

Vladimir Vučinić, Net++ technology

WHO ARE YOU?

POWERED BY **NET++** TECHNOLOGY



Net++
TECHNOLOGY

Who are you? (Identitet je novi perimeter)



Zamak pod opsadom (anatomija napada –

Vladimir Vučinić
direktor

Napomena: slajdovi su iz maja 2019.g.



Zamak pod opsadom

Bio jednom jedan zamak u kome su srećni živeli kralj i kraljica, princ i princeza sa svojim podanicima i vernim vitezovima čuvarima zamka. Sve je bilo divno i svi su se slagali i poštovali, sve dok jednog dana **Crni Stanko**, ne odluči da napadne zamak...

Crni Stanko beše strašni i nadaleko poznati napadač, lukav, mudar i snažan. Daleko se čuo loš glas o ovom opasnom crnom vitez u koji se beše odmetnuo i njegovoj odanoj družbi.

Teško koji zamak bi odoleo njegovim napadima...



Who are you? (Identitet je novi perimeter)

- 1. Korisnik/zaposleni radi i od kuće**
Isti nalog, ali drugi uređaj, druga mreža. VPN omogućava rad? Treba li?
- 2. SaaS aplikacija**
Posao se obavlja na tuđoj infrastrukturi. Kako i da li možemo da forsiramo pravila?
- 3. Dobavljač/partner radi na svom laptop-u**
Nema naš endpoint, nema naše politike, a ima pristup (VPN-om i više nego što treba)
- 4. Napadač sa kredencijalima**
Ima pristup, sve OK, zar ne?

Granica, perimeter je bila naša mreža, naš data centar, naš rack orman.

Posao se izmestio van naše mreže.

Posao više nije unutar mreže koju branimo!

Who are you? (Identitet je novi perimeter)

“Ko si ti?” ima najmanje 3 odgovora:

Korisnik (+ AI agent od nedavno)

Uređaj

Aplikacija

Who are you? (Identitet je novi perimeter)

“Ko si ti?” dodatni odgovori:

Mreža/Lokacija

Podaci

Privilegija

Napadač više ne “buši” firewall. On kupuje (ili krade) identitet!

Phishing i ostale prevare: Lažni direktor. Ažuriranje šifre. Hitno plaćanje fakture.
Cilj: krađa kredencijala

Keylogger ili infostealer. Dark web. Iscurili i objavljeni podaci. Aktivni stari nalozi.
Cilj: kredencijali (možda i sesija).

Zaboravljeni i ukradeni uređaji. Otpisana oprema.
Cilj: naravno, kredencijali.

Upad kod dobavljača/partnera/konsultanta (treće strane, supply chain attack).
Cilj: pogađate, kredencijali.

Šta je rešenje?

Who are you? (Identitet je novi perimeter) - REŠENJA

1. **IAM (Identity and Access Management)**

2. **ZTNA (Zero Trust Network Access)**

3. **PAM (Privileged Access Management)**

4. **Threat intelligence (exposure)**

Upravljanje identitetom (IAM)

