Deep 系列

AI 原生企业安全产品技术白皮书

面向企业数字化、云原生、数据与 AI Agent 环境的
统一安全体系

2026 年 8 月

状态：V3.5 版 / 对外公开 / 合作伙伴

目录

1. 摘要与设计目标

2. 背景与行业挑战

3. Deep 系列总体产品定义

4. 总体技术架构与技术原则

5. 统一安全对象、事件与数据架构

6. 统一安全底座与共性组件

7. DeepRadar 攻击面与漏洞风险管理

8. DeepFlow 网络流量分析与威胁检测

9. DeepEdge Web 应用与 API 安全

10. DeepCore 主机、容器与云原生运行时安全

11. DeepGate 身份与特权访问安全

12. DeepVault 数据安全治理

13. DeepRoute AI 大模型智能路由与安全网关

14. DeepCTI 威胁情报与安全知识

15. DeepBrain AI 安全分析与决策

16. DeepXDR AI 安全运营与自动响应

17. 跨产品协同与典型攻击闭环

18. 部署、高可用与容灾

19. 性能与工程技术指标

20. 安全开发与供应链安全

21. 合规与标准对齐

22. 产品演进路线与研发优先级

23. 商业化与交付架构

24. 结语

附录 A：参考框架与标准

附录 B：核心术语

附录 C：典型运营场景

1. 摘要与设计目标

Deep 系列的目标不是再构建一组互相孤立的安全产品，而是建立面向企业数字化、云原生、数据与 AI Agent 的安全能力体系。其基本方法是以安全对象为坐标，以统一数据和知识为连接，以确定性安全控制保证实时防护，以 AI 提升复杂分析和决策效率，以统一运营实现发现、检测、防护、治理、响应和验证闭环。原白皮书将这一方法概括为“安全对象 + 安全知识 + AI 决策 + 统一运营”。

安全对象	产品	核心职责	关键技术路线
资产/暴露面	DeepRadar	发现、识别、扫描、风险优先级	主动/被动发现、云 API、指纹图谱、漏洞关联、EPSS/威胁情报
网络	DeepFlow	看见通信、行为与网络攻击	AF_XDP/DPDK、流表、协议解析、NDR、行为基线、加密流量分析
应用	DeepEdge	Web/API/Bot/DDoS/业务流量防护	OpenResty、Hyperscan、语义 WAF、WASM、行为风控、边缘策略
计算	DeepCore	主机/容器/K8s 运行时防护	Rust/Aya、eBPF、LSM、TC/XDP、YARA、Falco/Sigma 规则体系
身份	DeepGate	IAM/SSO/MFA/PAM/零信任	OIDC/OAuth2/SAML、WebAuthn、JIT/JEA、连续授权、工作负载身份
数据	DeepVault	发现、分类分级、权限、审计、DLP	元数据目录、内容识别、语义分类、数据库审计、UEBA/DLP
AI 数据流	DeepRoute	模型路由、Guard、DLP、Token	AI Gateway、策略引擎、Prompt/Response Guard、Token Vault
威胁知识	DeepCTI	IOC、漏洞、恶意软件、TTP、规则知识	STIX/TAXII、知识图谱、规则标准化、情报评分
安全智能	DeepBrain	关联、调查、研判、推理	Security RAG、受控 Agent、工具调用、证据链、风险推理
安全运营	DeepXDR	Incident、Case、SOAR、响应、验证	事件编排、Playbook、响应执行器、威胁狩猎、运营度量

2. 背景与行业挑战

2.1 攻击面从网络边界扩展到多安全对象

- 互联网资产已经从 IP/域名扩展到 API、微服务、SaaS、云资源、容器、临时工作负载和第三方依赖。
- 身份边界从用户扩展到服务账号、API Key、证书、机器身份、工作负载身份以及 AI Agent 身份。
- 数据从数据库和文件扩展到对象存储、数据湖、API、SaaS、RAG 向量库、Agent Memory 和 Tool/MCP 返回。
- AI Agent 可以自主调用模型、工具、数据和企业 API，使 Prompt Injection、越权调用、数据外传和供应链风险进入传统安全体系。
- 攻击链跨越应用、主机、网络、身份和数据，单一产品的告警无法解释完整攻击路径。

2.2 V3.5 的设计判断

- 不是“所有安全能力 AI 化”，而是“确定性控制 + 行为分析 + 风险计算 + AI 推理”分层。
- 不是让一个超级产品吞并全部功能，而是保持产品边界清晰，通过统一底座形成系统能力。
- 不是依赖单一数据库，而是按数据访问模式采用列式分析、事务库、全文检索、对象存储、图与向量存储。
- 不是把 Agent 当作特殊用户，而是同时将 Agent、Workload、Tool、Model、Token、Data Flow 纳入安全对象。
- 不是用 LLM 替代规则，而是让 LLM 处理复杂语义、跨域关联和调查规划，并通过策略、权限和审批限制 AI 的执行权。

