確保企業安全性並提升應用程式效能

IT 的複雜性使安全性和應用程式效能面臨挑戰

使用 Riverbed 解決方案提升您的應用程式安全性 - 專為安全而設計並基於行業公認的安全標準

混合型網路提升了企業用戶的產能，但也達到了傳統安全控制的極限，各種漏洞成為無數新型攻擊的目標，被不法分子、罪犯和政府利用。

用戶不再坐在辦公桌前，不再使用公司發行和修補的系統，而且通常不再存取公司控制的資料中心的資料。今天的用戶可能自備筆記型電腦，坐在咖啡店內，連接到開放的 Wi-Fi 熱點，存取雲端中的資料。

儘管發生了巨大的變化，用戶仍然期望所使用的系統和所存取的資料在任何時候都是安全的。

另一個日益嚴重的威脅是「影子 IT」，這是 IT 消費化的自然結果。用戶對企業 IT 部門提供的服務不滿意，就會按自己的偏好部署服務。員工會使用很多常用的免費服務，這些 IT 服務完全不受 IT 部門控制，例如 Dropbox（免費文件儲存庫和交換），Google（免費檔案儲存、電子郵件、聊天室）、Facebook 和 Evernote 等等。不難想像，公司機密和智慧財產權意外洩露的風險有多大。

多年來，企業增加了一層又一層的威脅檢測工具，但資料洩露的問題完全沒有緩解，而是日益嚴重。資料和用戶的蔓延雪上加霜。諸多因素很容易釀就 IT 災難。

可視性

如果看不見，就無法提供保護

雖然最終目標是防止入侵，但這只是挑戰的一部分。請考慮以下的事項：

- 我瞭解我應該保護的所有資料嗎？
- 我用同樣的控制措施在同一層保護所有資料，還是使用不同的信任層？
- 我的控制措施有多脆弱？ 單一的破解會導致所有資料遺失嗎？

回答這些問題需要詳細的可視性，包括：

- 網路上有哪些系統
- 誰和誰在對話
- 哪些應用程式在執行
- 透過什麼連接埠/通訊協定
- 流量集中之處在哪裡

網路可視性不僅有利於清晰瞭解我們要保護的目標，同時也是大多數資訊安全法規的常見要求。

收集此資料的傳統方法是將由弱點和修補程式管理系統生

成的報告與透過應用程式團隊收集的資料相結合。為了測試這種控制措施，稽核員通常對資產清單的選定樣本進行手動審查，查看這些系統是否存在以及記錄的資料集是否完整。這種方法並不理想，因為資產清單幾乎從未完整，最多只能看到截至最後一次掃描的資料。

使用 Riverbed，您可以開發和維護持續、即時而準確的網路檢視，包括：

- ✓ 完善網路資產清單 - Riverbed 向您顯示網路上的所有用戶、應用程式、主機和裝置，以及目前和歷史設定檔案使用的所有連接埠/通訊協定。此清單反映了網路的即時檢視，甚至可以識別 IT 部門未意識到的未經授權的部署。
- ✓ 網路相依圖- Riverbed 顯示實際的依賴關係，這可能與網路上的預期依賴關係不同。這非常重要 - 但有時被忽略 – 以確保顯示最新網路檢視的關鍵。Riverbed 還顯示隨著依賴關係發生變更，例如新增或刪除相關主機、應用程式或服務，流量和行為會發生什麼變化。
- ✓ 實際使用 - Riverbed 記錄網路上的所有活動，為您提供有關誰在網路上、存取了哪些系統、使用哪些連接埠和通訊協定以及消耗了多少頻寬等詳細資訊。

背景

可視性工具是開發基線所必需的 - 瞭解正常情況。沒有這些基本知識，就不可能瞭解風險，無法確定攻擊者可能嘗試入侵的領域，而且不可能瞭解被入侵後如何恢復。Riverbed 觀察流量和報告詳細資訊，例如：