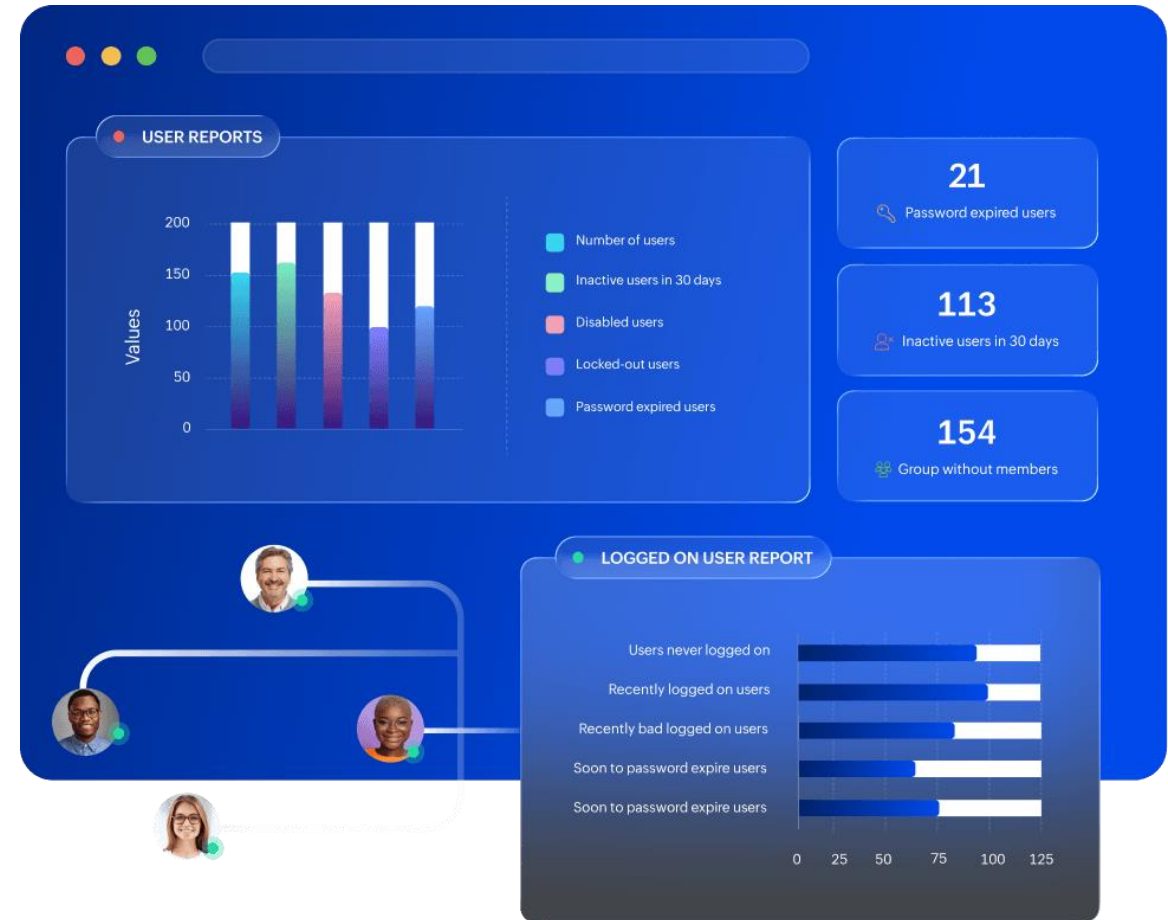
ManageEngine
AD360

ManageEngine AD360

Identity lifecycle management

Upravljanje sa korisnicima kroz intuitivnu konzolu, lakše i jednostavnije bilo da su Active Directory, Microsoft 365 ili Exchange u pitanju. Automatizujte prijem novozaposlenih (onboarding) kao i otpuštanje (offboarding), sprovedite upravljanje pristupom kroz definisane procese (workflows) i obezbedite usklađenost kroz izveštavanje. Rutinski zadaci postaju lakši, sigurniji i spremni za kontrolu.

- Centralizujte i standardizujte dodeljivanje prava za sve
- Automatizujte kritične i rutinske Active Directory poslove
- Omogućite pametnu, bezbednu i ne-intruzivnu AD delegaciju
- Ubrzajte dodeljivanje i oduzimanje prava kroz automatizaciju
- Na raspolaganju vam je preko 140 ugrađenih izveštaja što daje bolju vidljivost i lakše postizanje usklađenosti



ManageEngine AD360

Kontinualna usklađenost

Kontinualno pratite aktivnosti korisnika, promene u direktorijumu kao i prava pristupa kako bi obezbedili usklađenost sa regulativom. Uvid u podatke u realnom vremenu i izveštaji smanjuju rizik i demonstriraju vašu usklađenost bez napora.

- Pratite Active Directory alerte i promene
- Nadgledajte aktivnosti pristup fajlovima u vašem okruženju
- Pratite logovanje korisnika u realnom vremenu
- Detektujte anomalije i neuobičajeno ponašanje proaktivno
- Nadgledajte akcije privilegovanih korisnika
- Analizirajte događaje kako bi imali bolji uvid i pratili security trendove u organizaciji



ManageEngine AD360

Upravljanje pristupom

Omogućite korisnicima da sami upravljaju lozinkama i pristupnim podacima, uz zaštitu kritičnih sistema. Samouslužno resetovanje lozinke, jedinstvena prijava i višefaktorska autentifikacija smanjuju opterećenje IT tima, podižu nivo bezbednosti i sprečavaju incidente vezane za kompromitovane pristupne podatke.

