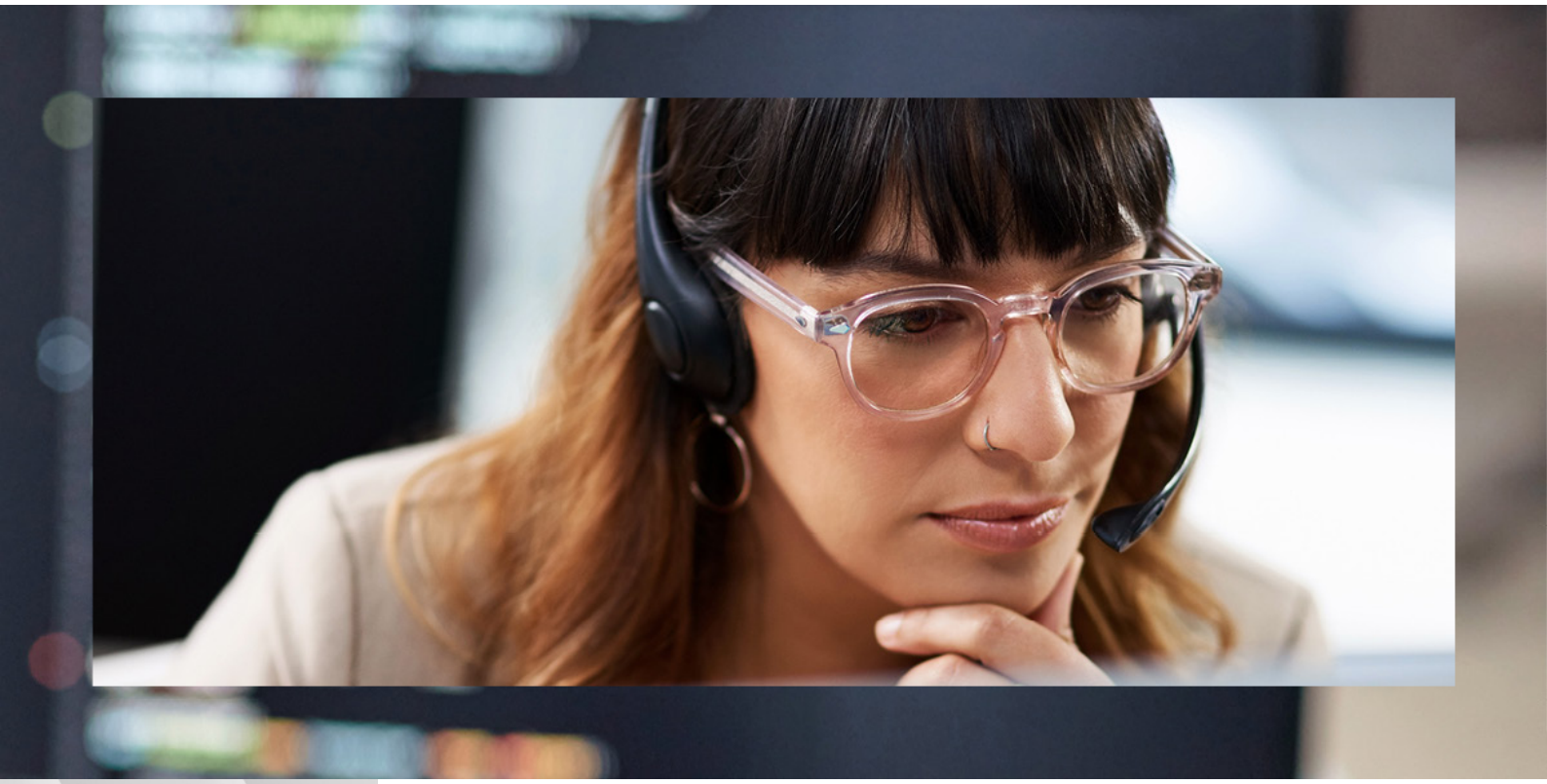

Advance your cyber resilience against ransomware with HPE Alletra Storage MP B10000

Introduction

In the modern digital landscape, ransomware has become a significant threat to organizations. Ransomware attacks are predicted to occur every two seconds, with global damage costs reaching $265 billion annually by 2031.[1] This malicious software encrypts valuable data, making it inaccessible, and demands a ransom for its release. The impact of a ransomware attack includes financial loss, reputational damage, and operational disruptions. As a result, organizations are seeking comprehensive ransomware detection and protection strategies to safeguard their digital assets.

