DOCUMENT · PROPOSAL

پروپوزال فنی و راهبردی NexGate

استقرار پلتفرم بومی PAM روی زیرساخت سازمانی شما، بدون وابستگی به تأمین‌کنندهٔ خارجی (Vendor)، با انطباق کامل با الزامات ملی و پشتیبانی مستقیم تیم توسعه‌دهنده در تهران.

VERSION	PREPARED BY	VALID UNTIL
۲.۷	تیمِ راهبردیِ DOTECH	۳۱ شهریور ۱۴۰۵

AUDIENCE	
CEO	مدیرعامل
CISO	مدیر ارشد امنیت اطلاعات
CIO	مدیر ارشد فناوری اطلاعات
VP INFRA	مدیر زیرساخت

شروع مطالعه

دانلود PDF (/proposal.pdf)

TABLE OF CONTENTS

15

گام بعدی · جلسه مهندسی

NEXT STEPS · SIGN-OFF

EXECUTIVE ONE-PAGER

خلاصهٔ مدیریتی · ۹۰ ثانیه

مسئله

بیش از ۸۰ درصد از حملاتِ موفق، از مسیرِ حساب‌های دارای دسترسیِ بالا رخ می‌دهد. سازمان‌های ایرانی هم‌زمان با نبودِ ضبطِ نشست‌های حساس، انطباقِ ناقص با الزاماتِ نظارتیِ ملی، و وابستگی به تأمین‌کنندگانِ خارجیِ تحتِ تحریم مواجه‌اند.

راهکار

NexGate یک پلتفرمِ بومیِ PAM در قالبِ یک باینریِ Go است که ده پروتکلِ صنعتی را بومی پردازش، هر نشست را ضبط و قابلِ جست‌وجو می‌کند و گزارشِ انطباق با تقویمِ شمسی می‌دهد — تماماً درون‌سازمانی و بدونِ ارتباطِ بیرونی.

بازگشتِ سرمایهٔ تخمینی	زمانِ پیاده‌سازیِ کامل	قابلیت در ۱۰ پروتکلِ بومی
۱۲–۱۸ ماه	۱۲ هفته	۱۵۰

مطالعهٔ سندِ کامل

رزرو دموی خصوصی (/contact)

01 · EXECUTIVE SUMMARY

خلاصه اجرایی

بر اساس برآورد Forrester، بیش از ۸۰ درصد از حملات سایبری موفق به سازمان‌ها، از مسیر سوءاستفاده از حساب‌های دارای دسترسی بالا (Privileged Accounts) صورت می‌گیرد. در دو سال اخیر، سازمان‌های ایرانی با چهار چالش اصلی در این حوزه روبه‌رو بوده‌اند: عدم نظارت بر فعالیت پیمانکاران خارجی، نبود ضبط نشست‌های حساس SSH و RDP، انطباق ناقص با چارچوب‌های نظارتی ملی، و وابستگی به تأمین‌کنندگانِ خارجی (Vendor) که در شرایط تحریم، دسترسی به به‌روزرسانی امنیتی و پشتیبانی مستقیم را محدود کرده‌اند.

سامانه NexGate یک پلتفرم بومی PAM است که این چهار چالش را در یک محصول یکپارچه پاسخ می‌دهد. موتور NPE در قالب یک باینری Go، پروتکل‌های RDP، VNC، SSH، Telnet و کنسول‌های پایگاه داده را به‌صورت بومی و بدون نیاز به مؤلفهٔ جانبی یا عاملِ اجباری (Agent) پردازش می‌کند. هر نشست به‌صورت فریم‌به‌فریم با فشرده‌سازی Zstd ضبط می‌شود، محتوای ضبط با OCR قابل جستجو است و گزارش‌های انطباق با تقویم شمسی به‌صورت توکار ارائه می‌گردد.

استقرار محصول روی زیرساخت خصوصی سازمان یا کلاستر Kubernetes داخلی انجام می‌شود. هیچ ارتباطی با سرورهای بیرونی برای ارسالِ Telemetry یا اعتبارسنجیِ لایسنس برقرار نمی‌شود. پشتیبانی کامل زبان فارسی از سطح پنل مدیریتی تا مستندات فنی، از ابتدا در طراحیِ محصول لحاظ شده است.

