保护您的零信任数据中心 - 您的数据堡垒

无论是在本地还是云端，数据中心都保存着最敏感的数据和应用，这些资产如同王冠上的宝石一样珍贵。无论这些数据和应用位于何处，企业都必须为其提供保护。了解零信任数据中心的组成并确保组织拥有适当的防护措施来保护自身及其数据安全，这一点非常关键。

缺乏可见性

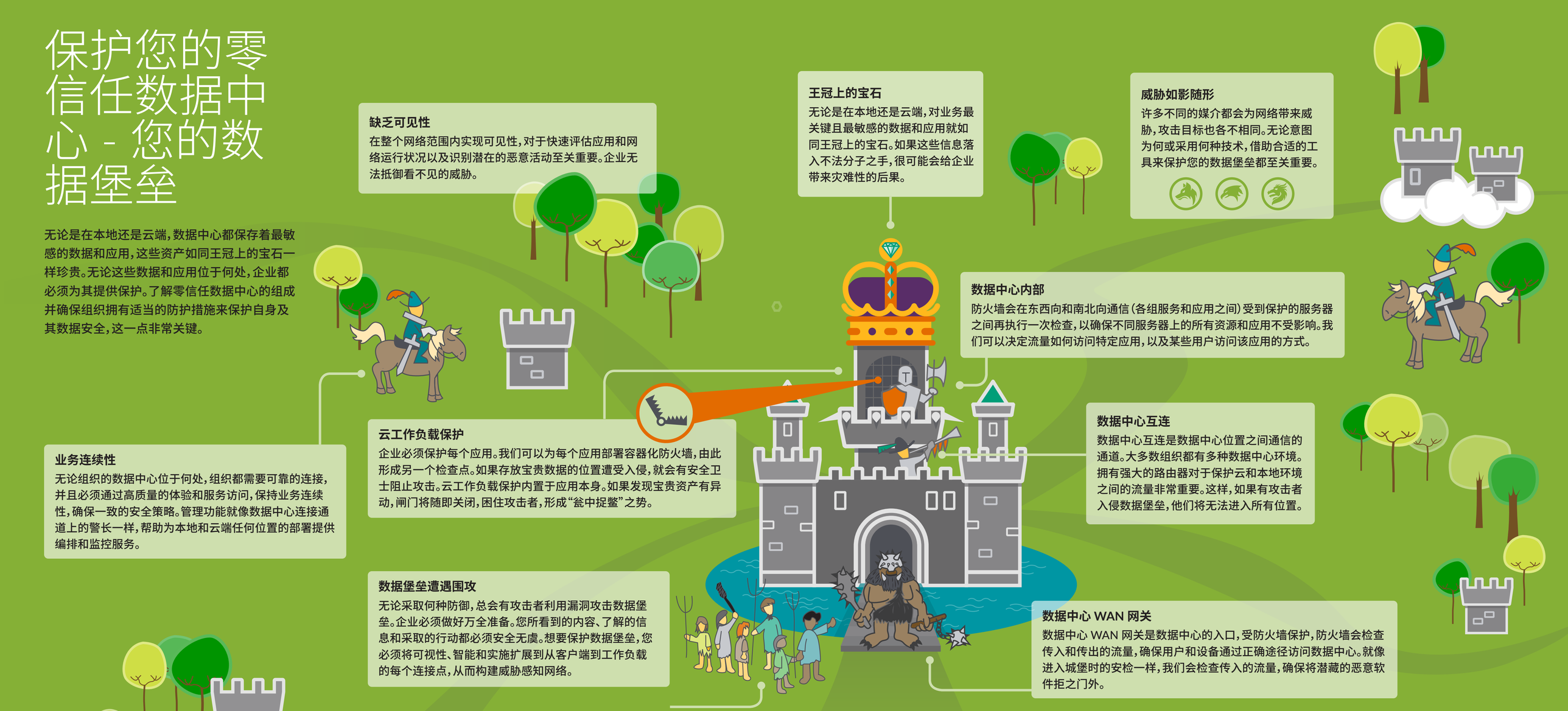
在整个网络范围内实现可见性，对于快速评估应用和网络运行状况以及识别潜在的恶意活动至关重要。企业无法抵御看不见的威胁。

王冠上的宝石

无论是在本地还是云端，对业务最关键且最敏感的数据和应用就如同王冠上的宝石。如果这些信息落入不法分子之手，很可能会给企业带来灾难性的后果。

威胁如影随形

许多不同的媒介都会为网络带来威胁，攻击目标也各不相同。无论意图为何或采用何种技术，借助合适的工具来保护您的数据堡垒都至关重要。



数据中心内部

防火墙会在东西向和南北向通信（各组服务和应用之间）受到保护的服务器之间再执行一次检查，以确保不同服务器上的所有资源和应用不受影响。我们可以决定流量如何访问特定应用，以及某些用户访问该应用的方式。

业务连续性

无论组织的数据中心位于何处，组织都需要可靠的连接，并且必须通过高质量的体验和服务访问，保持业务连续性，确保一致的安全策略。管理功能就像数据中心连接通道上的警长一样，帮助为本地和云端任何位置的部署提供编排和监控服务。

云工作负载保护

企业必须保护每个应用。我们可以为每个应用部署容器化防火墙，由此形成另一个检查点。如果存放宝贵数据的位置遭受入侵，就会有安全卫士阻止攻击。云工作负载保护内置于应用本身。如果发现宝贵资产有异动，闸门将随即关闭，困住攻击者，形成“瓮中捉鳖”之势。

数据中心互连

数据中心互连是数据中心位置之间通信的通道。大多数组织都有多种数据中心环境。拥有强大的路由器对于保护云和本地环境之间的流量非常重要。这样，如果有攻击者入侵数据堡垒，他们将无法进入所有位置。

数据堡垒遭遇围攻

无论采取何种防御，总会有攻击者利用漏洞攻击数据堡垒。企业必须做好万全准备。您所看到的内容、了解的信息和采取的行动都必须安全无虞。想要保护数据堡垒，您必须将可视性、智能和实施扩展到从客户端到工作负载的每个连接点，从而构建威胁感知网络。

数据中心 WAN 网关

数据中心 WAN 网关是数据中心的入口，受防火墙保护，防火墙会检查传入和传出的流量，确保用户和设备通过正确途径访问数据中心。就像进入城堡时的安检一样，我们会检查传入的流量，确保将潜藏的恶意软件拒之门外。

云时代的威胁感知网络

零信任数据中心提供威胁感知网络，最终可提高安全性，同时降低复杂性并简化管理。当组织赋予网络威胁感知能力时，网络便能更快检测到攻击，让攻击者不再有立足之地。用户、应用、基础架构，当然还有您的宝贵数据都将获得充分保护。

JUNIPER NETWORKS

PN:3050145