3. Deep 系列总体产品定义

3.1 十大产品定位

Deep 系列由十个相互协同、可独立销售的产品组成。产品边界以安全对象和控制责任为准，避免重复建设。

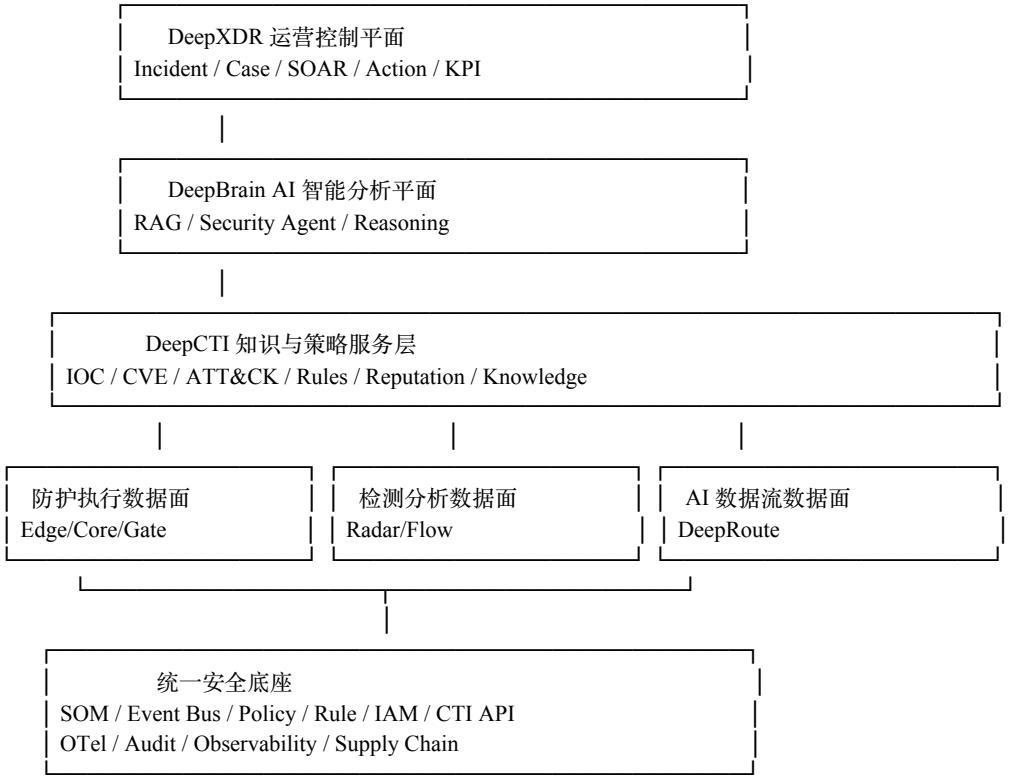
产品	一句话定位	安全对象	主要输出
DeepRadar	持续攻击面与漏洞风险管理	资产/暴露面	资产图谱、指纹、漏洞、暴露风险
DeepFlow	高性能网络流量分析与 NDR	网络/连接/协议	Flow、网络事件、威胁告警、攻击路径证据
DeepEdge	AI 原生 WAAP 与边缘安全平台	Web/API/业务流量	阻断、挑战、限流、策略、业务风险
DeepCore	AI 原生 CWPP/运行时检测与响应	主机/VM/容器/K8s	运行时事件、检测、隔离、阻断
DeepGate	统一身份、PAM 与零信任访问	用户/机器/Workload/Agent 身份	认证、授权、会话、特权控制
DeepVault	企业数据安全治理	数据库/文件/对象/AI 数据	数据目录、分类分级、访问风险、DLP
DeepRoute	AI 大模型智能路由与安全网关	Agent→LLM→Response/Tool 数据流	模型路由、Guard、DLP、Token
DeepCTI	威胁情报与安全知识平台	Threat/Vulnerability/TTP/Rule	IOC、漏洞、TTP、规则、知识 API
DeepBrain	AI 安全分析与决策引擎	跨域安全事件	Incident、Attack Story、调查计划、研判
DeepXDR	统一安全运营与自动响应控制平面	全安全对象	Case、Playbook、Action、验证、报表

3.2 产品边界原则

- DeepRadar 负责“发现与风险优先级”，不承担持续运行时防护。
- DeepFlow 负责“网络观察与检测”，不取代 DeepEdge 的在线 Web 防护。
- DeepEdge 负责“应用/网络入口数据面防护”，不承担主机 EDR。
- DeepCore 负责“计算运行时”，不承担企业级 IAM/PAM。
- DeepGate 负责“谁可以访问什么”，而 DeepRoute 负责“AI 请求以什么模型、什么策略、什么数据边界运行”。
- DeepVault 负责企业数据资产和数据治理，DeepRoute 只在 AI 数据流经过网关时实施 AI DLP。
- DeepCTI 是知识服务，不把所有产品数据复制成一份数据库。
- DeepBrain 负责分析和决策建议；确定性阻断由各产品数据面执行。
- DeepXDR 是运营控制平面，负责 Case/Playbook/Action/验证，而不是重新实现各产品检测引擎。

4. 总体技术架构与技术原则

4.1 五类技术平面



4.2 核心技术原则

1. 控制面与数据面分离：高吞吐路径不依赖 LLM、数据库事务或复杂同步调用。
2. 实时路径与异步路径分离：阻断、限流、认证等毫秒级控制与 AI 调查、知识检索解耦。
3. 规则优先、行为增强、风险融合、AI 推理：四层能力叠加而不是互相替代。
4. 统一身份：人、机器、服务、Agent、Workload 使用可验证身份建立服务间信任。
5. 零信任：任何跨产品调用都需要身份、授权和上下文，默认拒绝高风险操作。
6. 可观测性原生：Logs/Metrics/Traces/Events 统一关联，支持安全事件与业务调用链关联。
7. 供应链可信：代码、依赖、容器、规则、插件、Agent、WASM 制品均可验证来源和完整性。
8. 可回滚：规则、模型路由、策略、Agent 版本和响应动作均采用版本化与灰度机制。
9. 故障安全：核心数据面故障时优先保证业务连续性；安全控制支持 fail-open/fail-close 按策略选择。
10. AI 最小权限：AI Agent 只能获得完成任务所需的最小工具、数据、权限、预算和执行步数。

4.3 技术栈建议

领域	推荐基线	设计目的
语言	Go + Rust；前端 Vue3/TypeScript	Go 做控制面与服务编排；Rust 做高

		性能 Agent/数据面组件
网络数据面	DPDK / AF_XDP / XDP / eBPF / io_uring（按场景）	高吞吐、低延迟、减少内核/用户态拷贝
应用网关	OpenResty + LuaJIT + C/C++ 高性能库 + WASM 扩展	兼顾成熟代理能力、规则性能与安全扩展
规则/检测	Hyperscan、RE2/PCRE2、YARA、Sigma、Falco、OPA/Rego	高速特征匹配、行为检测、策略即代码
消息	Kafka 或兼容事件总线	解耦采集、检测、分析、存储与响应
流处理	Flink / 自研 Rust/Go Stream Processor	窗口聚合、状态机、实时关联
分析存储	ClickHouse	安全事件、Flow、统计与高吞吐分析
全文检索	OpenSearch	全文、日志、审计、自由检索
事务数据	PostgreSQL	租户、组织、策略、配置、Case 元数据
对象存储	S3/MinIO/OSS	PCAP、文件、样本、长期归档
图/关系	图数据库或 PostgreSQL 图扩展	资产关系、攻击路径、身份关系
向量	Qdrant/Weaviate/Milvus	Security RAG 与语义检索
身份	OIDC/OAuth2/SAML/WebAuthn; SPIFFE/SVID	用户身份与 Workload Identity
可观测性	OpenTelemetry + Prometheus/Grafana	统一 Logs/Metrics/Traces/Events
供应链	SBOM + Cosign/Sigstore + SLSA 路线	制品签名、来源验证、可追溯
部署	Kubernetes + Helm/Operator；裸机/VM 作为边缘数据面选项	云原生控制面与高性能数据面兼容

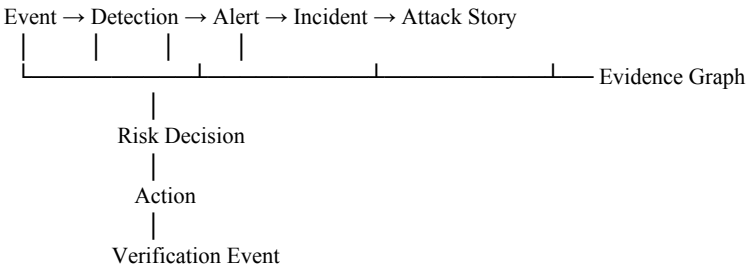
5. 统一安全对象、事件与数据架构

5.1 Security Object Model（SOM）

实体	关键字段	关系
Asset	AssetID、类型、Owner、Criticality、Lifecycle	has Service / Workload / Vulnerability / Event
Identity	IdentityID、Type、Owner、Trust Level	owns Session / Permission / Token
Workload	WorkloadID、Host、Pod、Image、Runtime	runs Process / connects Network
Application	AppID、URL、API、Tech Stack	exposes API / uses Data
Network	NetworkID、VPC、Subnet、Zone	contains Asset / carries Flow
Data	DataID、Classification、Sensitivity、Owner	accessed by Identity/Agent