۱۵۰
قابلیت مستند و قابل ممیزی در پنل مدیریتی

۱۰
پروتکلِ بومی بدون نیاز به تأمین‌کنندهٔ خارجی

۶۰ ثانیه
زمان نصب پایه روی کلاستر k3s

02 · STRATEGIC PROBLEM

بیان راهبردی مسئله

سازمان‌های ایرانی فعال در حوزه‌های بانکی، مخابراتی و انرژی، عموماً با چهار دسته چالش مشخص در مدیریت دسترسی‌های حساس مواجه‌اند که در ادامه به‌تفصیل ارائه می‌شود:

ناتوانی در ارائه شواهد به نهاد ممیز

در زمان بازرسی سالانه نهاد ناظر یا حسابرس مستقل، ارائه ضبط جلسات کاری مدیران سامانه و پیمانکاران به‌صورت قابل استناد ممکن نیست. این وضعیت ریسک مستقیم در امتیاز انطباق ایجاد می‌کند.

حساب‌های Orphan متعلق به پیمانکاران سابق

حساب‌های پیمانکاران خارجی و داخلی پس از پایان پروژه به‌صورت خودکار غیرفعال نمی‌شوند و به‌عنوان مسیرهای بالقوهٔ نفوذ باقی می‌مانند.

وابستگی به تأمین‌کنندگانِ خارجیِ تحت تحریم

محدودیت در مسیر پرداخت، کندی فرآیند پشتیبانی و عدم دسترسی به به‌روزرسانی‌های امنیتی، چرخه عمر محصول را در سازمان متوقف می‌کند.

تعدد ابزار برای یک کاربر مدیر

هر مدیر سامانه به‌طور همزمان با شش ابزار جداگانه (Bastion، گذرگاه شعب، Password Vault ،VPN، فایل‌سرور و گزارش‌گیر) سر و کار دارد. یکپارچه‌سازی این ابزارها در یک دروازه واحد، ضرورت عملیاتی است.

هزینه مستقیم سالانه ناشی از این چالش‌ها، شامل ساعت کاری ازدست‌رفته، جریمه‌های ممیزی و ریسک نشت داده، برای یک سازمان متوسط ایرانی به‌طور تخمینی **۱۲ تا ۳۰ میلیارد تومان** برآورد می‌شود.

03 · HOW IT WORKS

چگونه NexGate کار می‌کند

هر کاربر — چه مدیرِ سامانه، چه پیمانکار — برای رسیدن به سرورهای حساس، باید از **هستهٔ NexGate** عبور کند. هیچ مسیرِ مستقیمی میانِ کاربر و سرورِ هدف باز نمی‌ماند؛ همهٔ ترافیک در یک باینریِ Go احراز، فیلتر و ضبط می‌شود.

پردازشِ پس‌زمینه	دروازهٔ SSH	API مدیریتی
سیاست‌ها	فیلترِ دستور	کنترلِ دسترسی	تأیید چندعاملی
مخزنِ رمز	ممیزی	ضبطِ نشست	جستجوی متنی

همهٔ ترافیک از این هسته عبور می‌کند — هیچ مسیرِ مستقیمی باز نمی‌ماند.

اتصالِ کنترل‌شده

سرورها و سامانه‌های هدف

TARGETS

پایگاه‌های داده

PostgreSQL · MySQL · MSSQL · Mongo · Redis

خوشهٔ Kubernetes

apiserver · etcd · k9s

سرورهای Linux / Windows

SSH · RDP · VNC · Telnet

تجهیزات شبکه

Cisco · Juniper · MikroTik

DATA LAYER · لایهٔ داده

PostgreSQL 16 | Redis 7 | ضبط + پشتیبان · S3

SECURITY · سرویس‌های امنیتی

Vault · AES-256-GCM | ClamAV | Squid

اتصالات بیرونی

هویت · LDAP/AD · SAML · OIDC ↔ SIEM · Splunk · Elastic · Syslog ↔ ITSM · JIRA · ServiceNow

SECURITY

Ed25519 برای امضا، X25519 برای تبادل کلید، AES-256-GCM برای رمزنگاری بسته‌ها.

FOOTPRINT

یک باینری، حدود ۸۰ مگابایت. مصرف پایه ۸ هستهٔ پردازشی و ۱۶ گیگابایت حافظه، تا ۱۲٬۴۸۰ نشستِ هم‌زمان در شرایطِ آزمونِ بار.

