实时缓解数据中心网络安全风险，确保业务零中断

数据中心关键基础设施漏洞，代价不容小觑

数据中心为 AI 后端与推理系统提供支持，对现代企业至关重要。然而，正因这一举足轻重的地位，数据中心所承受的风险也随之加剧。如果未能及时修补 CVE 漏洞或遭遇零日攻击，企业便可能面临经济损失、声誉受损、服务中断。

在如今的威胁形势下，补丁部署空窗期已然成为严重安全隐患。攻击者只需数小时即可利用 CVE 漏洞发起攻击，而防御者往往需要数周甚至数月，才能在生产环境中完成补丁的测试与部署。

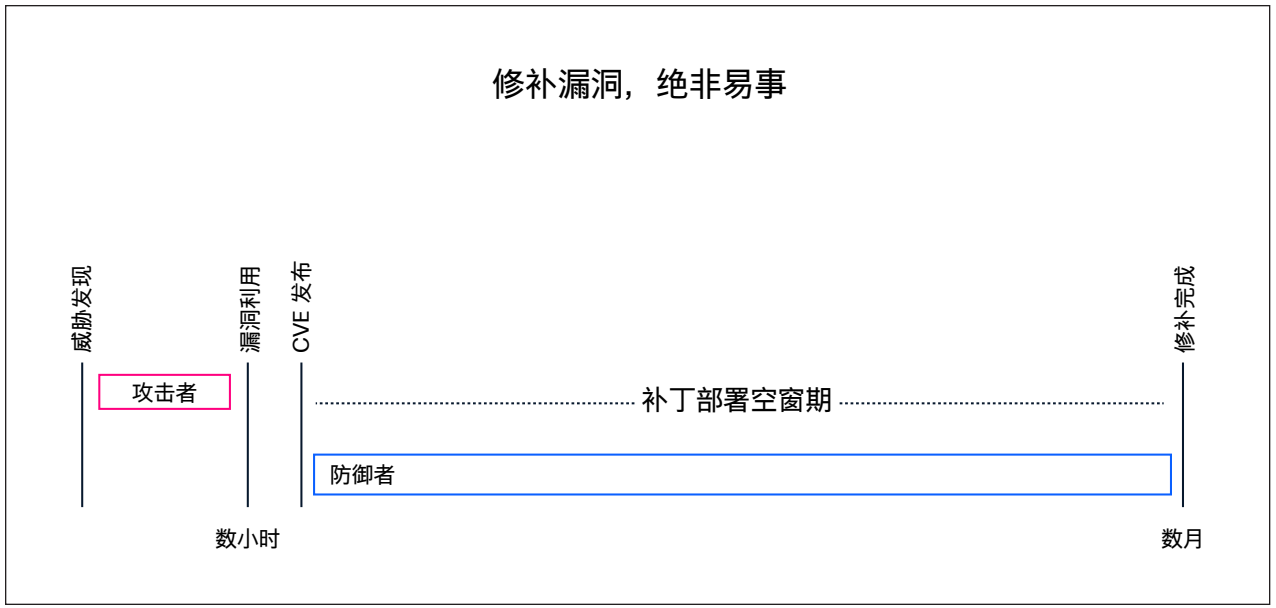

图 1. 漏洞修补面临重重挑战

Cisco® Live Protect 彻底改写了这一局面，它能为 Cisco Nexus® 交换机提供即时漏洞防护功能，在不中断网络运行的情况下阻止攻击。要想保障数据中心基础设施的平稳运行，持续的安全防护与高可用性保障缺一不可。传统的 CVE 漏洞修补方式往往伴随着业务中断与系统停机风险。面向 N9000 系列交换机的 Cisco Live Protect 可提供实时防护，快速缓解漏洞风险，在无需紧急维护或临时升级的情况下，持续保障系统安全稳定运行。

为什么选择 Cisco Live Protect？

传统修补方式往往需要预留维护窗口、重启设备，还可能面临停机风险。Cisco Live Protect 提供了一种颠覆性的安全防护方法：

- **零停机：**无需重启交换机，即可将安全策略直接应用于运行中的系统。
- **即时防护：**一旦发现威胁，即可迅速屏蔽相关漏洞，无需等待常规 PSIRT 升级计划。
- **持续验证：**借助 eBPF 驱动的安全可观测性，维护安全态势。
- **高效运维：**待完整 PSIRT 升级包部署完成后，安全 SMU（即“防护盾”）随之自动移除。