Agent	AgentID、Owner、Runtime、Purpose	uses Token / calls Tool / accesses Data
Model	ModelID、Provider、Capability、Risk	invoked by Agent
Tool	ToolID、MCP/HTTP/API、Capability、Risk	called by Agent
Threat	ThreatID、IOC、TTP、Actor	targets Asset / matches Event
Vulnerability	CVE/CNVD、CVSS、EPSS、Affected	affects Asset
Event	EventID、Timestamp、Source、Entity IDs	generates Alert
Alert	AlertID、Severity、Confidence、Rule	aggregates into Incident
Incident	IncidentID、Risk、Status、Owner	contains Alerts / Actions
Action	ActionID、Type、Target、Approval、Result	changes security state

5.2 五级安全事件模型增强为“事件 + 证据 + 决策 + 动作”



V3.5 增加 Evidence Graph 概念：任何 AI 结论必须能够回溯到事件、规则、情报、资产、身份和时间线证据；任何自动响应必须能够回溯到策略、审批、执行结果和验证结果。

5.3 OTel 兼容的安全遥测

统一遥测建议兼容 OpenTelemetry 的 Logs、Metrics、Traces、Events 与 Resource 语义，使安全事件可以与应用调用链和基础设施遥测关联。OpenTelemetry 的 Semantic Conventions 为 traces、metrics、logs、profiles 和 resources 提供统一语义，事件模型也明确了 timestamp、severity、attributes 等结构。

- 所有事件至少包含 event.id、event.time、event.type、source.product、tenant.id、asset.id 或 workload.id。
- 跨系统关联使用 trace.id、span.id、session.id、request.id、incident.id 等上下文。

- 敏感字段采用 classification、redaction、hash、tokenization 标记，避免日志成为新的数据泄露面。
- 事件 Schema 版本化，支持向后兼容和多版本消费。

5.4 数据分层

数据层	主要数据	存储	典型保留
L0 原始遥测	原始日志/Packet/文件/进程事件	对象存储/边缘缓冲	按需/1 年+
L1 规范事件	SOM Security Event	Kafka + ClickHouse	30–180 天热数据
L2 检测结果	Alert/Detection	ClickHouse/OpenSearch	90 天+
L3 事件与证据	Incident/Case/Evidence	PostgreSQL + Object Storage	长期
L4 知识	IOC/CVE/TTP/Rules	CTI 专用库 + PostgreSQL	持续更新
L5 语义知识	Embedding/RAG	向量库	随知识版本更新

6. 统一安全底座与共性组件

6.1 Identity & Trust Fabric

- 用户身份：OIDC/OAuth2/SAML + WebAuthn/FIDO2。
- 服务身份：短时证书、mTLS、SPIFFE ID/SVID 路线。
- Agent 身份：AgentID + Owner + Runtime + Environment + Token。
- 工作负载身份：Kubernetes/VM/主机通过 Workload Identity 获取短生命周期凭据。
- 所有跨产品 API 使用服务身份，不使用长期静态共享密钥。

SPIFFE 提供 SPIFFE ID、SVID 和 Workload API，用于在异构环境中建立可验证的工作负载身份；SVID 可用于建立 mTLS 安全通道，因此适合作为 Deep 系列内部服务与 Agent/Workload 身份的技术参考。

6.2 Policy Fabric

- 统一策略对象：Subject、Object、Action、Context、Effect、Obligation。
- 策略分为访问策略、检测策略、响应策略、数据策略、AI 策略五类。
- 支持策略版本、灰度、优先级、冲突检测、回滚和审批。
- 策略执行尽可能在数据面本地完成，避免实时请求依赖中心控制面。
- OPA/Rego 或兼容策略即代码模型用于复杂授权和合规规则；高频数据面策略编译为本地执行结构。

6.3 Rule Fabric

DeepCTI 统一接收、清洗、去重、评分和版本化规则；各产品只消费自身需要的规则类型。规则必须具有来源、版本、置信度、适用范围、ATT&CK 映射、误报统计、回滚版本和测试样本。

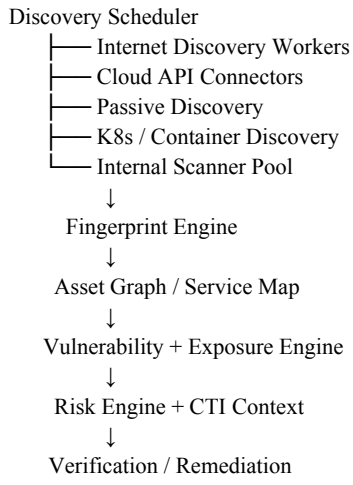
6.4 Action Fabric

动作	执行产品	安全要求
封禁 IP/域名	DeepEdge/DeepFlow	TTL、审批、幂等、自动过期
隔离主机	DeepCore	高危审批、回滚、业务白名单
禁用身份	DeepGate	JIT、双人审批、会话吊销
冻结数据访问	DeepVault	事务性、审计、最小范围
吊销 Agent Token	DeepRoute	即时吊销、缓存失效、审计
阻断 Tool	DeepRoute	Tool 风险等级、参数策略、审批
创建 Case	DeepXDR	证据自动关联
更新 CTI	DeepCTI	来源、置信度、TTL、去重

7. DeepRadar 攻击面与漏洞风险管理

DeepRadar 是企业动态攻击面地图。V3.1 已定义互联网/内网/云/K8s 资产发现、指纹、漏洞、弱口令、配置风险、暴露面监测与风险评分；V3.5 将其进一步升级为“资产图谱 + 暴露图 + 风险优先级 + 持续验证”平台。

7.1 技术架构



7.2 V3.5 增强能力

- Attack Surface Graph：将资产、域名、服务、漏洞、证书、云资源、身份和暴露关系图化。
- Exposure Path：计算“互联网入口 → 应用 → 主机 → 身份 → 数据”的潜在攻击路径。

- Continuous Validation：关键资产按风险动态调整扫描频率，而不是固定周期。
- Vulnerability Prioritization：CVSS + EPSS + CISA KEV/在野利用情报 + Asset Criticality + Exposure + Compensating Controls。
- 安全验证：高风险漏洞支持无破坏验证、虚拟补丁验证和修复后复测。
- 资产置信度：主动发现、云 API、流量、Agent、DNS 等来源形成资产置信度评分。