- 現在系統正在做什麼
- 誰是系統的管理員和普通用戶
- 如果系統當機，會影響哪些業務部門或流程
- 在入侵前後的數分鐘內發生什麼情況

攻擊通常會導致功能降低或完全中斷。對中斷的財務和生產成本建模可幫助您制定適當的資訊保護工具和程式預算。它還可以幫助您確定最好在何處部署冗餘系統和生產資料副本。

瞭解攻擊之前和之後的行為對於補救至關重要。瞭解這些情況將幫助您確定攻擊是否只是一個騷擾，如指令碼 kiddy 的探測，還是專門盜取智慧財產權的針對性入侵。

Riverbed 的應用感知網路效能監控 (aaNPM) 工具套件可提供這一精確背景資訊，還可以輕鬆地將此資料整合到安全資訊和事件管理 (SIEM) 以及資產管理資料庫中。

信任但要驗證

我們當然想信任我們的員工，他們實際上也值得信賴，但現實是，最容易的網路防禦入侵方式就是冒充員工。許多方式可以造成員工憑據的洩露，一些比較常見和流行的手段是：

- 魚叉式網路釣魚
- 網站和社交網路惡意外掛程式
- Pineapple 攻擊
- 利用社交工程方式進入實體辦公樓
- 在公司停車場留下一堆感染了惡意軟體的 USB

這些攻擊之所以危險的原因是，攻擊者一旦獲得了對網路的任何類型的存取權限，就幾乎無法偵測或監視攻擊者的行為，因為攻擊者的身份被誤認為是員工。

觀察和稽核網路周界內的連接通常被稱為跟蹤橫向移動。從以往的經驗來看，這是一個成本高昂的方法，因為網路擁有大量的足跡。但是，Riverbed 能夠利用網路本身作為偵測的方法，在控制成本的同時，為整個區域網路和廣域網路提供卓越的可視性。

Riverbed 不僅能夠維護所有橫向移動的詳細歷史，而且可以針對此稽核跟蹤應用控制措施，對違反可接受用途和監管要求的情況或潛在的惡意活動提出預警。

標準和一致性

隨著網路的增長，路由器、防火牆、代理和其他裝置的數量都在以驚人的速度增長。不幸的是，我們很快會發現，要控制所有裝置都如預期運行，非常困難。

- 冗餘網路路徑是否與主網路路徑一樣安全？
- 是否建立了任何意外的路徑？
- 是否存在任何臨時/應急/測試弱點？
- 每個路由器、防火牆和代理是否具有相同的最新設定？
- 所有這些裝置是否按照最佳作法進行設定？

應用 Riverbed 的設定管理和建模技術，組織可以在受控制的情況下解決問題。您可以：

- 管理設定變更
- 確保設定遵循 PCI 安全委員會、NIST、DoD 或其他

組織建議的最佳實踐
- 計劃基礎設施生命週期，包括終止支援
- 進行強大的生存性分析
- 模擬常見攻擊的影響，例如 DDoS、DNS 放大、HTTP 放大等
- 根據稽核框架快速記錄
- 在全球範圍內自動套用超過 1,500 個基於行業最佳實踐的即開即用規則、安全標準以及符合組織標準和需求的自訂規則和範本

Riverbed 的網路規劃和設定管理工具套件將這種風格的工作流程套用到日常操作中。

補救

安全行業中強調預防。但是，不可避免，仍然可能遭受入侵。這使得補救的準備同樣重要。儘管有多層預防性安全保護，例如防火牆、防病毒和惡意軟體偵測，仍然可能遭受入侵。這時應該怎麼做？

修復過程中最重要的步驟是控制入侵，縮小攻擊範圍，並儘快恢復執行。要控制住找人問責的衝動，因為這些資訊往往是錯誤的，而且無助於災難恢復。

Riverbed 的網路可視性工具可以幫助您回答一些重要問題：

- 攻擊者如何獲取存取權限？
- 攻擊者檢查和/或竊取了什麼？
- 攻擊者如何隱藏證據並離開？

現在的攻擊者很少研究密碼提示或嘗試其他形式的暴力攻擊方法。相反，常用的技術是對有一定存取權限的人員應用社交工程方法。工作量少，回報大。用這種方法，攻擊更容易擴散到整個網路。也許是一個特權用戶登入到普通工作站時，沒有清除快取記憶體的憑據。攻擊者發現後，可以用來模擬特權用戶，從而獲得對網路上更多資源的存取權限。