- Uvedite prilagodljivu višefaktorsku autentifikaciju (MFA)
- Omogućite krajnjim korisnicima samouslužno upravljanje lozinkama
- Proaktivno obavestavajte korisnike o predstojećem isteku lozinke
- Bezbedno sinhronizujte lozinke između sistema
- Pojednostavite pristup jedinstvenom prijavom (SSO)
- Nametnite dvofaktorsku autentifikaciju za Windows prijave
- Omogućite korisnicima da ažuriraju podatke u direktorijumu i pretražuju zaposlene

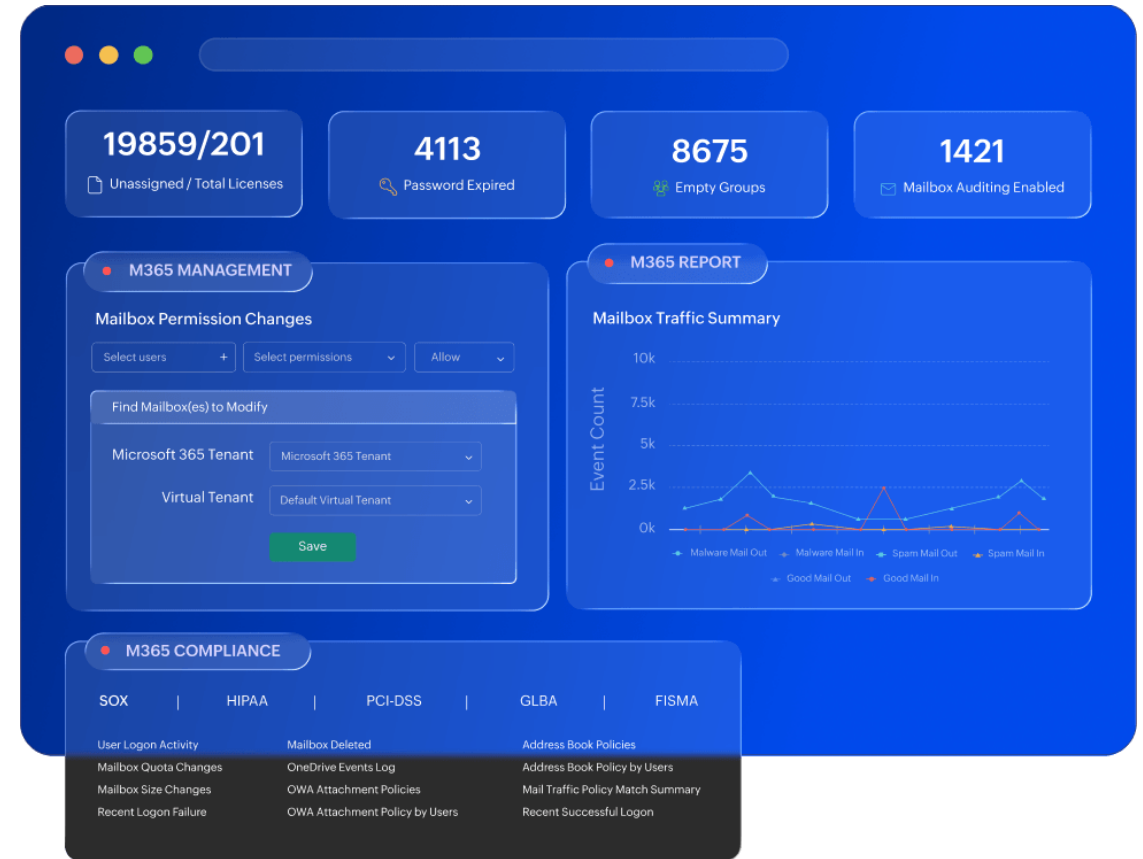


ManageEngine AD360

Hybrid identity management

Dobijte objedinjen uvid i kontrolu nad identitetima u lokalnim i cloud okruženjima. Centralizujte dodelu identiteta, upravljanje pristupom i nadzor kako biste primenjivali politike, obezbedili usklađenost i donosili odluke zasnovane na podacima u hibridnim IT sistemima.

- Objedinjeno izveštavanje i revizija u okruženjima Active Directory i Microsoft 365, uključujući Azure AD (Entra ID), Exchange, SharePoint, Teams, OneDrive i druge poslovne platforme.
- Upozorenja u realnom vremenu za kritične događaje, sumnjive aktivnosti i probleme usklađenosti.
- Centralizovana administracija sa delegiranim upravljanjem identitetima i pristupom.
- Optimizujte bezbednost identiteta, upravljanje i operativnu efikasnost u lokalnim i hibridnim okruženjima.



