riverbed

SOLUTION BRIEF

Identify, Remediate and Protect against Security and Compliance Risks

Gartner finds that 88% of respondents view cybersecurity-related risk as a business risk, not just a technology risk. The rise of remote work and increased use of mobile devices and distributed cloud services have expanded the threat landscape for organizations. Costly ransomware attacks, data breaches, and deeply embedded supply chain vulnerabilities have become common occurrences in the corporate sphere. Unpatched network vulnerabilities remain a prominent attack vector exploited by ransomware groups. Shadow IT regularly introduces applications and software that IT is often unaware of and can create unknown security vulnerabilities.

Security Not Just for SecOps

IT managers simply can't afford to ignore security as security and compliance incidents can cause performance problems (Enterprise Management Associates). A lack of security awareness among network teams can lead to blind spots when investigating the root cause of service issues. Providing network teams with security visibility is essential as the network is often viewed as the culprit for any service problem.

IT needs solutions that provide broad threat detection, investigation, and mitigation of incidents that bypass perimeter security. Security problems like data exfiltration, brute forcing, scanning and more can be detected using enterprise-wide visibility with network performance management (NPM) or digital experience management (DEM) solutions.

Alluvio by Riverbed Reduces Security and Compliance Risks

The Alluvio™ Unified Observability portfolio of NPM and DEM solutions functions as a supplement to IT teams' cyber-security tools. It offers security analytics and forensics that enable robust incident detection and threat hunting, plus preventative compliance capabilities. The list below provides more details:

- **Broad network security**: Alluvio™ NetProfiler Advanced Security Module transforms network data into security intelligence, providing essential visibility and forensics for broad threat detection, investigation, and mitigation. By capturing and storing all network flow across the enterprise, the Advanced Security Module detects and investigates unusual traffic patterns, such as zero-day events, data exfiltration, suspicious connections, DDoS attacks, and other advanced persistent threats that bypass typical preventative measures or originate inside the network. As a result of the NetProfiler Advanced Security Module enterprise-wide incident forensics, IT can visualize the complete scope of an attack and hunt for entrenched threats.

- **Incident forensics:** Alluvio™ AppResponse captures and stores all packets at up to microsecond granularity. This ensures that details about performance and security incidents are readily available for incident response and forensic analysis. For example, AppResponse users can search for signs of threats, like Log4J, within the body, URL, and header of application traffic. Additionally, users can leverage AppResponse's rich DNS analysis, to identify common attacks like command-and-control (C2), data theft, phishing, and ransomware.
- **Remediation of device vulnerabilities:** Alluvio™ Aternity prevents vulnerabilities in device operating systems and applications by identifying non-compliant or unpatched software. It automatically discovers user devices and operating systems, so IT can quickly determine whether these items need replacement, upgrading/patching, or no action at all.
- **Insight into Shadow IT Usage:** Alluvio Aternity also helps organizations monitor and manage Shadow IT, or unauthorized cloud/SaaS applications, which are often unsecure. By monitoring the usage and performance of cloud-delivered applications from the perspective of the end user's device, Aternity can help enterprises tackle the financial, management, and security challenges of Shadow IT.

Additionally, the Alluvio platform-wide initiative of automated orchestration supports Alluvio AppResponse, NetProfiler, NetIM, and Portal to prevent business-impacting security issues. It enables users to automatically update, backup, and restore IT infrastructure to a known good state. Automated orchestration allows monitoring devices to quickly revert to a stable state after a security incident; provides a preventative security measure to avoid stale, possibly insecure machines; and helps meet internal compliance policies.

Benefits of Alluvio by Riverbed

With the strong security and compliance capabilities provided by Alluvio, IT can avoid potentially disruptive security attacks and breaches. Better visibility into security and compliance results in:

- Decreased security and compliance risk
- Better network performance
- Reduced device vulnerabilities
- Faster security incident detection and response
- Operational cost efficiency

For more information about Riverbed security and compliance capabilities, go to riverbed.com/solutions/security-compliance.

riverbed®

Riverbed — Empower the Experience

Riverbed is the only company with the collective richness of telemetry from network to app to end user that illuminates and then accelerates every interaction so that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com/unified-observability.