7.3 性能与工程目标

指标	设计目标	扩展方式
资产规模	10 万级资产周期扫描	Worker Pool 弹性扩展
紧急漏洞	支持分钟级任务编排	CTI → Scheduler 增量触发
指纹识别	规则库 + HTTP/TLS/Banner + 组件识别	无状态水平扩展
风险计算	资产变更/情报变化实时重算	事件驱动
误报治理	指纹置信度 + 多源交叉验证	反馈回流

8. DeepFlow 网络流量分析与威胁检测

DeepFlow 面向高带宽企业网络、云网络和无法安装 Agent 的设备，承担网络可见性、NDR、C2、横向移动、DNS 隧道和数据外传检测。V3.1 已将 AF_XDP、DPDK、PF_RING、零拷贝以及 100Gbps+ 集群作为设计路线；V3.5 进一步强化数据面工程。

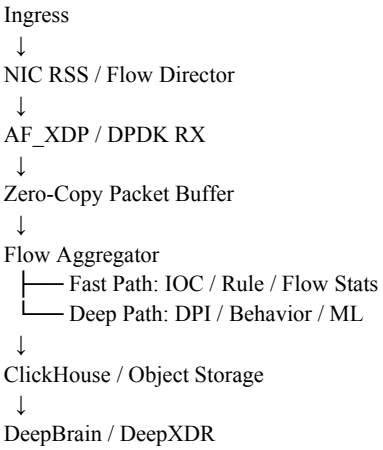
8.1 高性能数据面

- 采集：TAP/SPAN、AF_XDP、DPDK、eBPF、VPC Flow Logs、NetFlow/IPFIX。
- 分发：按 5-tuple/flow hash 做 ECMP/专用分流，保证同一会话尽量落到同一检测节点。
- 内存：固定内存池、无锁/低锁队列、NUMA-aware CPU affinity。
- 解析：先 Flow 元数据，再按风险升级到 L7 DPI，避免所有流量都做深度解析。
- 检测：规则、IOC、行为基线、统计特征和 ML 并行执行。
- 存储：Flow 元数据进入 ClickHouse；高价值 PCAP/样本进入对象存储。

8.2 加密流量分析

- 不依赖解密即可使用 TLS 版本、Cipher、SNI、证书链、JA4/JA3 类指纹、连接时序、包长分布、Beacon 周期等特征。
- 通过流行为识别 C2、隧道、异常外传和横向通信。
- 对企业可控流量可选 TLS 解密，但解密必须在授权、隐私和密钥生命周期约束下运行。

8.3 100Gbps+ 工程路线



设计目标：单节点吞吐与实际 NIC、包长、协议解析深度强相关；V3.5 不以单一“100Gbps”数字作为产品承诺，而采用可验证的 Benchmark Profile：10/25/40/100Gbps，分别定义包长分布、协议比例、规则量、采样率和 CPU 使用率。

9. DeepEdge Web 应用与 API 安全

DeepEdge 是 AI 原生 WAAP 与边缘安全数据面。V3.1 已覆盖 WAF、API、Bot、DDoS/CC、业务风控、WASM/DSL 边缘策略；V3.5 将数据面明确为 OpenResty/Nginx 高性能代理 + 高速检测库 + 行为状态机 + WASM 扩展。

9.1 防护引擎

层	技术	职责
Protocol	OpenResty/Nginx + TLS/HTTP/HTTP2/HTTP3	协议解析、连接管理、路由
Fast Rule	Hyperscan/RE2/PCRE2	高吞吐特征匹配
Semantic	结构化参数解析 + libinjection/语义特征	减少编码/语法绕过
Behavior	Session/Identity/Device/Business State	Bot、CC、账号接管、业务滥用
Risk	信誉 + 情报 + 资产 + 行为	统一风险分
AI Assist	ML/LLM 异步分析	变种、业务语义、规则生成辅助
Edge Ext	WASM/受限 DSL	自定义安全逻辑、灰度、快速回滚

9.2 WAF V3.5

- 规则库：OWASP CRS + 自研语义规则 + DeepCTI 漏洞规则 + 紧急虚拟补丁。
- 规则执行：将静态规则预编译/分组；按协议、路径、参数、风险选择性执行。

- 绕过防御：统一 URL 解码、Unicode 规范化、重复参数处理、JSON/XML 解析、Multipart 解析。
- 语义 WAF：从“正则匹配”升级到“请求语义 + 参数语义 + 数据流语义”。
- 反馈闭环：误报/漏报样本自动进入规则测试集，规则发布必须经过回归测试。

9.3 WASM 安全扩展

WebAssembly 模块在沙箱中运行，可用于扩展边缘策略而不直接暴露宿主运行时能力；其安全模型强调模块与宿主之间的隔离和受控 API。

- WASM 模块禁止任意文件、网络、进程等宿主能力，采用显式 capability。
- 模块必须签名、版本化、资源限额化，并支持灰度和自动回滚。
- 边缘策略不允许直接访问租户之外的数据。
- 安全关键规则仍由原生 Fast Path 执行，WASM 用于扩展而非替代核心 WAF。

10. DeepCore 主机、容器与云原生运行时安全

DeepCore 以 Agent + eBPF + Runtime Security 为核心，覆盖 Linux/Windows/VM/Container/K8s。V3.1 已明确 eBPF kprobe/tracepoint、LSM、Rust/Aya、Falco、OPA/Kyverno、Trivy 和实时阻断；V3.5 将其重构为“观测—检测—策略—阻断”分层运行时架构。

10.1 Agent 架构

```
DeepCore Agent
├── Collector
│   ├── eBPF Event Collector
│   ├── Windows ETW/Sysmon-compatible Collector
│   └── Container/K8s Metadata
├── Normalizer
├── Local State / Process Graph
├── Detection Engine
│   ├── Rule Engine
│   ├── Behavior Engine
│   └── Reputation Engine
├── Enforcement
│   ├── eBPF LSM
│   ├── TC/XDP
│   ├── cgroup / seccomp
│   └── OS Native Controls
└── Control Channel
    ├── Policy
    ├── Rule
    └── Upgrade
```

10.2 检测能力

- 进程：父子进程异常、Living-off-the-Land、Shell、解释器、反射加载、进程注入。
- 文件：WebShell、恶意文件、敏感目录修改、勒索加密行为、持久化。
- 网络：异常外连、C2、端口扫描、反向 Shell、横向移动。
- 身份：sudo/SUID、凭据访问、异常账号、SSH key 使用、服务账号滥用。
- 容器：特权容器、HostPath、Namespace 异常、容器逃逸、恶意镜像行为。
- K8s：Admission、RBAC、ServiceAccount、Secret 访问、危险 API、异常 Pod。
- 内核：eBPF LSM/tracepoint/kprobe 观测，关键场景使用 LSM/TC/XDP 进行阻断。

10.3 规则体系

DeepCore 统一吸收 Falco、Sigma、Wazuh、KubeArmor、Tetragon、auditd 等规则思想，转换为 Deep Runtime Rule DSL，并统一 ATT&CK 映射、严重性、条件、状态机和阻断动作。规则源不等于规则执行器；外部规则必须经过语义归一化、冲突检测、测试和签名后才能进入生产。