DEPLOYMENT

Helm · Kubernetes-native Chartِ امضاشده · پشتیبانی از محیط Air-Gapped و مخزن داخلی.

مدل دسترسی در سه نقش پایه طراحی شده است:

- **مدیر سامانه** از طریق مرورگر یا کلاینت SSH به دروازه متصل می‌شود و دسترسی به سرورهای هدف تنها از مسیر هسته برقرار می‌گردد.
- **پیمانکار خارجی** از طریق کیوسکِ موقت، در محدوده مجاز تعریف‌شده توسط مدیر، دسترسی موقت می‌گیرد.
- **ممیزِ مستقل** از طریق پنل گزارش‌گیری به نشست‌های ضبط‌شده و لاگ تغییرناپذیر، دسترسی فقط‌خواندنی دارد.

ده ماژولِ تخصصی، تحت یک هسته واحد.

هر ماژول به‌منظور رفع یک نقصِ ساختاری در راهکارهای رقیب بازار بین‌المللی، از پایه طراحی و پیاده‌سازی گردیده است. مجموعه ماژول‌ها در ادامه به‌تفصیل ارائه می‌شود.

MODULE · 01

موتور پروتکل بومی · NPE

هسته سامانه، یک باینری واحد به زبان Go است که ده پروتکل کاربردی صنعتی شامل SSH، HTTPS، RDP، Telnet، VNC، Kubernetes API، PostgreSQL، MySQL، Oracle، MSSQL را به‌صورت بومی پیاده‌سازی نموده است. هیچ‌گونه وابستگی خارجی به دیمن (daemon) یا پراکسی‌های جانبی وجود ندارد.

10 PROTOCOLS | SINGLE BINARY | GO 1.22

Footprint: ~80MB · Throughput: 12,480 concurrent sessions (load-test) · Latency overhead: < 4ms p99

MODULE · 02

استقرارِ توزیع‌شده‌ی مرکز و منطقه · Central + Zone

امکان استقرار چندین گرهٔ NexGate در مناطق و شعبِ مختلف، با اتصال کاملاً رمزنگاری‌شده میان آن‌ها. هر منطقه قادر به اجرای مستقل، احراز هویت محلی و ارائه گزارش خود است؛ در عین حال، سیاست‌ها از مرکز اعمال می‌گردد.

MULTI-REGION | ED25519 | X25519 | AES-256-GCM

Enrollment: mutual cryptographic identity / Failover: active-active

MODULE · 03

کیوسکِ موقت · Ephemeral Kiosk

ارائه محیط کاری ایزولهٔ کاملاً مجازی برای پیمانکاران و کاربران موقت. پس از پایان جلسه، تمامی آثار، فایل‌ها و حافظهٔ محیط به‌صورت خودکار، پاک‌سازی می‌گردد. سه سطحِ منابع (برنزی، نقره‌ای، طلایی) متناسب با نوع کاربر در دسترس است.

FULLY ISOLATED | AUTO-WIPE | 3 TIERS

Tier 1: 1GB / 1 vCPU · Tier 2: 2GB / 2 vCPU · Tier 3: 6GB / 4 vCPU

MODULE · 04

فیلتر دستوری در سطح پروتکل · Command Filtering

هر دستوری که از سمت کاربر ارسال می‌گردد، پیش از رسیدن به سامانهٔ هدف، توسط موتور فیلتر NexGate تجزیه و در برابر سیاست‌های امنیتی ارزیابی می‌شود. دستورات پرریسک به‌صورت بلادرنگ مسدود می‌شوند و رویداد کامل برای ممیزی ثبت می‌شود.

PROTOCOL-AWARE | REAL-TIME | POLICY-DRIVEN

Coverage: SQL · shell · kubectl verbs / Latency overhead: < 1ms

MODULE · 05

چارچوب گزارش‌گیری انطباقی · Compliance Spine

تولید خودکار گزارش‌های انطباقی برای پنج چارچوب نظارتی شامل ISO 27001، SOC 2 Type II، PCI-DSS v4، حفاظت از دادهٔ شخصی (قانونِ صیانت) و الزاماتِ سازمانِ افتا. هر بند گزارش، مستقیماً به شواهد ضبط‌شده در سامانه پیوند داده می‌شود و قابل ارجاع برای ممیز است.