Hewlett Packard Enterprise provides advanced solutions to fortify your data against sophisticated ransomware attacks. Implementing robust defense strategies at the storage level is essential, as it serves as the last line of defense for your data. To prevent catastrophic outages resulting from ransomware attacks, we utilize both traditional and emerging security technologies to identify threats before IT disruptions occur. HPE Alletra Storage MP B10000 incorporates cutting-edge ransomware detection and protection technologies to keep your data secure.

[1] "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," Cybercrime Magazine, July 7, 2023.

TD SYNNEX Public Sector

DLT

HPE GreenLake

Ransomware detection and protection with HPE Alletra Storage MP B10000

The B10000 provides on-array intelligent ransomware detection and recovery technologies to help ensure your data remains resilient against ransomware attacks.[2] It also simplifies your workflow for detection, protection, and recovery with seamless orchestration, thanks to the streamlined data management experience offered by the Data Services Cloud Console.

Built-in ransomware detection

The B10000 offers built-in ransomware detection integrated into the storage operating system software. Using anomaly detection methods, the B10000 can identify encrypted incoming I/Os in real time, generating quick alerts for potential ransomware threats. This advanced detection technology is dynamic and adaptive, capable of detecting both traditional ransomware and newer, more sophisticated variants that traditional techniques might miss. When ransomware detection is activated on a virtual storage volume in the source system, it can also be enabled on the corresponding volume in the target replication system. This capability provides customers with crucial visibility and awareness to prevent catastrophic consequences from ransomware attacks.

Furthermore, the ransomware detection capability in the B10000 supports integration with third-party security solutions, including security information and event management (SIEM) and extended detection and response (XDR). This allows customers to employ multiple methods to enhance their security posture. It is also available for HPE Alletra Storage MP Disconnected, a block storage solution for isolated environments without an internet connection.

Comprehensive cyber resiliency workflow

In addition to providing storage-level ransomware detection capability, HPE also enables customers to comply with the NIST Cybersecurity Framework (CSF). This is achieved through a comprehensive cyber resilience workflow that aligns with the six essential NIST functions that provide a holistic approach to managing and mitigating cybersecurity risks.

- **Govern:** Advisory and Professional Services from HPE enable customers to implement ransomware protection policies and monitor results with security infrastructure, policies, and controls, helping ensure continuous governance over ransomware risks.
- **Identify:** HPE provides security hardening guides and data protection insights from Data Services Cloud Console (see Figure 1) to help storage administrators identify risks to their data and workloads. It recommends best practices for enhancing storage security to help ensure compliance with NIST security standards. Additionally, HPE assists customers to further identify risks in their environment that can be mitigated throughout development, manufacturing, and delivery processes through HPE's secure supply chain.[3]

[2] Available in HPE Alletra Storage MP B10000 software release 10.5.0 in Q3 of 2025.

[3] HPE Secure Supply Chain white paper.