10.4 性能目标

指标	设计目标
CPU	正常负载 < 3%，高风险检测可按策略提升
Memory	常态 < 200MB，按模块启用动态调整
事件延迟	本地检测目标毫秒级；控制面不参与实时阻断
断网	本地缓存与断点续传
阻断	本地策略优先；云端策略作为异步更新
升级	签名验证 + 灰度 + 自动回滚

11. DeepGate 身份与特权访问安全

DeepGate 将 IAM、SSO、MFA、PAM、堡垒机、零信任访问统一到身份安全控制平面。V3.1 已明确 OIDC/OAuth2/SAML、WebAuthn、RBAC/ABAC、JIT/JEA、SSH/RDP/DB 审计和上下文授权；V3.5 增加 Workload Identity 与连续授权。

11.1 身份类型

- Human Identity：员工、管理员、外部协作人员。
- Machine Identity：API Key、证书、服务账号。
- Workload Identity：Pod、VM、服务实例。
- Agent Identity：AI Agent、Owner、Purpose、Runtime。
- Privileged Identity：数据库、Linux/Windows、网络设备、云控制台特权账号。

11.2 授权模型

```
Decision = f(
  SubjectIdentity,
  Resource,
  Action,
  DevicePosture,
  NetworkContext,
  Time,
  Risk,
  DataClassification,
  SessionHistory
)
```

- RBAC 负责稳定的角色权限；ABAC/Policy 用于上下文约束。
- JIT/JEA 默认用于高风险特权访问。
- 高风险会话支持二次认证、命令控制、实时审计和自动吊销。
- 连续授权：风险变化后重新评估，不把一次登录视为永久信任。
- Agent 权限必须同时绑定 AgentID、Owner、Environment、Purpose 和有效期。

12. DeepVault 数据安全治理

DeepVault 建立数据资产全生命周期治理能力，包括发现、分类分级、权限治理、数据库审计、DLP 和异常访问。V3.1 已覆盖数据库、文件、对象存储、SaaS 与 AI 向量库；V3.5 强调数据流图与 AI 数据治理。

12.1 数据安全架构

```
Data Sources
 ├─ DB / NoSQL
 ├─ File / Object Storage
 ├─ SaaS / API
 ├─ Data Lake / Warehouse
 └─ RAG / Vector DB / Agent Memory
      ↓
Discovery → Classification → Data Graph
      ↓
Policy / Access Risk / UEBA / DLP
      ↓
Audit → Alert → Block / Quarantine → Verify
```

12.2 分类分级

- 规则识别：正则、字典、格式、哈希、上下文。
- 语义识别：文档分类、代码/合同/财务等业务语义。
- 结构化数据：表/列/字段级敏感性。
- 非结构化数据：文件内容、OCR、元数据。

- AI 数据：System Prompt、RAG chunk、Memory、Tool Response、Model Output。

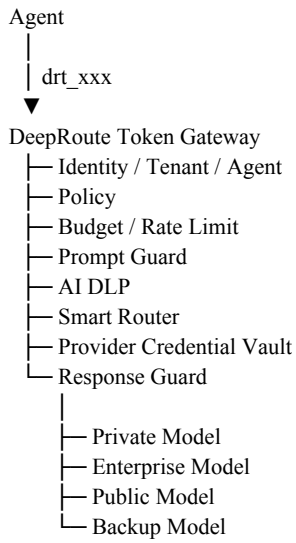
12.3 数据流图

DeepVault 不只回答“数据在哪里”，还要回答“谁、何时、通过什么应用、以什么方式访问了什么数据，并最终流向哪里”。该数据流图可与 DeepRoute 的 AI DLP、DeepGate 的身份策略和 DeepFlow 的网络行为联动。

13. DeepRoute AI 大模型智能路由与安全网关

DeepRoute 是 V3.5 中边界最明确的 AI 安全产品：只聚焦 Route + Guard + DLP + Token。原白皮书明确其目标是让 Agent 通过一个 Token 接入多个模型，并在 Prompt/Response 两侧实施安全控制；它不承担完整 Agent 主机安全、完整 IAM、企业 DLP 或全面 MCP 治理。

13.1 One Token → All Models



13.2 Smart Routing

- 能力路由：通用、推理、代码、多模态等任务选择模型。
- 风险路由：敏感数据优先企业/私有模型。
- 成本路由：预算、Token 成本和租户配额约束。
- 性能路由：延迟、负载、成功率和上下文长度。
- 可靠性路由：健康检查、Failover、Circuit Breaker。
- 策略路由：Agent/Owner/Environment/Classification/Use Case → Allowed Models。

13.3 Guard + DLP

- Prompt Guard：Prompt Injection、Jailbreak、越权指令、危险代码/URL、敏感内容。

- Response Guard：敏感信息、凭据、内部知识、违规内容。
- AI DLP：Prompt、Response、RAG、Tool/MCP 返回、Memory 五类数据流。
- 策略动作：Allow / Transform / Redact / Require Approval / Block。
- 所有阻断必须输出可解释原因、策略版本和证据。

13.4 Token 安全

- Token 绑定 AgentID、Tenant、Owner、Environment、Allowed Models、Rate Limit、Budget、Data Policy、Security Policy、Expiration。
- Token 不等于真实 Provider API Key；真实 Key 保存在安全密钥存储中。
- 支持轮换、吊销、短期 Token、Scope 和缓存失效。
- 推荐在高安全场景引入设备/Workload 身份绑定，降低 Token 泄露后的可重放风险。

13.5 MCP Gateway 边界

DeepRoute 可以对 MCP Tool 调用做认证、参数安全、DLP 与审计，但不扩展为完整 MCP 管理平台。完整 Tool 注册、资产治理和运行时执行环境仍由相关平台承担。原白皮书对此边界已有明确约束。

14. DeepCTI 威胁情报与安全知识

DeepCTI 是整个体系的横向知识底座，统一 IOC、漏洞、恶意软件、APT、TTP、规则和威胁活动知识，并通过 API/事件总线向各产品提供实时上下文。V3.1 已定义 STIX/TAXII、IOC TTL、来源评分、规则知识和 ATT&CK 映射。

14.1 知识域

知识域	核心对象	消费者
IOC	IP/Domain/URL/Hash/Email	DeepEdge/Flow/Core/Brain
Vulnerability	CVE/CNVD/CVSS/EPSS/KEV/PoC 元数据	DeepRadar/Edge/Core/XDR
Malware	Family/Hash/YARA/Behavior/C2	Core/Flow/Brain
Threat Actor	Actor/Campaign/Infrastructure/TTP	Brain/XDR
TTP	ATT&CK Technique/Sub-technique	Flow/Core/Brain/XDR
Rule	Sigma/YARA/Falco/WAF/Runtime	各检测引擎
Behavior	Beacon/Scan/Exfil/Privilege/Abuse	Flow/Core/Edge/Vault
Security Knowledge	案例/处置/FAQ/Playbook	Brain/XDR