5 FRAMEWORKS | EVIDENCE-BOUND | SCHEDULED EMAIL

SLA: گزارشِ ماهانه در کمتر از ۱۰ دقیقه تولید می‌شود / Retention: ≥ ۷ سال

MODULE · 06

هویتِ یکپارچهٔ سازمانی · Federated Identity

اتصال یکپارچه به منابع احراز هویت موجود سازمان، اعم از OpenID Connect، OAuth 2.0، SAML 2.0، Active Directory، LDAP و Keycloak درون‌سازمانی (on-premise). سیاست‌های دسترسی به‌صورت نقش‌محور، زمان‌محور، جغرافیایی و مبتنی بر آدرس آی‌پی قابل تعریف هستند.

POLICY | RBAC | MFA · TOTP | SSO

Sources: 6+ providers / Onboarding: یکپارچه / Offboarding: یکپارچه

MODULE · 07

دروازهٔ SSH و عامل محلی · SSH Gateway + Local Agent

توسعه‌دهندگان قادرند با ابزارهای آشنای خود (psql، kubectl، k9s، mysql client) از طریق یک عامل محلی سبک، به سامانه‌های هدف متصل شوند. تمامی ترافیک از هسته عبور می‌کند و تحت ضبط و فیلترینگ کامل قرار می‌گیرد.

TUI MENU | PORT 2222 | NATIVE TOOLS

Agent size: < 28MB / OS: Linux · macOS · Windows

MODULE · 08

فوروارد توکن سخت‌افزاری · Hardware Token Forwarding

توکن سخت‌افزاری احراز هویت کاربر، روی پورت USB لپ‌تاپ خود کاربر باقی می‌ماند و صرفاً عملیات امضای رمزنگاری موردنیاز، از طریق تونل امن به سامانه هدف ارسال می‌گردد. سرور راه‌دور، هیچ‌گاه به کلیدِ خصوصیِ داخلِ توکن دسترسی نخواهد یافت.

PER-OP CONSENT | REMOTE-SAFE | PER-USER

Standards: PIV · PKCS#11 / Use case: امضای دیجیتال راه‌دور بدون افشای کلید

MODULE · 09

ضبط رمزنگاری‌شده با جستجوی متنی · Encrypted Recording + OCR

ضبط کامل ویدئویی و متنی تمامی جلسات با کدکِ اختصاصیِ کم‌حجم (codec) (حدود ۲۵۰ کیلوبایت بر دقیقه، معادلِ یک‌چهارمِ حجمِ ضبطِ راهکارهای رقیب). فایل ضبط با کلید envelope encryption مخصوص همان نمونهٔ سامانه قفل می‌شود و خارج از سامانه قابل پخش نیست.

4× SMALLER | ENVELOPE ENCRYPTED | OCR INDEXED

Format: .nxr (proprietary) / Search: full-text across millions of session-minutes

MODULE · 10

بومی‌سازی کامل زنجیرهٔ تأمین · Sovereign Supply Chain

کدمنبع کامل، توسط یک تیم مهندسی مستقر در ایران توسعه یافته است. به‌روزرسانی‌ها از مخزن سازمانی کارفرما توزیع می‌شود، استقرار کاملاً درون‌سازمانی است و سرور، کلیدها و داده‌ها زیرِ کنترلِ کاملِ سازمانِ خریدار قرار می‌گیرد؛ پشتیبانی به زبان فارسی و در ساعتِ کاریِ ایران ارائه می‌شود.

PERSIAN SUPPORT | CUSTOMER-CONTROLLED | NO VENDOR LOCK

Codebase: 180,000+ LOC / Audits: 35+ / Migrations: 149 / Team: Iran-based

فهرست تفصیلی ۱۵۰ قابلیت در صفحه قابلیت‌ها → (features/)

مقایسه با راهکارهای موجود

مقایسه تفصیلی NexGate در برابر CyberArk، BeyondTrust، Wallix و راهکارهای چینیِ ممیزیِ پایگاه‌داده (DAS) در صفحه مقایسه ارائه شده است. پنج محور تمایز کلیدی محصول در بازار ایران به شرح زیر است:

1. عدم برقراری هرگونه ارتباط با سرورهای بیرونی برای Telemetry یا اعتبارسنجیِ لایسنس.
2. پشتیبانی کامل زبان فارسی در پنل مدیریتی، مستندات و گزارش‌ها از ابتدا.
3. قیمت‌گذاری ریالی و فاکتورِ رسمیِ مالیاتی، بدون ریسک نوسان ارز یا تحریم پرداخت.
4. پشتیبانی مستقیم از سوی تیم توسعه‌دهنده محصول مستقر در تهران.
5. گزارش‌های انطباق با تقویم شمسی و قالب‌های منطبق با چارچوب‌های نظارتی ملی.