ManageEngine AD360

AD360 se sastoji iz 6 modula. Možete i da izaberete pojedinačne module, već prema vašim potrebama:

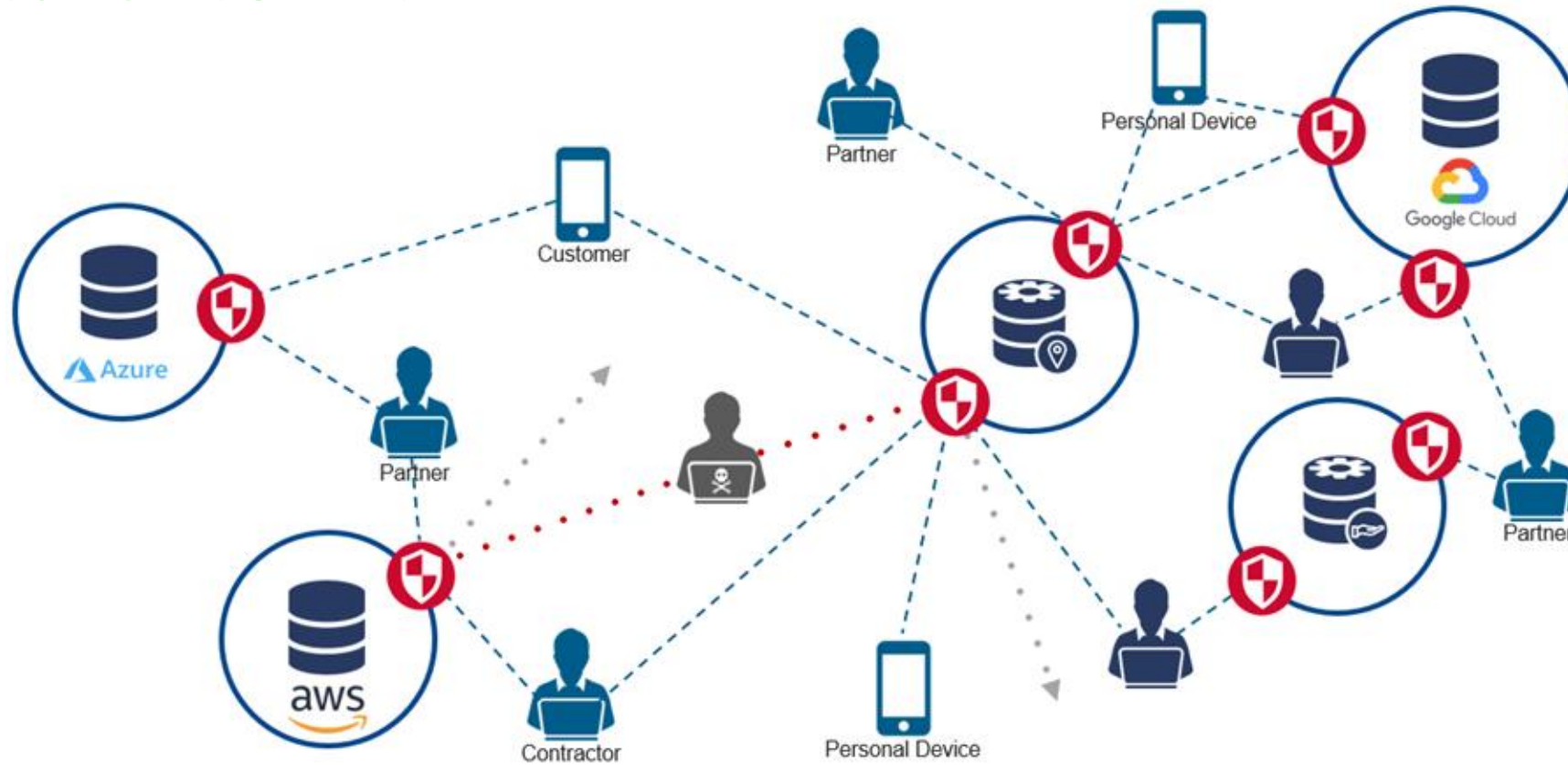
- **ADManager Plus:** AD, Exchange, and Microsoft 365 management and reporting.
- **ADSelfService Plus:** Self-service password management, and SSO and MFA implementation.
- **ADAudit Plus:** UBA-driven auditing and threat detection for AD, file servers, and Windows Servers.
- **Exchange Reporter Plus:** Reporting, auditing, monitoring, and content searching for Exchange Server, Exchange Online, and Skype for Business.
- **M365 Manager Plus:** Management, reporting, auditing, monitoring, automation, and alerting for Microsoft 365 services.
- **Recovery Manager Plus:** Enterprise backup and restoration for AD, Microsoft 365 and Exchange, Azure, and Google Workspace servers.