14.2 情报质量

- 来源可信度、时效性、命中率、误报率、交叉验证。

- IOC TTL 动态化：不同类型、来源和置信度采用不同生命周期。
- 多源去重与实体合并。
- 情报 → 检测规则 → 命中 → 反馈 → 重新评分闭环。
- 支持 STIX/TAXII 与外部平台集成。

15. DeepBrain AI 安全分析与决策

DeepBrain 定位为 AI 辅助安全分析师，而不是无约束的自动攻击/阻断代理。V3.1 已定义告警降噪、攻击链重建、威胁研判、Security RAG、自然语言调查、处置方案生成和人机审批。

15.1 V3.5 Security Agent Runtime

```
Incident
  ↓
Context Builder
  ├─ SOM Entities
  ├─ CTI Knowledge
  ├─ Historical Cases
  ├─ Timeline
  └─ Evidence
  ↓
Planner
  ↓
Tool Policy Check
  ↓
Tool Call
  ├─ ClickHouse Query
  ├─ CTI Search
  ├─ Asset Lookup
  ├─ Flow Query
  ├─ Core Query
  └─ Response Simulation
  ↓
Evidence Store
  ↓
Reasoning / Risk Decision
  ↓
Human Approval / Action Proposal
```

15.2 AI 安全边界

- 工具白名单：每个 Security Agent 只拥有必要工具。
- 参数策略：工具调用参数必须经过 schema 校验和策略检查。
- 预算限制：Token、时间、步骤数、查询范围和并发数。
- 读写分离：调查 Agent 默认只读；写操作进入审批。
- 证据优先：AI 结论必须引用事件、规则、情报或查询结果。
- 模型隔离：不同安全域可使用不同模型，不把敏感数据发送到不允许的 Provider。

- Prompt/Tool 审计：记录输入、工具调用、关键中间结果和最终动作，但敏感内容按策略脱敏。

15.3 AI 可靠性

- RAG 使用混合检索：关键词 + 向量 + 图关系。
- 重要结论采用二次验证：规则/查询/第二模型交叉验证。
- 高危响应不由 LLM 单独决定。
- 所有模型、Prompt Template、RAG Index 和 Tool Schema 版本化。
- 模型升级必须经过安全回归集和幻觉/越权测试。

NIST 的生成式 AI 风险管理框架强调对生成式 AI 生命周期和风险进行系统管理，V3.5 将其思想映射到模型调用、数据治理、Agent 工具权限、评估和人机协同等环节。

16. DeepXDR AI 安全运营与自动响应

DeepXDR 是统一安全运营控制平面，汇聚全产品事件、告警、Incident 和 Action，负责调查、Case、SOAR、响应、验证和运营度量。V3.1 已定义统一告警、Incident、攻击链、资产风险、威胁狩猎、Case、SOAR 和自动响应。

16.1 SOAR 架构

```
Trigger
  ↓
Context Enrichment
  ↓
Risk / Policy Check
  ↓
Playbook
  ├─ Parallel Actions
  ├─ Approval Gate
  ├─ Conditional Branch
  └─ Retry / Timeout
  ↓
Action Executor
  ↓
Verification
  ↓
Close / Escalate / Learn
```

16.2 Action Executor

- 每个动作具备唯一 ActionID、目标、策略版本、审批记录、执行状态和结果。
- 动作必须幂等；重复执行不能扩大影响。
- 高危动作支持双人审批。
- 动作必须有超时、重试上限和回滚路径。

- 验证器负责确认风险是否消失，而不是把“命令执行成功”当成“风险已消除”。

16.3 运营 KPI

指标	V3.5 目标	说明
MTTD	已知威胁 < 5 分钟	从事件发生到检测
MTTR	高危事件 < 30 分钟	从告警到初步处置
告警闭环率	> 95%	SLA 内完成处置
误报率	< 10%（目标）	按场景分别统计
自动响应率	> 60%（成熟阶段）	仅统计允许自动化场景
高危漏洞暴露窗口	< 7 天（目标）	发现到修复/缓解
AI 结论可证据化率	> 95%（目标）	关键结论可追溯证据
响应验证率	> 95%	Action 后自动验证

17. 跨产品协同与典型攻击闭环

17.1 Web 入侵闭环

11. DeepRadar 发现暴露 Web 服务与高风险漏洞。
12. DeepCTI 提供漏洞在野利用、IOC 和 TTP 上下文。
13. DeepEdge 在入口阻断攻击并生成请求证据。
14. DeepFlow 观察 C2、横向移动和异常外连。
15. DeepCore 发现 Web 进程异常拉起 Shell、文件落地或容器逃逸。
16. DeepBrain 将多产品事件按时间、实体、TTP 和情报关联为 Incident/Attack Story。
17. DeepXDR 触发封禁、隔离、账号暂停和取证 Playbook。
18. 验证结果回流 DeepRadar、DeepCTI 和 DeepBrain。

17.2 内部数据窃取

19. DeepGate 发现异常登录与风险身份。
20. DeepVault 发现异常大批量数据访问。
21. DeepFlow 发现外传行为。
22. DeepBrain 计算影响范围和合规风险。
23. DeepXDR 联动冻结身份、数据权限和网络外传。

17.3 AI Agent 数据外传

24. DeepGate 识别 Agent 身份、Owner 和企业资源权限。
25. DeepVault 标记客户合同为高敏数据。

26. Agent 将数据放入 Prompt。
27. DeepRoute Prompt Guard + AI DLP 在模型调用前阻断或要求审批。
28. DeepFlow 发现异常外连时提供网络证据。
29. DeepBrain 判断是否存在 Prompt Injection / 越权路径。
30. DeepXDR 吊销 Agent Token、暂停资源会话并创建调查 Case。
31. DeepRoute、DeepGate、DeepVault 的状态回流形成闭环。

18. 部署、高可用与容灾

18.1 部署模式

模式	适用	架构
SaaS	中小企业、快速开通	多租户控制面 + 弹性数据面
私有化	大型企业/政企/金融	K8s 控制面 + 本地数据面/存储
一体化	<500 资产或 PoC	单节点/小集群
分布式	>5000 资产/高流量	采集、计算、存储独立扩展
混合云	多云/数据主权	本地数据面 + 云端控制/AI，可按数据级别分层

18.2 高可用

- 控制面无状态化；状态存储在 PostgreSQL/Redis/对象存储等持久化组件。
- Kafka 采用多副本；事件允许重放。
- ClickHouse 采用分片 + 副本；查询与写入解耦。
- Edge/Flow/Core 数据面支持多活和本地自治。
- Agent/Sensor 本地缓冲，断网可续传。
- 策略、规则、模型路由、WASM 和 Agent 均支持版本化与回滚。
- Action Executor 支持幂等、超时和重试。
- 跨地域部署采用异步复制和明确的数据主权边界。