مشاهده جدول کامل مقایسه فنی ← (compare/)

06 · COMPLIANCE & REGULATORY

انطباق با الزامات نظارتی

آمادگی برای ارزیابیِ سازمانِ افتا (افتای ریاست‌جمهوری)

معماریِ محصول و کنترل‌های امنیتیِ آن مطابق با چارچوبِ دستورالعمل‌های سازمانِ افتا و الزاماتِ IRBC (تداومِ کسب‌وکار و مدیریتِ ریسکِ اطلاعات) تنظیم شده‌اند. مستنداتِ پشتیبان شاملِ ماتریسِ کنترل و شواهدِ فنی برای ارائه به ارزیاب فراهم است.

ISO 27001 و ISO 27017

گزارش‌گیری خودکار برای کنترل‌های A.9 (Access Control) و A.12 (Operations Security) با خروجی قابل ارائه به ممیز.

PCI-DSS v4

پشتیبانی از الزامات بندهای ۷، ۸ و ۱۰ شامل شناسایی، تصدیق و رهگیری دسترسی به دادهٔ دارندگانِ کارت.

SOC 2 Type II

لاگ تغییرناپذیر مبتنی بر Hash Chain و گزارش‌های منظم قابل صدور برای ممیز.

الزامات نظارتیِ داخلی ایران

تطابق با ابلاغیه‌های امنیت شبکه و خدمات پرداخت، با نگاشت مستقیم به کنترل‌های پلتفرم.

07 · SUPPORT & SLA

تعهداتِ سطحِ خدمات، در قراردادِ رسمیِ سالانه.

شاخص‌های زیر، حداقلِ تعهداتِ سطحِ خدماتِ NexGate برای محیطِ تولیدِ سازمان است. شاخص‌های دقیق‌تر، در ضمیمهٔ قرارداد، متناسب با مقیاسِ پیاده‌سازی، تنظیم خواهد گردید.

PRODUCTION UPTIME · MONTHLY

۹۹٫۹۵٪

دسترس‌پذیری ماهانه

CRITICAL · INITIAL RESPONSE

< ۱۵ دقیقه

پاسخ‌گویی به حادثهٔ بحرانی

CVE · CRITICAL SEVERITY

< ۴ ساعت

انتشار patch امنیتی

OPTIONAL · MANAGED MODE

۷×۲۴

پایش خوشهٔ مشتری

سطح ۱ · حادثهٔ بحرانی

SEV-1 · OUTAGE

توقف کاملِ سامانه یا از دست رفتنِ یکی از ماژول‌های هسته. تماسِ تلفنیِ مستقیم با تیمِ پاسخ به حادثهٔ NexGate در دسترسِ شبانه‌روزی.

< ۱۵ دقیقه

INITIAL RESPONSE

سطح ۲ · اختلالِ عملکرد

SEV-2 · DEGRADATION

کاهشِ کیفیتِ خدمات بدون توقفِ کامل. کانال‌های ارتباطی شامل تیکتِ اولویت‌دار و چتِ مستقیم با مهندس پاسخ‌گو در ساعتِ کاری.

< ۱ ساعت

INITIAL RESPONSE

سطح ۳ · مشاورهٔ فنی

SEV-3 · ADVISORY

سوالاتِ پیکربندی، طراحیِ سناریوهای جدیدِ دسترسی، بهینه‌سازیِ سیاست‌ها. کانالِ ارتباطی، پورتالِ سازمانی است.

< ۲۴ ساعت

BUSINESS HOURS · IRT

به‌روزرسانیِ امنیتی

CVE · PATCH RELEASE

انتشارِ patch برای آسیب‌پذیری‌های شناسایی‌شده، با اطلاع‌رسانیِ زودهنگامِ اختصاصی به تیمِ امنیتِ سازمان و راهنمایِ کاملِ به‌روزرسانی.