Riverbed 可以幫助您瞭解攻擊者的興趣目標。透過跟蹤入侵者在網路上的路徑，可以瞭解加強哪些區域的存取控制或額外隔離能夠強化未來的防禦。攻擊者會定期修改或刪除日誌，以刪除其留下的任何痕跡。Riverbed 可以透過擷取所有資料封包來阻止這種行為 - 當日誌看起來可疑時，資料封包會呈現真實情況。

Riverbed 的應用感知網路效能監控 (aaNPM) 工具套件可提供此項功能，還可以輕鬆地將此資料整合到安全資訊管理 (SIM) 工具中。

> 使用 Riverbed 產品，「您可以快速識別未授權的網路流量模式」，這是「任何關注安全的企業必須具備的」。
>
> Doug Tamasanis，
> Kronos 首席 IT 架構師/網路和安全總監

分支機構

如果我們相信「一條鏈的強度取決於最薄弱的一環」，那麼我們最好注意分支機構，因為它可能是一個薄弱環節。

與資料中心不同，分支機構是員工所在的地方。但是，分支機構通常幾乎沒有 IT 人員，與資料中心相比，物理安全性不夠強，安全預算有限。

SaaS 交付的應用程式（如 Microsoft 的 Office 365、Google Docs、Salesforce 等）快速增長，使本來傳輸到資料中心的分支機構流量大量轉移到網際網路上。這一點以及網際網路頻寬與 MPLS 頻寬之間的價格差異共同導致了分支機構網際網路突破現象的上升。

現在，和資料中心一樣，分支機構也必須具備可視性、背景、標準、一致性和補救措施。

這是 SteelHead 裝置發揮第二種作用的地方。 在傳統應用中，SteelHead 部署用於廣域網路加速，提供許多其他功能，無需額外的成本，方便安全團隊使用。

具體來說，每個 SteelHead 都可以同時作為：

- 分散式資料封包擷取裝置，可存取分支機構中或傳輸到網際網路的流量
- NetFlow 產生裝置，產生分支機構中每個對話的記錄，並集中饋送用於橫向移動跟蹤和報警
- 主機平台，您可以在其中執行一般安全控制程式，例如防火牆或內容過濾器
- 將分支機構連接到雲端安全服務（如 Zscaler）的分

流點

此外，由於分支機構缺乏資料中心的安全性，您必須維護本機伺服器、儲存和備份，以保障用戶的產能。採用 Riverbed SteelFusion，您可以在資料中心集中管理分支機構的儲存。然後隨時將工作資料集傳輸到您的分支機構。SteelFusion 使用 SSL 從資料中心安全地提供資料，並透過進階 AES 256 位加密對分支機構使用的資料進行加密。讓未經管理員驗證的人員無法存取被盜裝置或磁碟機中的資料。透過 SteelFusion 集中控制和保護資料，可以降低業務營運風險，削減分支機構 IT 成本，還能更有效地利用資料中心的投資。

減少攻擊面積

透過資料集中和恢復效率消除風險和加強安全性。

據說銀行劫匪威利·薩頓說過：「我搶劫銀行，是因為錢在那裡」。今天的駭客可能會說，「我攻擊分支機構，是因為……」

無論用戶或資料位於何處，人們都需要存取資料。許多工作都需要人們在不適合儲存本機資料副本的地方花時間。用於支援這種受限環境的傳統方法經常導致應用程式效能差、可用性不穩定。 當員工無法安全地存取他們需要的內容時，可交付成果可能會延遲或錯失。