18.3 故障模式

故障	默认策略
控制面不可用	数据面继续执行最近一次有效策略
CTI 不可用	使用本地缓存情报，不阻断核心业务
LLM 不可用	安全检测/规则继续运行，AI 分析降级
Kafka 不可用	边缘本地缓冲；恢复后重放
ClickHouse 不可用	实时检测继续，事件暂存
DeepRoute Provider 不可用	Failover 到允许模型

规则发布失败	保留上一版本并自动回滚
Agent 升级失败	保留旧版本并回滚

19. 性能与工程技术指标

以下指标均为 V3.5 研发设计目标或 Benchmark 验收指标，不等同于在所有硬件、协议和业务条件下的商业承诺。原 V3.1 已提出 DeepFlow 100Gbps+、DeepEdge 10 万 QPS、DeepCore CPU <3% 等设计目标；V3.5 将这些指标进一步转化为可测试的工程 Profile。

产品/组件	V3.5 设计目标	验收方法
DeepFlow	集群 100Gbps+；按 10/25/40/100Gbps Profile	固定包长、协议比例、规则量、CPU/NIC 利用率
DeepEdge	单节点 10 万 QPS 级起步；按业务模型扩展	TLS/HTTP/HTTP2/HTTP3、多规则、真实连接模型
DeepCore	正常 CPU <3%；内存 <200MB 目标	不同主机、容器密度和事件率
DeepGate	单节点 5000 TPS 级；集群横向扩展	认证/授权/MFA/JIT 混合场景
DeepRadar	10 万资产级扫描调度	并发 Worker、扫描类型和带宽控制
DeepRoute	低毫秒级网关额外开销目标；Guard 按策略启用	不同 Prompt 长度、DLP 规则量、Provider
DeepBrain	告警入库 <1s；常规 AI 分析 <10s 目标	固定模型、RAG、工具链路
DeepXDR	事件关联秒级至分钟级	多源事件注入与 Playbook
ClickHouse	亿级数据秒级分析目标	标准化查询集 + 并发测试

19.1 五级检测引擎

级别	引擎	用途	实时性
L1	规则	WAF/Sigma/YARA/Falco/策略	最高
L2	信誉/IOC	IP/Domain/Hash 等	最高
L3	行为	状态机、基线、序列	高
L4	风险	资产/身份/漏洞/情报融合	高/异步
L5	AI 推理	复杂语义、多跳攻击链	异步

实时数据面永远不依赖 L5 AI 才能完成基本安全控制；AI 是增强层。该原则延续 V3.1 的“规则与策略负责确定性安全控制，LLM 负责理解和推理”的设计。

20. 安全开发与供应链安全

20.1 SDL

- 设计阶段：Threat Modeling、Attack Surface Review、Security Architecture Review。
- 开发阶段：SAST、DAST、SCA、Secret Scan、Container Scan。
- 测试阶段：Fuzzing、协议解析测试、规则回归、性能 Benchmark、安全回归。
- 发布阶段：SBOM、制品签名、漏洞门禁、Release Attestation。
- 运行阶段：运行时完整性、版本漂移、Agent/插件版本核验。
- 响应阶段：CVE 快速定位、SBOM 反查、紧急升级与回滚。

20.2 制品可信链

Source
↓
Build
↓
SBOM
↓
Security Tests
↓
Sign / Attest
↓
Registry
↓
Deploy Verification
↓
Runtime Integrity

Sigstore 提供面向软件制品的签名、验证与透明日志能力，支持发布文件、容器镜像、二进制和 SBOM 等制品的供应链可信验证；V3.5 建议将其作为 Deep 系列制品签名和溯源的技术路线之一。

20.3 安全插件/WASM/规则

- WASM、规则、YARA/Falco/Sigma、自定义 DSL、Agent Tool Schema 都必须签名。
- 规则执行器只接受可信来源、合法版本和经过测试的规则。
- 插件具有 capability、CPU、memory、time、network 等限制。
- 生产规则发布前必须经过样本回归、误报测试和性能测试。

21. 合规与标准对齐

标准/框架	主要关联产品	V3.5 对齐方向
NIST CSF 2.0	全产品	Identify / Protect / Detect / Respond / Recover
MITRE ATT&CK	DeepCTI/Core/Flow/Brain/XDR	TTP 映射、检测覆盖度、攻击链

OWASP Top 10 / API Top 10	DeepEdge	WAF/API 安全
CNCF Cloud Native Security	DeepCore	容器/K8s/供应链/运行时
STIX/TAXII	DeepCTI	情报交换
ISO/IEC 27001/27002	Gate/Vault/Core/XDR	访问、数据、运营、事件
SOC 2	Gate/Vault/XDR	安全性、可用性、处理完整性、保密性
GDPR/PIPL	Vault/Gate/Edge	个人数据发现、访问、DLP、审计
PCI DSS	Edge/Core/Vault/Flow	支付数据、访问、日志与监控
等保 2.0	全体系	身份、边界、入侵检测、审计、数据保护
NIST AI RMF / GenAI Profile	Route/Brain/Vault/Gate	AI 风险、数据、治理、人机协同
MCP	DeepRoute/Brain	Tool 调用、认证、策略、DLP、审计

原白皮书已经将 NIST CSF 2.0、MITRE ATT&CK、OWASP API Security、CNCF Cloud Native Security、STIX/TAXII、ISO 27001/27002、等保 2.0 和 MCP 列为主要参考框架。V3.5 在此基础上增加 AI 风险管理、OpenTelemetry、Workload Identity 和软件供应链可信技术路线。

22. 产品演进路线与研发优先级

22.1 三阶段产品工程路线

阶段	目标	优先产品/组件	关键验收
P0 底座	统一身份、SOM、消息、规则、CTI、审计	DeepGate/DeepCTI/Unified Core	统一租户、AssetID、Event Schema、规则发布
P1 可销售产品	形成独立收入产品	DeepEdge/DeepCore/DeepRadar	应用、主机、ASM 三条产品线稳定
P2 高性能与协同	NDR/数据/AI 安全形成闭环	DeepFlow/DeepVault/DeepRoute	跨产品 Incident 与 Action
P3 AI 原生	Security Agent 与 AI 数据面	DeepBrain/DeepRoute	证据化推理、One Token、AI DLP
P4 平台化	统一控制、策略和自动响应	DeepXDR	MTTR、自动化率、验证闭环

22.2 建议研发顺序

32. 先建设统一租户/组织/身份、AssetID、SOM/Event Schema、消息总线、审计和规则中心。

33. DeepEdge 与 DeepCore 优先形成可销售的高性能数据面。

34. DeepRadar 作为资产与漏洞底座，与 DeepCTI 打通。

35. DeepFlow 采用独立高性能数据面路线，避免与通用控制面耦合。
36. DeepGate 建立统一身份与特权控制，并逐步增加 Workload/Agent Identity。
37. DeepVault 先做数据目录、分类分级和数据库审计，再扩展 DLP。
38. DeepRoute 先做 Token Gateway + Smart Routing + DLP，再增加 Guard/MCP。
39. DeepBrain 先做 Security RAG + 查询助手，再发展受控 Security Agent。
40. DeepXDR 最后把全产品 Action 串起来，形成自动化运营控制平面。