< ۴ ساعت

SEV-1 CVE · CRITICAL

- دریافت رایگانِ تمامیِ به‌روزرسانی‌های امنیتی در طولِ دورهٔ قرارداد.
- گزارشِ ماهانه از وضعیتِ سرویس، رویدادهای امنیتی و توصیه‌های پیکربندی.
- دسترسی به Repository خصوصی برای دریافتِ patchهای انتشاریافته.
- کارگاهِ آموزشیِ سالانه برای تیمِ فنیِ سازمان به‌صورت حضوری یا آنلاین.

ارزش راهبردی برای مدیریت ارشد

برای CEO: کاهش ریسک اعتباری ناشی از نشت داده، انطباق کامل با الزامات نظارت ملی و حذف وابستگی به تأمین‌کنندهٔ خارجی که در شرایط تحریم، تجدید قرارداد و دریافت پشتیبانی برای آن ممکن نیست؛ و در کنار آن، کاهشِ هزینهٔ تملکِ کل (TCO) با حذفِ لایسنس‌های ارزی و یکپارچه‌سازیِ چند ابزار در یک پلتفرم — با دورهٔ بازگشتِ سرمایهٔ تخمینیِ ۱۲ تا ۱۸ ماه.

برای CISO: دیدِ ۳۶۰ درجه روی تمامی نشست‌های حساس، توانایی پاسخگویی به درخواست‌های ممیز در کمتر از یک روز کاری و کنترل متمرکز سیاست‌های دسترسی در یک پنل واحد.

برای CIO: حذف شش ابزار موازی در فرآیند مدیریت دسترسی، کاهشِ هزینهٔ عملیات (به‌طورِ تخمینی تا ۴۰ درصد) و کاهشِ چشمگیرِ ساعتِ کاریِ ازدست‌رفتهٔ مدیرانِ سامانه.

برای مدیر زیرساخت: استقرار با Helm روی کلاسترهای k3s یا Kubernetes در کمتر از یک ساعت، در قالب یک Image و یک باینریِ واحد، با مسیرِ سادهٔ ارتقا به نسخه‌های بعدی.

اعدادِ مالیِ این بخش، برآوردِ تخمینی بر پایهٔ سازمان‌های مشابه است و رقمِ نهایی پس از ارزیابیِ سناریوی سازمانِ شما تعیین می‌شود.

09 · RETURN ON INVESTMENT

محاسبهٔ بازگشتِ سرمایه

نمونهٔ زیر برای سازمانی با ۲۰۰ کاربرِ هم‌زمان مدل‌سازی شده است. اعداد **تخمینی** و صرفاً جهتِ نمایشِ منطقِ بازگشتِ سرمایه‌اند؛ رقمِ دقیق پس از ارزیابیِ سناریوی سازمانِ شما تعیین می‌شود.

هزینهٔ فعلیِ سالانه (مجموع)

۱۲ تا ۳۰ میلیارد تومان

جریمه‌های ممیزی ۳ تا ۸ + ساعتِ کاریِ ازدست‌رفته ۴ تا ۱۰ + ریسکِ نشتِ داده ۵ تا ۱۲ میلیارد تومان.

سرمایه‌گذاری در سالِ اول

لایسنس + استقرار + آموزش

لایسنسِ سالانهٔ ریالی، هزینهٔ پیاده‌سازیِ ۱۲ هفته‌ای و آموزشِ تیمِ داخلی.

صرفه‌جوییِ خالص از سالِ دوم

حذفِ هزینهٔ ارزی

حذفِ هزینهٔ تأمین‌کنندهٔ خارجی، کاهشِ زمانِ ممیزی از سه هفته به سه روز، و کاهشِ ریسکِ مالیِ نشتِ داده.

دورهٔ بازگشتِ سرمایه (تخمینی)

۱۲ تا ۱۸ ماه

مدیریتِ ریسکِ پیاده‌سازی

چهار ریسکِ اصلیِ هر پروژهٔ استقرارِ PAM و راهکارِ متناظرِ NexGate برای کاهشِ آن:

RISK 01

اختلال در سرویس‌های فعلی هنگامِ مهاجرت

کاهش: مهاجرتِ مرحله‌ای: ابتدا روی محیطِ آزمایش، سپس سامانه‌های غیربحرانی و در نهایت سامانه‌های حیاتی.

