace přihlašovacích údajů na samostatnáých koncových bodech	Řešení poskytuje možnost správy přihlašovacích údajů i pro stanice a servery na OS MS Windows, které nejsou trvale připojeny do korporátní sítě.	Požadované