ZTNA

Symantec ZTNA

Symantec ZTNA

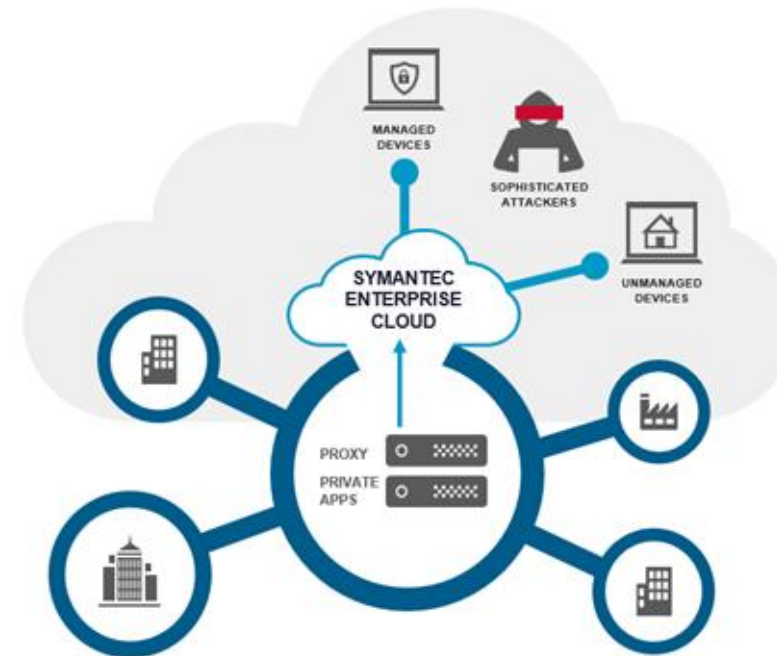
Application centric



Symantec ZTNA

Zamenite vaš VPN sa ZTNA

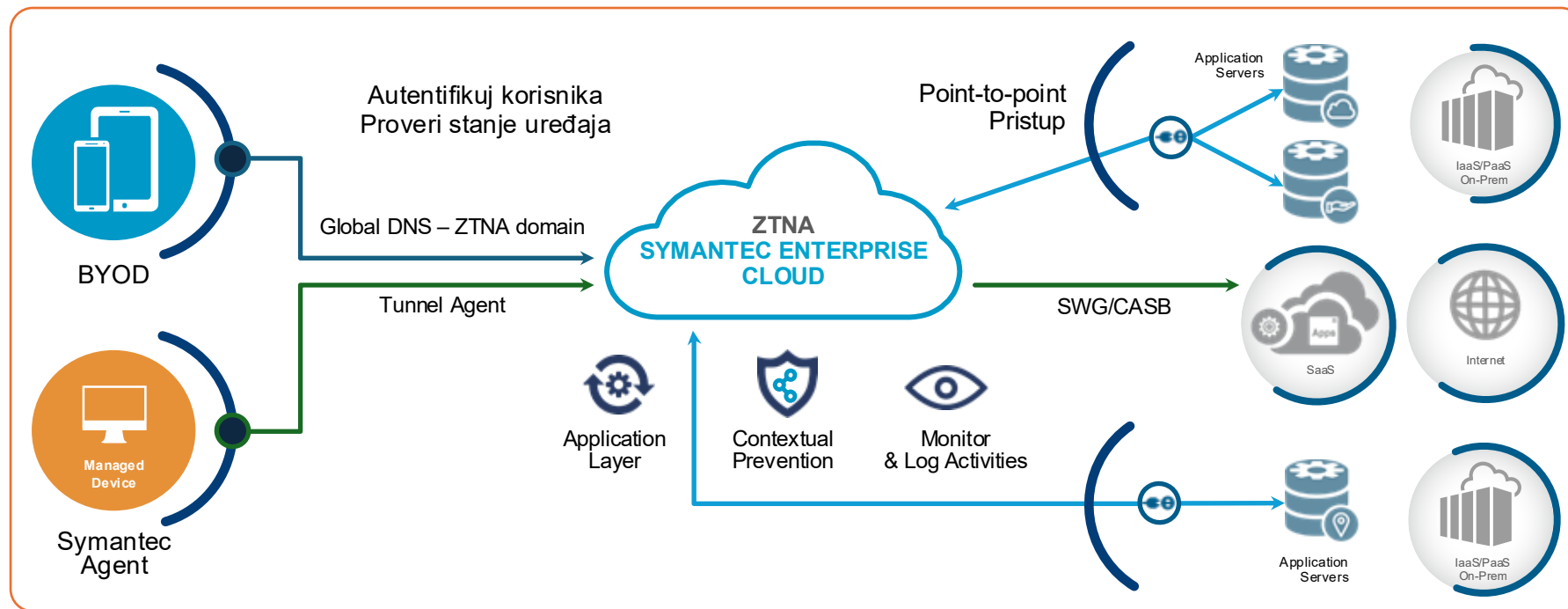
Security	Uklonite mrežnu izloženost napadima i sprečite “lateralna kretanja” Svi resursi su sakriveni i nevidljivi za korisnike koji nisu autorizovani Full Audit – svi podaci o pristup i aktivnostima su vidljivi
UX	Prava agentless podrška (uključujući native RDP & SSH) Odličan UX
OPEX	Lako upravljanje i održavanje, zahvaljujući SaaS prirodi proizvoda