資料中心專用於保護系統和資料，幫助確保智慧財產權的完整性，確保業務連續性，並在中斷和災難後進行恢復。即使在可以安全地維護本機資料副本的地方，分支機構和遠端辦公室通常也缺乏資料中心用於保護資料和應對風險的持續保護機制。

Riverbed 解決方案在資料中心應用資料整合和集中，消除了遠端位置儲存資料的相關操作風險和低效率。虛擬伺服器和資料可以透過加密工作階段傳輸到遠端辦公室，保持所有資料處於靜止加密狀態，同時持續備份，建立幾乎即時的還原點目標。用戶能夠體驗到高效能和高可用性，因為存取位置在本地，而完整資料保留在資料中心內。如果發生災難，可以在幾分鐘內將資料恢復到全球的任何地方。

企業可以在任何地點開展全球範圍的業務，而不會使資料面臨風險。Riverbed 透過行業標準 TLS 1.2 或 IPSEC 加密保護傳輸中的資料，並使用符合 FIPS 140-2 標準的 AES 256 位加密來保護快取記憶體的使用中資料。

降低風險最重要。我們是一家律師事務所，必須保護資料，因為我們必須保護客戶的利益。」

Searl Tate，

工程部總監

Paul Hastings

Riverbed 解決方案為客戶提供了從分支機構存取資料的可行方法。將所有資料集中回資料中心可立即提升安全狀態，並將有限的安全資源集中到較少的位置。

控制

安全和效能問題

將系統從所有網路中斷連接並鎖在庫中可能是最安全的做法，但這樣的用戶體驗是不可接受的，會導致用戶無法進行業務交易，或以影子 IT 方式部署替代系統。

Riverbed 還利用安全可視性和分類所使用的相同工具和資料收集方法，提供行業領先的效能管理。

Riverbed SteelCentral Performance Management 是唯一一款將企業級最終用戶、應用程式和網路效能管理集成到一個解決方案中的效能管理套件。Riverbed 提供可視性、分析和洞察力，使公司能夠在最終用戶注意到問題、致電客服中心投訴或轉投其他服務之前檢測和修復應用程式效能問題。

透過結合業界領先的效能管理[1]和安全可視性，最終用戶可以進一步降低複雜性和成本。

總結

當今的 IT 環境非常複雜。網路連接、存取裝置和資料儲存庫的多樣性使得確保所有這一切，同時保持可接受的效能的工作比僅僅幾年前更具挑戰性。

[1] Riverbed 效能管理部是 2015 年 Gartner 網路效能管理和診斷魔力象限的領導者。

鑒於體系結構的這些變化，我們必須改變有關安全威脅的觀念和解決方案。我們不再使用單一的資料中心來集中管理公司的所有寶貴資源。因此，我們必須擴大防範安全威脅的範圍，並提升應對這些威脅的準備措施。

Riverbed 提供獨特的解決方案組合，可以：

- 幫助將分散式資料合併到少數高度安全的資料中心
- 自動記錄環境中的所有內容以及各個系統如何相互依賴，以確保安全性和資料可用性
- 促進應急規劃的假設分析
- 維護分支機構和資料中心內所有橫向網路活動的稽核追蹤
- 將安全智慧與效能管理相結合，提供最具成本效益的解決方案

「我們的設計工程師保持了一直以來的高水平表現，而且現在的工作環境更靈活，也更安全。」

Marco Malavolta
IT 基礎設施主管，
WAMGROUP

Riverbed®公司簡介

Riverbed 是应用性能基础设施的领导者，年收入超过 10 亿美元，为混合型企业提供最全面的平台，确保理想的应用性能，持续的数据可用性，并主动监测和解决性能问题，不会影响业务性能。Riverbed 助力混合型企业将应用性能转化为竞争优势，最大化员工生产率，借助 IT 创造新型运维灵活性。Riverbed 目前拥有 28000 余家客户，其中包括 97%的财富百强企业和 98%的福布斯全球百强企业。更多内容敬请浏览 www.riverbed.com。