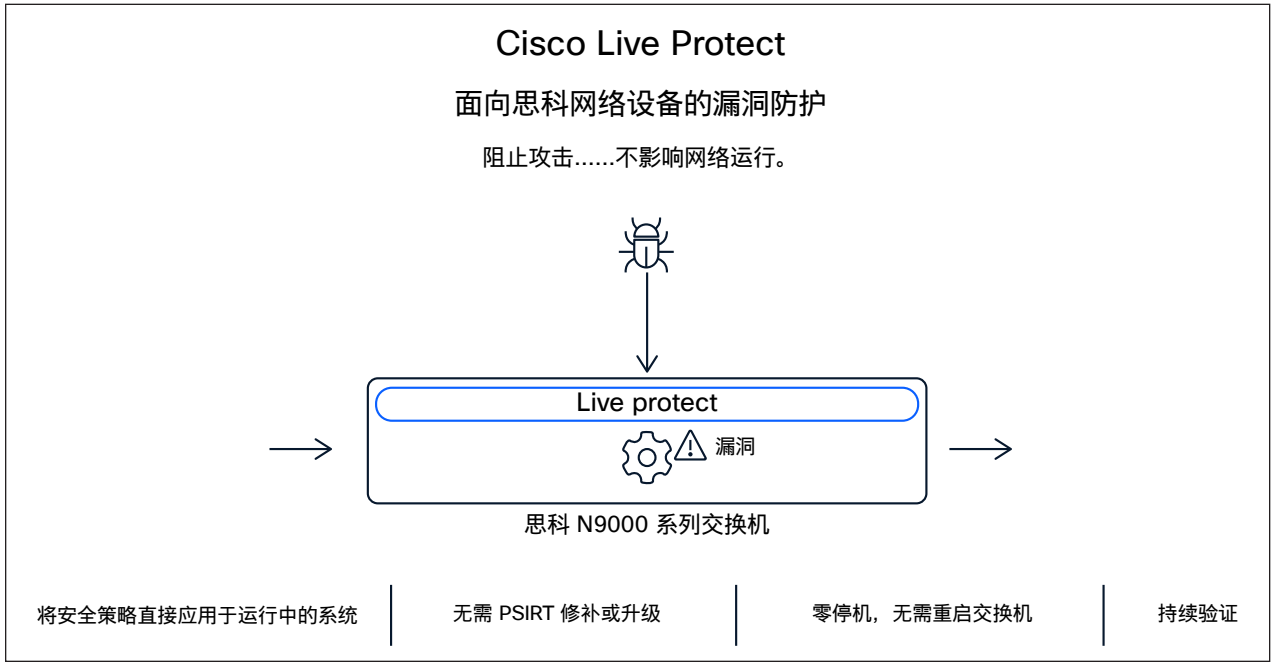

图 2. Live Protect

由 eBPF 驱动的创新

Cisco NX-OS 自 10.6(1)F 版本起直接内置企业级 Tetragon 代理，这一创新之举也让思科成为业界首家实现该功能的厂商。借助 eBPF 技术，Live Protect 可提供深入内核级的可视性和策略执行能力，覆盖以下场景：

- 防止权限提升
- 保护控制平面
- 加强 API 和 CLI 安全防护
- 监测文件 I/O 活动

支持的平台

Live Protect 面向持有 **Essential 或更高级别许可证**的 Nexus 客户提供。

Cisco NX-OS 10.6(2)F 版本支持的平台：

- 思科 N9300 和 N9200 固定式平台（内存 ≥ 24GB）
- 思科 N9300 智能交换机
- 思科 N9400 系列交换机

运作方式

Cisco Live Protect 利用先进的 eBPF 技术，为数据中心网络设备提供实时安全防护。其配置方式非常灵活，不仅支持通过 Cisco NX-OS CLI 或 API 对单台设备进行管理，也支持借助 CI/CD 流水线实现整个数据中心架构的全面自动化管理。Nexus Dashboard 提供集中式协调能力，能够即时显示受 CVE 漏洞影响的设备，自动部署安全防护措施，并持续监测其防护效果。

组件

- **Cisco Live Protect：** 运用 eBPF 技术，为网络设备提供内核级防护
- **Tetragon 代理：** 将针对 CVE 漏洞的补偿性控制措施编译为可部署的 eBPF 策略
- **Nexus Dashboard：** 作为集中式控制台，可用于统一协调、深入洞察并全面监测所有 Cisco Nexus 交换机
- **集成工具：** 支持通过 API、CLI 和 CI/CD 流水线与现有环境集成，实现无缝自动化部署与管理

Live Protect 可简化 Cisco NX-OS 和 Cisco ACI® 环境的升级流程并持续缓解漏洞风险，无论是基础设施核心，还是整套系统，都能确保安全防护不中断、性能表现不受影响。