RISK 02

مقاومتِ کاربران در برابرِ تغییرِ ابزار

کاهش: حفظِ ابزارهای آشنای کاربران (kubectl، psql، کلاینتِ RDP) از طریقِ گذرگاهِ SSH و کیوسکِ موقت.

RISK 03

وابستگی به یک تأمین‌کنندهٔ داخلی

کاهش: استقرارِ کاملاً درون‌سازمانی؛ سرور، کلیدها و داده‌ها زیرِ کنترلِ سازمانِ خریدار، بدونِ هیچ ارتباطی با بیرون.

RISK 04

ناهماهنگی با زیرساختِ موجود

کاهش: پشتیبانی از تمامیِ منابعِ هویتی (OIDC، SAML، AD، LDAP) و SIEMهای رایج (Syslog، Elastic، Splunk) از روزِ اول.

شرایط تجاری و قیمت‌گذاری

مدلِ قیمت‌گذاریِ NexGate بر اساسِ سه فاکتورِ اصلی تعیین می‌شود: **تعدادِ کاربرانِ هم‌زمان**، **تعدادِ منابعِ هدفِ تحتِ پوشش** (سرور، پایگاهِ داده، تجهیزِ شبکه) و **سطحِ پشتیبانیِ انتخابی** (استاندارد، حرفه‌ای یا Managed). قراردادها به‌صورتِ سالانهٔ ریالی منعقد می‌شود و امکانِ پرداختِ مرحله‌ای متناسب با فازهای پیاده‌سازی فراهم است.

BRANCH

طرحِ شعبه

استقرارِ تک‌نقطه‌ای، تا سقفِ ۵۰ کاربرِ هم‌زمان.

پشتیبانیِ استاندارد

ENTERPRISE

طرحِ سازمانی

استقرارِ توزیع‌شدهٔ مرکز و منطقه، تا ۵۰۰ کاربرِ هم‌زمان.

پشتیبانیِ حرفه‌ای

NATIONAL

طرحِ ملی

زیرساخت‌های کلانِ ملی و چندمنطقه‌ای، با کاربرِ نامحدود.

پشتیبانیِ Managed

سه طرحِ بالا نمونه‌اند؛ پیکربندی و قیمتِ نهایی متناسب با سناریوی سازمانِ شما تنظیم می‌شود.

PRICING REQUEST

با تکمیلِ فرمِ تماس و درجِ تعدادِ کاربر، صنعتِ سازمان و چالشِ فعلی، در کمتر از ۴۸ ساعتِ کاری پیش‌فاکتور با شرایطِ سفارشی‌سازی‌شده برای سازمانِ شما ارسال خواهد شد.

درخواست پیش‌فاکتور (/contact)

سناریوی نمونهٔ کاربرد

سناریوی زیر **فرضی ولی واقع‌گرایانه** است و صرفاً برای نمایشِ مسیرِ ارزش‌آفرینی ارائه می‌شود. یک اپراتورِ زیرساختیِ متوسط با ۱۸۰ کاربرِ ادمین، ۴۵۰ سرورِ تحتِ مدیریت، و الزامِ پاسخگویی به ممیزیِ نهادِ ناظر در هر شش ماه.

BEFORE · پیش از NexGate

- آماده‌سازیِ گزارشِ ممیزی: ۳ هفتهٔ نفر-تیم.
- شش ابزارِ موازی برای مدیریتِ دسترسی.
- دو موردِ نشتِ اعتبارنامه در سالِ گذشته.

AFTER · پس از NexGate

- آماده‌سازیِ گزارش: کاهش به ۳ روز.
- ادغامِ تمامیِ ابزارها در یک پنلِ واحد.
- چرخشِ خودکارِ رمز، ریسکِ نشتِ اعتبارنامه را به حداقل رساند.

13 · IMPLEMENTATION METHODOLOGY

روشِ پیاده‌سازی، در چهار فازِ کنترل‌شده.