Symantec ZTNA

ZTNA može da se aktivira u minutima

ZTNA radi i sa upravljivim i sa neupravljivim klijentima



Symantec ZTNA

ZTNA koristi DLP, Threat Prevention i Web Isolation



Least Privilege Access

Sprečavanje "lateralnog kretanja"

Svi resursi su sakriveni i nevidljivi za neautorizovane korisnike



Real Time Forensics

Full Audit – pristup i sve akcije su vidljive



Application Layer Protection

Inline DLP, Threat Protection, Web Isolation



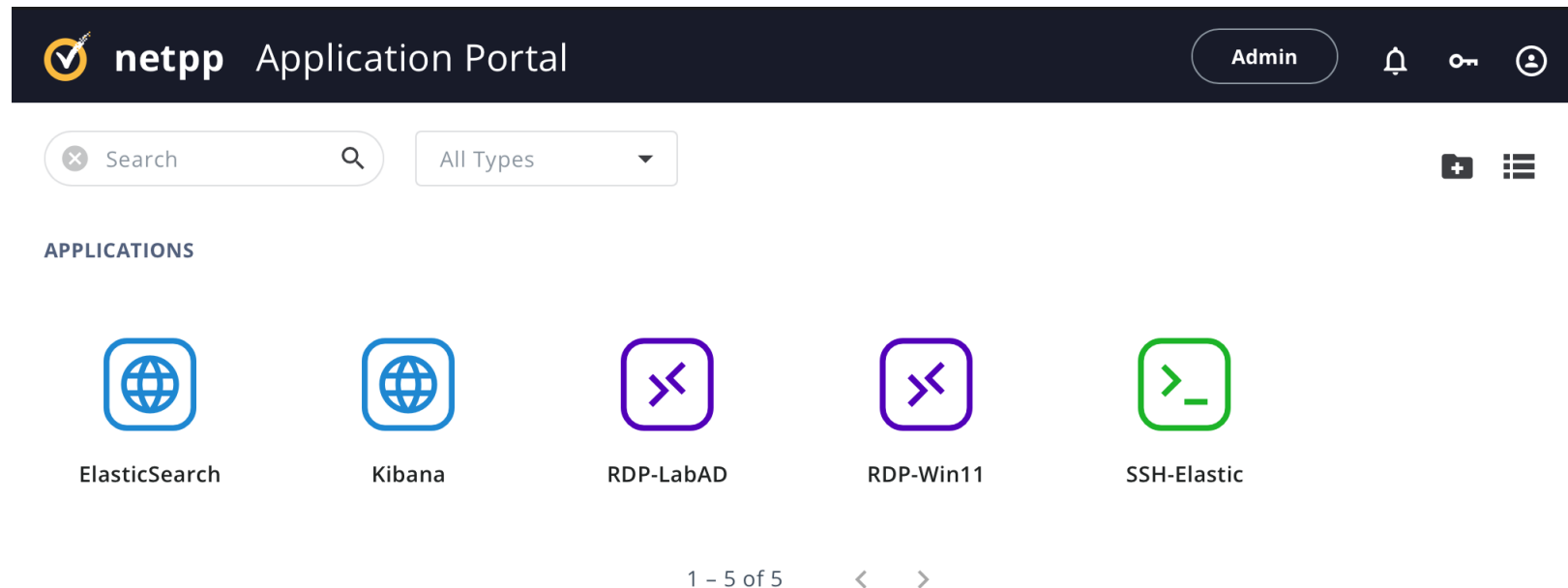
Agent or Agentless

Prava agentless podrška (uključujući native RDP & SSH)

Symantec Single Agent (takođe Mobile) podrška

Symantec ZTNA

Može li jednostavnije?



