SOLUTION BRIEF

FortiDeceptor 带来一种新的威胁防御方法

管理层摘要

不管一次入侵事件的发生是源自组织内部还是外部，都需要数月的时间来发现并执行补救措施。在这个时间窗内，组织可能会产生巨大的财务和名誉损失。为了避免这种情况，网络安全架构师们应该进行前向思考，比如部署 Fortinet FortiDeceptor 在组织网络中，来欺骗和重定向攻击者，使攻击远离组织的高价值资产。这将显著降低安全风险带来的不利后果。

FortiDeceptor 是一款基于欺骗技术的创新安全产品，能够在内部或外部的网络威胁对组织产生损伤前对威胁进行欺骗、暴露和消除。在攻击发生前创建一个欺骗网络来迷惑攻击者，发生攻击时 FortiDeceptor 分析任何威胁活动并通过 Fortinet Security Fabric 共享信息给网络中的全部安全控制点来执行保护措施。不像其他的威胁欺骗解决方案，FortiDeceptor 易于部署，易于集成进企业现有安全架构，并且能够执行自动化威胁响应。

FortiDeceptor FortiDeceptor通过如下方式提升组织威胁防御水平：

- 补全组织的入侵防御能力版图
- 将攻击重定向到欺骗系统
- 作为威胁的早期预警系统
- 自动化响应内部和外部威胁
- 快速部署，第一天就获得欺骗能力

快速执行有效的威胁检测与响应是十分有挑战的工作

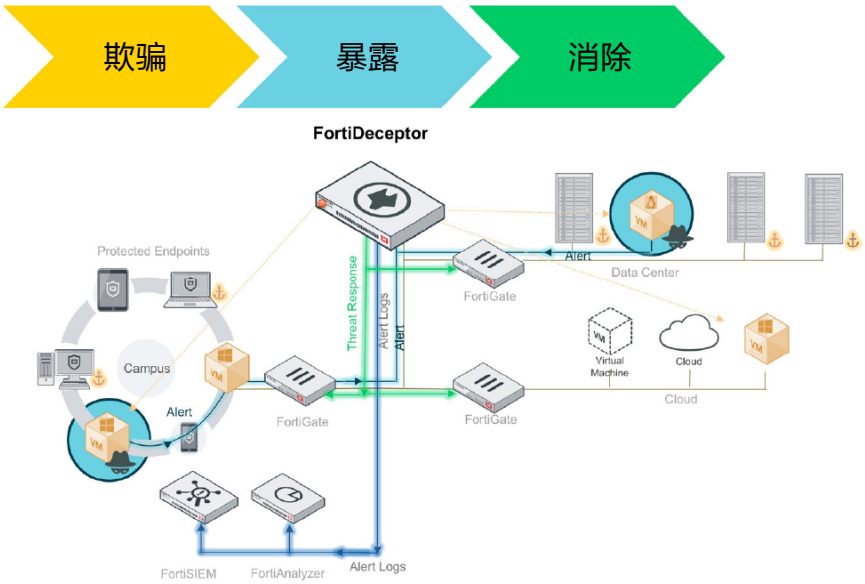
威胁不仅会从组织外部发起，也经常发起于组织内部。但是，大多数单点安全解决方案通常关注在某一方面，而不是两者兼顾。根据 Verizon 2018 数据失窃调查报告显示，三分之二的失窃事件是来自外部主体，三分之一来自内部主体。而且，68% 的入侵事件在其被发现前已经在组织内潜伏了数月，在这期间内，其给组织带来的风险和影响会以指数级增长。

当网络威胁防御建设与攻击者和恶意软件的水平迭代演进时，新的高级威胁防御技术通常需要更多的资源来交付、部署和维护。此外，这些新技术通常还只是单点安全方案，也难以与现有安全架构形成有机整体。

使用FortiDeceptor来欺骗、暴露和消除威胁

Fortinet FortiDeceptor 使用了先进的攻击欺骗技术来检测与响应来自组织内部和外部的威胁。它在组织网络中创建蜜罐、欺骗系统、诱饵等来迷惑攻击者，并与 Fortinet Security Fabric 无缝整合，拥有强大的威胁分析能力和实时防御能力。FortiDeceptor 的完整攻击欺骗周期请参考下方示意图。

在初始的攻击欺骗阶段，网络安全团队可以在企业网、数据中心或云中以 VM 形式部署欺骗系统和诱饵来模拟真实资产。欺骗系统可以仿真如用户终端和 IoT 设备以及数据中心服务器。诱饵可以安装在一个欺骗系统中或真实终端上。在这种情况下，数据、应用和服务会以逼真的方式来诱骗来自内部或外部的攻击者。



接下来，在暴露阶段，一个攻击者的行为和通过网络的横向移动踪迹会被记录下来并按时间线进行关联分析，来看本次攻击是否是一次更大的攻击活动的一部分。与此同时，安全管理员会被告警，并且威胁会被通过可视化界面管理的工作流来快速验证。产生的相关日志会发送给 SIEM（安全信息与事件管理）系统来让组织可以在一个安全管理平台统览所有安全事件。

最后，在消除阶段，获取的情报能够让安全团队进行进一步事件调查，并执行手动补救措施或让 FortiDeceptor 自动处理，以达到主动进行损伤控制的目的。

可执行的、自动化的，部署方便的攻击欺骗系统

FortiDeceptor 相比其他威胁欺骗方案有很多优势。通过与 Fortinet Security Fabric 集成，可以与其他安全控制点，如 FortiGate 下一代防火墙，进行协同联动，对威胁进行自动化防御，并在损伤发生前对攻击进行实施阻断。

FortiDeceptor 还提供了可执行的可视化展现，通过基于 GUI 的威胁地图来让网络安全架构师快速发现威胁活动的目标，监控攻击，并执行调查取证。整个分析流程会将时间线和攻击活动关联分析，并进行可视化形式展现。

FortiDeceptor 同时易于交付、部署和管理。用户可以根据实际情况选择部署 VM 或物理设备到云或数据中心环境中。管理员还可以集中管理并自动化部署欺骗系统 VM，诱饵和相关服务。对于管理员来说，这项优点可以让其降低很多工作量，因为欺骗系统和诱饵的部署、创建和运行是无需持续对其进行管理干预的，这对于本就工作量沉重的安全运营团队来说是十分重要的。

持续创新让用户更从容获得安全

通过使用这项对用户十分友好的攻击欺骗技术，Fortinet 证明了自己仍然是一个安全创新者。FortiDeceptor 是能够十分有效对抗内部或外部威胁的安全方案，并防患于未然。通过与 Fortinet Security Fabric 集成来共享可执行的威胁情报，对威胁进行自动化响应，FortiDeceptor 会是网络安全架构师的有力帮手。

[1] "2018 Data Breach Investigations Report," Verizon, March 2018.

FORTINET®

www.fortinet.com

March 21, 2019 10:52 AM

375208-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:sb-FortiDecptor:sb-fortideceptor-032119-1100am