روالِ پیاده‌سازیِ پیشنهادی، مبتنی بر یک متدولوژیِ ساختاریافته است که به‌منظورِ کاهشِ ریسکِ عملیاتی و تضمینِ تحویلِ نتایجِ قابلِ سنجش، در پیاده‌سازی‌های پیشین آزموده شده است.

۱

WEEK 01-02

کشف و نیازسنجی

تحلیل معماری موجود و نقشه‌برداری منابع

شناسایی کاربران، نقش‌ها و خط‌مشی‌های دسترسی

تعیین منابع هویتی موجود (AD / LDAP / Keycloak)

تدوین سند Scope-of-Work

DELIVERABLE

Discovery Report · Scope-of-Work

۲

WEEK 03-05

استقرارِ زیرساخت

نصب خوشهٔ NexGate روی محیط مشتری

اتصال به منابع هویتی موجود

پیکربندی سیاست‌های پایه و ماژول‌های ضبط

یکپارچه‌سازی با SIEM موجود

DELIVERABLE

Production-Ready Cluster · Baseline Policies

۳

WEEK 06-09

مهاجرتِ کنترل‌شده

انتقال تدریجی کاربران و سامانه‌های هدف

اعمال فیلترهای دستوری و سناریوهای انطباق

آموزش ادمین‌ها و توسعه‌دهندگان

صحت‌سنجیِ سیاست‌ها در محیطِ عملیاتی

DELIVERABLE

Migration Report · Training Records

۴

WEEK 10-12

تثبیت و انتقالِ مالکیت

اجرای ممیزی نهایی امنیتی و آزمونِ نفوذ کنترل‌شده

تولید نخستین گزارش‌های انطباق

انتقالِ مالکیتِ عملیاتیِ روزمره به تیمِ داخلی، با تداومِ پشتیبانیِ سالانهٔ NexGate

برنامه‌ریزی روالِ نگه‌داشتِ بلندمدت

DELIVERABLE

Compliance Report · Ownership Hand-Off

پرسش‌های متداول

آیا برای استفاده از NexGate نیاز به نصبِ عامل (Agent) روی سرورهای هدف است؟ +

در صورتِ قطعِ کاملِ سرورِ NexGate، آیا دسترسیِ اضطراری به سرورها ممکن است؟ +

داده‌های ضبط‌شده در چه فرمتی و کجا نگهداری می‌شوند؟ +

آیا سورس‌کد در اختیارِ سازمانِ خریدار قرار می‌گیرد؟ +

در پایانِ قرارداد، تکلیفِ داده‌های ضبط‌شده چیست؟ +

پشتیبانی در ساعاتِ غیراداری چگونه است؟ +

آیا NexGate با راهکارهای DLP و SIEM موجود ادغام می‌شود؟ +

حداقلِ زیرساختِ موردنیاز برای استقرارِ آزمایشی چیست؟ +

آیا توسعه‌دهندگان می‌توانند با ابزارهای آشنای خود کار کنند؟ +

زمانِ آموزشِ تیمِ داخلی چقدر است؟ +

SIGN-OFF · DEMO REQUEST

NEXT STEP · گامِ بعدی

گامِ بعدی، یک جلسهٔ مهندسیِ ۴۵ دقیقه‌ای است.

رزرو دموی خصوصی ↗ (contact/)

بازگشت به وب‌سایت ↗ (/)

دانلود نسخهٔ PDF ↓ (proposal.pdf/)

پس از مطالعهٔ این سند، پیشنهاد می‌گردد یک جلسهٔ فنیِ مشترک، میان تیمِ امنیت و زیرساختِ سازمانِ شما و تیمِ مهندسیِ NexGate برگزار گردد. در این جلسهٔ ۴۵ دقیقه‌ای، سامانه بر اساسِ سناریوهای واقعیِ سازمانِ شما ارائه خواهد شد و پرسش‌های فنیِ تیمِ شما مستقیماً توسطِ مهندسانِ توسعه‌دهنده پاسخ داده می‌شود.

PROPOSAL BY

تیمِ راهبردیِ DOTECH

TEHRAN · HELSINKI

CONTACT

sales@nexgate.ir
(mailto:sales@nexgate.ir)
support@nexgate.ir
(mailto:support@nexgate.ir)

REFERENCE

PROP-NXG-2026-05

VALID UNTIL · ۳۱ شهریور ۱۴۰۵
(۲۰۲۶/۰۹/۲۲)