V3.1 的产品演进路线同样遵循“先底座、再防护、后智能、终平台”的节奏；V3.5 将该思路进一步转化为研发依赖关系。

23. 商业化与交付架构

23.1 独立销售 + 组合销售 + 平台化

模式	产品	价值
单产品	DeepEdge / Core / Radar / Gate / CTI / Route	快速形成明确采购理由
组合	Edge+Radar、Core+Radar、Gate+Vault、Route+Gate	形成场景闭环，提高客单价
平台	DeepXDR + 全产品	统一运营、数据和自动响应，面向中大型客户

23.2 SaaS 优先产品

- DeepCTI API：标准化威胁知识服务，适合 API/订阅模式。
- DeepRadar Cloud：互联网攻击面持续监测，天然适合 SaaS。
- DeepRoute：AI Token + 模型路由 + DLP，适合按 Token/调用量/Agent 数量计费。
- DeepEdge Cloud：WAF/API/Bot/边缘安全适合按流量/QPS/域名计费。
- DeepXDR SaaS：适合按资产/事件量/数据量/运营席位计费。

23.3 私有化交付

政企、金融、关键基础设施客户可采用本地控制面、数据面与本地模型；跨境/敏感数据场景支持数据不出域、离线规则更新和本地 AI。

24. 结语

Deep 系列 V3.5 的核心不是“增加更多产品”，而是把十个安全产品组织成一个技术体系：DeepRadar 发现，DeepFlow 看见，DeepEdge 保护应用，DeepCore 保护运行时，DeepGate 治理身份，DeepVault 治理数据，DeepRoute 治理 AI 数据流，DeepCTI 提供威胁知识，DeepBrain 提供 AI 分析与推理，DeepXDR 负责统一运营和响应。

在工程上，V3.5 强调高性能数据面、控制面与数据面分离、规则与行为优先、AI 异步增强、统一身份、统一事件、统一策略、可观测性、供应链可信和可验证的性能 Benchmark。

在 AI 安全方面，DeepRoute 与 DeepBrain 被严格区分：DeepRoute 是 AI Data Plane Security，负责 Route + Guard + DLP + Token；DeepBrain 是 Security Intelligence，负责跨域分析、调查、推理和决策建议。这一边界能够避免 AI 安全产品在功能上无限膨胀，同时形成清晰的产品价值。

最终目标是建立一个能够持续学习、持续验证、持续响应的企业安全系统：安全数据形成事件，事件形成知识，知识驱动检测，检测触发防护，防护结果反哺知识，AI 在证据约束下提升分析与决策效率，最终形成安全运营闭环。

附录 A：主要参考框架与标准

- NIST Cybersecurity Framework 2.0：企业网络安全风险治理与安全能力框架。
- MITRE ATT&CK Enterprise / Cloud：攻击者战术、技术与过程知识体系。
- OWASP Top 10 / API Security：Web 与 API 应用安全设计参考。
- CNCF Cloud Native Security：云原生供应链、构建、部署和运行时安全。
- STIX 2.1 / TAXII 2.1：威胁情报结构化表达与交换。
- ISO/IEC 27001:2022 / 27002:2022：信息安全管理体系与控制措施。
- OpenTelemetry：统一 Logs / Metrics / Traces / Events / Resource 语义。
- SPIFFE：工作负载身份、SVID 与 Workload API。
- Sigstore / Cosign：软件制品签名、验证与透明日志。
- NIST AI RMF / Generative AI Profile：生成式 AI 风险管理参考。
- Model Context Protocol（MCP）：AI 模型与工具/上下文连接的协议体系。
- WebAssembly Security Model：沙箱隔离与受控宿主能力。

附录 B：核心术语

缩写	英文	中文
ASM	Attack Surface Management	攻击面管理
NDR	Network Detection and Response	网络检测与响应
WAAP	Web Application and API Protection	Web 应用与 API 综合防护
CWPP	Cloud Workload Protection Platform	云工作负载防护平台
CSPM	Cloud Security Posture Management	云安全态势管理
IAM	Identity and Access Management	身份与访问管理
PAM	Privileged Access Management	特权访问管理
CTI	Cyber Threat Intelligence	网络威胁情报
XDR	Extended Detection and Response	扩展检测与响应
SOAR	Security Orchestration, Automation and Response	安全编排、自动化与响应
MCP	Model Context Protocol	模型与工具/上下文连接协议
RAG	Retrieval-Augmented Generation	检索增强生成
SOM	Security Object Model	统一安全对象模型
IOC	Indicator of Compromise	入侵指标
TTP	Tactics, Techniques and Procedures	攻击战术、技术与过程
EPSS	Exploit Prediction Scoring System	漏洞利用预测评分

SVID	SPIFFE Verifiable Identity Document	可验证工作负载身份文档
SBOM	Software Bill of Materials	软件物料清单
MTTD	Mean Time to Detect	平均检测时间
MTTR	Mean Time to Respond	平均响应时间

附录 C：典型安全运营场景

C.1 0day 紧急响应

41. DeepCTI 接收漏洞情报并进行可信度、EPSS/在野利用和影响版本评估。
42. DeepRadar 根据影响版本立即启动增量扫描。
43. DeepEdge 对互联网暴露应用下发虚拟补丁或临时策略。
44. DeepCore 检查受影响主机和容器的运行时迹象。
45. DeepFlow 检测相关 C2、扫描和利用后的外连行为。
46. DeepXDR 创建紧急 Incident 并跟踪修复。
47. DeepRadar 复测并关闭风险，结果回流 CTI。

C.2 月度威胁狩猎

48. 分析师选择 ATT&CK TTP 或威胁活动。
49. DeepBrain 检索 DeepCTI 和历史案例。
50. DeepBrain 生成 ClickHouse/Flow/Core 查询。
51. 分析师审查结果并形成 Case。
52. IOC/TTP 回流 DeepCTI，形成新规则。
53. DeepXDR 记录运营效果并更新检测覆盖度。

C.3 AI Agent Prompt Injection

54. Agent 获取外部内容，其中包含恶意 Prompt Injection。
55. DeepRoute Prompt Guard 标记潜在越权指令。
56. Agent 尝试访问高敏数据，DeepGate/DeepVault 判断权限和数据等级。
57. 数据进入模型前，DeepRoute AI DLP 识别敏感内容。
58. 根据策略执行 Block / Redact / Approval。
59. DeepBrain 根据 Agent 行为、来源、数据和 Tool 调用构建调查链。
60. DeepXDR 在确认高风险后吊销 Token、暂停会话并创建 Case。
61. 处置结果用于更新 Agent 风险基线和安全策略。