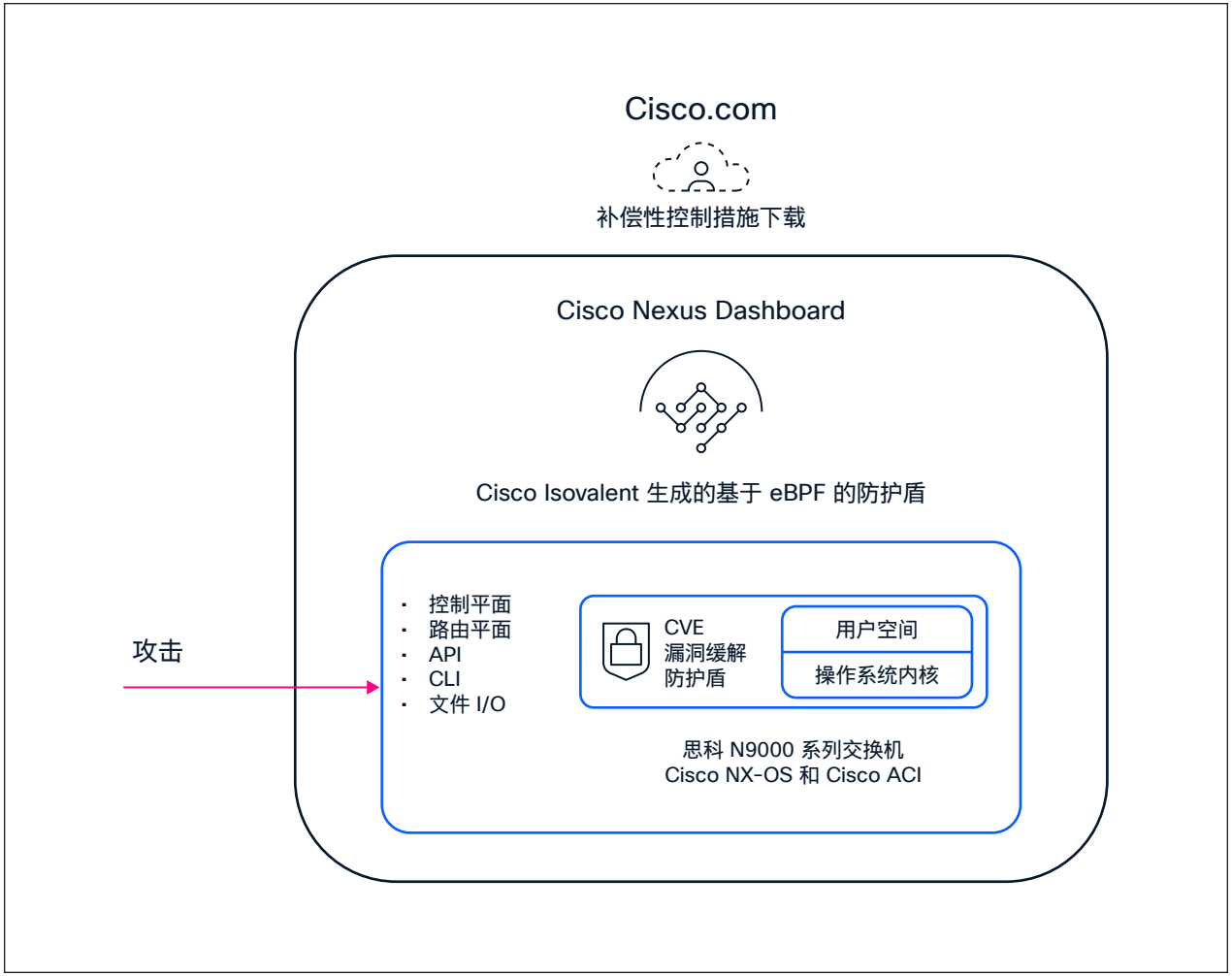

图 3.　面向思科 N9000 系列交换机的 Live Protection 和 CVE 漏洞缓解方案

了解详情

利用 Cisco Live Protect 保护数据中心，畅享实时自动化安全防护与零停机体验。

如需了解详情，请访问 Cisco Live Protect 博客或立即联系思科代表。

资源

Cisco Live Protect 网页

观看视频，了解 Cisco Live Protect 的实际应用

Cisco NX-OS 版本说明。

应用场景

行业	Cisco Nexus 与 Live Protect 关键应用场景
金融服务	• 实时缓解 CVE 漏洞风险 • 防范零日攻击 • 最大限度缩短关键应用停机时间 • 提升合规水平，随时应对审计需求
医疗健康	• 保护患者敏感数据 • 实时缓解 CVE 漏洞风险 • 保障医疗系统持续稳定运行 • 满足合规要求 (如 HIPAA)
零售和电子商务	• 保障支付与客户数据安全 • 最大限度缩短高峰期的停机时间 • 实时防范 CVE 漏洞与零日攻击 • 符合 PCI 数据安全标准
政府和公共部门	• 实现集中式安全协调 • 快速应对零日威胁 • 满足监管合规要求 • 保障敏感信息，确保公共服务持续正常运行
电信和服务提供商	• 抵御高级威胁 (如 DDoS) • 保持网络性能持续稳定 • 实现安全运维自动化 • 实现集中式策略管理
能源和公用事业	• 保障关键控制系统安全 • 实时缓解 CVE 漏洞和零日攻击风险 • 满足监管合规要求 • 保障系统韧性和正常运行时间
教育和科研	• 保护知识产权与敏感数据 • 保障数字资源持续可用 • 实时应对安全威胁 • 实现安全运维自动化
制造业	• 保障 OT 和 IT 环境安全 • 实时缓解漏洞风险 • 保护知识产权 • 确保运维连续性

C22-5771857-00 02/26