PAM

ManageEngine
PAM360

Net++
TECHNOLOGY

ManageEngine PAM360



SSL/TLS certificate i SSH key upravljanje



Privileged account and session management (PASM)



Privilege elevation and delegation management (PEDM)



Privileged user behavior analytics (PUBA)



Application credential security



Application and command control



Iscrpno izveštavanje radi usklađenosti i praćenja aktivnosti



Contextual integration with IT management tools, and business workflow automation



Secrets and workload identity management



Privileged task automation

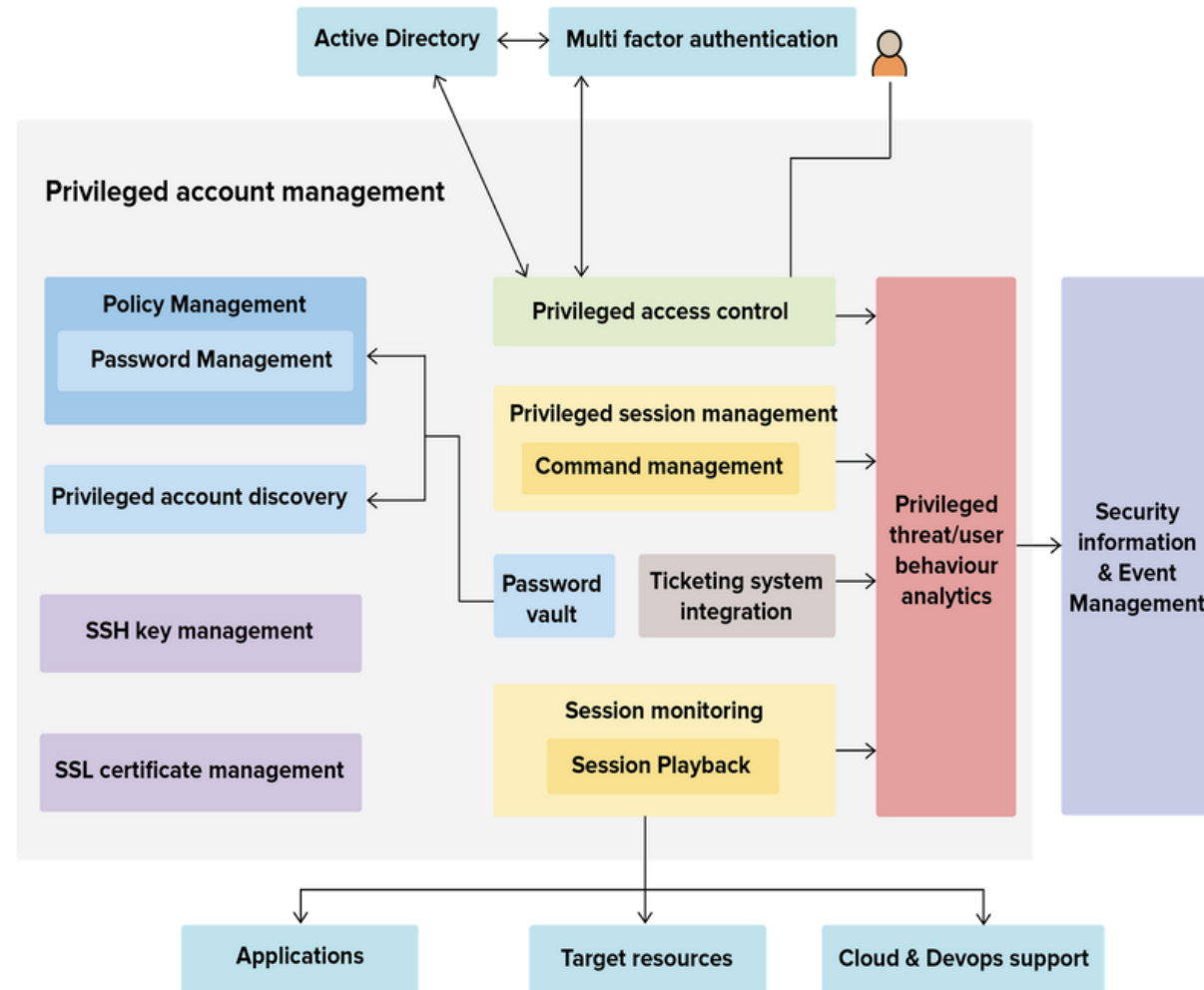


Endpoint privilege management

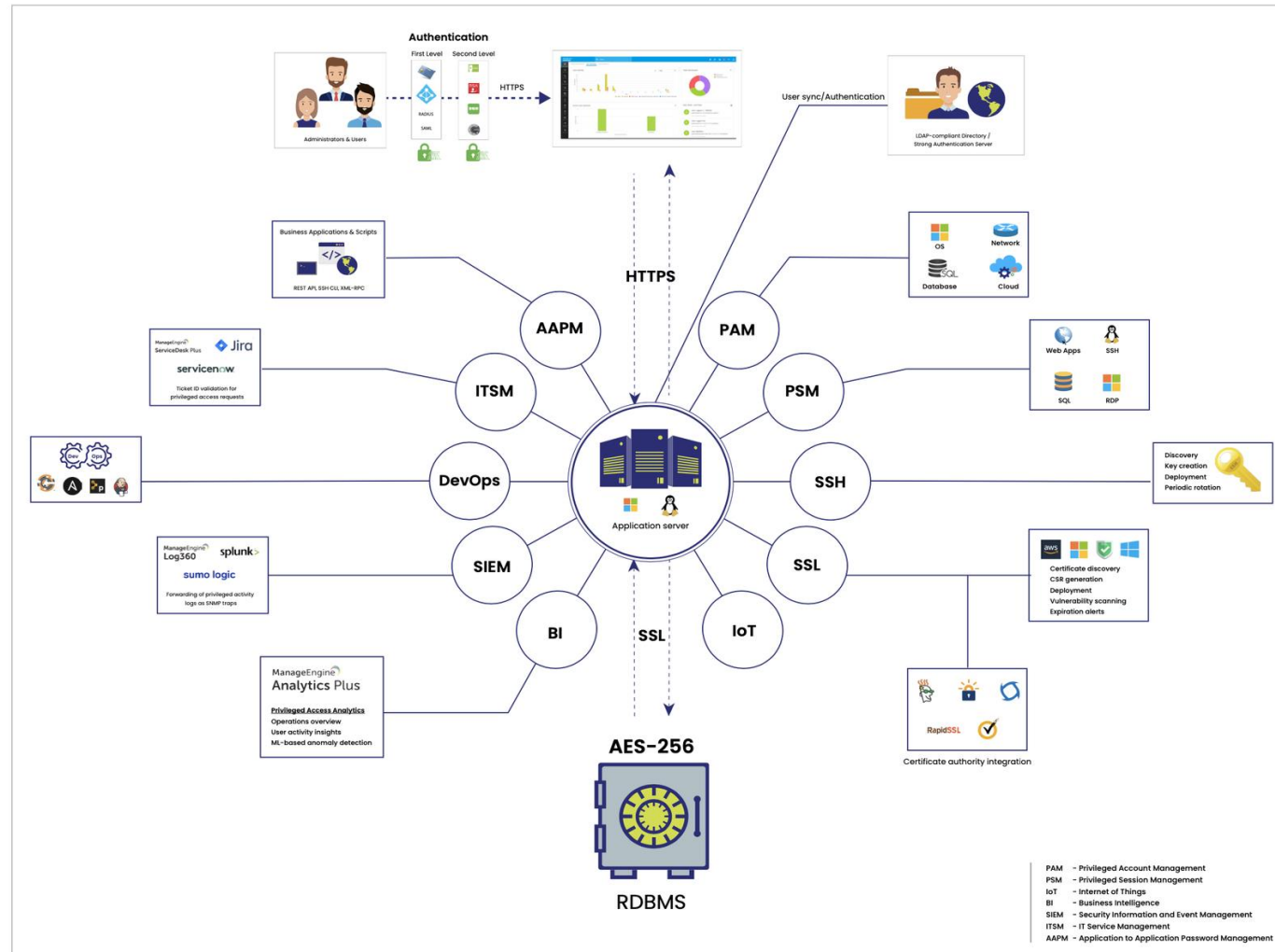


Cloud infrastructure and entitlement management (CIEM)

ManageEngine PAM360 - moduli



ManageEngine PAM360 - arhitektura



Threat intelligence

Glog Security
Predictions ili
Munit.io

Glog Security Predictions

Ključne mogućnosti

- **Attack Surface Discovery:** Maintain a continuous, zero-touch view of your digital footprint, including subdomain enumeration, technology fingerprinting, and the detection of exposed services.
- **Email Ecosystem Security:** Perform comprehensive assessments of email authentication policies (DMARC, SPF, DKIM) to prevent spoofing and ensure secure communication channels.
- **Proactive Domain Squatting Detection:** Identify brand impersonation, typosquatting, and phishing domains before they are weaponized. The system analyzes permutations and live indicators to prioritize risks to your brand.
- **Dark Web & External Threat Monitoring:** Integrate dark web feeds to anticipate emerging attack patterns and monitor for brand-specific threats.
- **Credential & Stealer Log Analysis:** Monitor for leaked credentials and analyze "stealer logs" from infected devices to identify compromised accounts before they can be used for unauthorized access.

Munit.io SAGA

Ključne mogućnosti – koji sve podatke nudi

- Dark web (forums, markets, shops)
- Comm, networks (Telegram + more)
- Social media (Facebook, Twitter + more)
- Dark web (credential leaks)
- Stealers & Leaks
- Attack surface
- Phishing and domains

HVALA!

PITANJA?

POWERED BY **NET++** TECHNOLOGY



Net++
TECHNOLOGY