- **Protect:** The B10000 utilizes Virtual Lock immutable snapshots, dual authorization, role-based access control (RBAC), and so on to secure data, platforms, and infrastructure and help minimize the impact of cybersecurity incidents. The immutable snapshots serve as unalterable recovery points, helping ensure data can be restored following an attack. In addition, the Data Services Cloud Console provides management recommendations for snapshots protection.[4]
- **Detect:** The B10000 actively detects anomalies indicative of malicious encryption. It continuously monitors storage environments for ransomware-like patterns, such as rapid file modifications or encryption attempts. Over time, these models become more refined, leading to quicker and more precise threat detection.
- **Respond:** When a ransomware threat is detected, the system automatically initiates responses such as notifying administrators with alerts that detail the time the suspicious encryption event was detected and highlights the involved volume. It also generates a short-lived, immutable snapshot at the point the threat is detected to help facilitate rapid recovery with minimal data loss.
- **Recover:** In the event of a breach, the solution facilitates the restoration of uncorrupted data from the tamper-proof immutable snapshots, significantly reducing recovery time and costs. Additionally, it helps identify the last good snapshots taken before the onset of an anomaly as the potential recovery point.[5] This capability is crucial for helping minimize data loss and ensure a swift recovery from ransomware attacks or other data-compromising incidents.

  Furthermore, ransomware detection and protection can be integrated with any B10000 disaster recovery topologies, such as the HPE Active Peer Persistence business continuity solution, for rapid recovery. In the event of a ransomware attack, you can quickly fail over to a second site and recover from immutable snapshots once a noninfected recovery point is identified while your IT team addresses issues at the primary site or if recovery from the primary site is not possible. Furthermore, an air-gapped solution such as the HPE Cyber Resilience Vault can be utilized at a third site with three data center Active Peer Persistence (3DC APP), offering an additional recovery option. These comprehensive solutions offer multiple and faster recovery methods during a ransomware attack, significantly reducing business downtime costs and increasing the likelihood of a full recovery.

[4,5] Available in Data Services Cloud Console software release in Q3 of 2025.

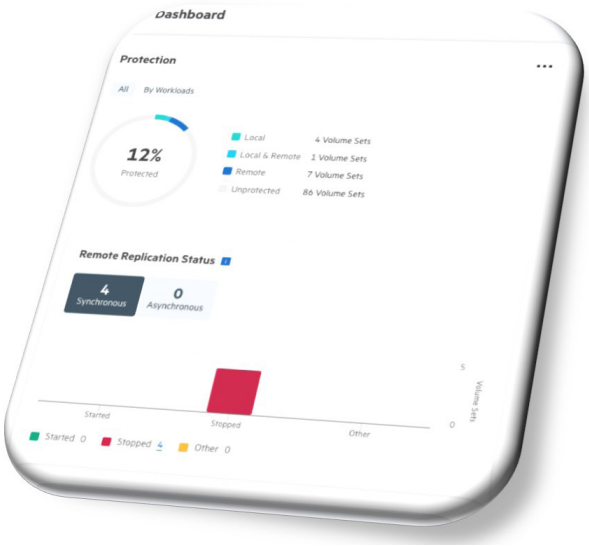

Figure 1. Data protection insights from DSCC

Overall, this workflow—combining anomalous encryption detection, automated response, and tamper-proof immutable snapshots capabilities—creates a comprehensive ransomware defense system. It is designed to be integrated organization-wide, orchestrating proactive ransomware responses and guiding recovery through an automated and streamlined approach.

Achieve ransomware peace of mind with cyber resilient storage. Guaranteed

We're so confident in the built-in ransomware defense capabilities of B10000 and our professional services expertise that we're now offering a new cyber resiliency guarantee. This guarantees you access to an HPE Services expert within 30 minutes of reporting an outage resulting from a ransomware incident, enabling you to rapidly address and mitigate the impact of a cyberattack. And it assures you that all immutable snapshots created on the B10000 remain accessible for the specified retention period.

Dual-layer protection from applications to storage

HPE offers a comprehensive stack of solutions that help fortify each layer of your data center against the most sophisticated ransomware attacks. In addition to the storage layer protection delivered by the B10000, you can also leverage rapid recovery from HPE Zerto Software, to help ensure robust data protection and swift restoration of applications.

HPE Zerto provides continuous data protection with near-synchronous replication at the hypervisor layer. It employs an encryption analyzer that uses a signatureless approach, assessing data patterns and analyzing entropy to detect unusual encryption which indicates potential ransomware activity. HPE Zerto's journal continuously captures and logs changes made to virtual machines (VMs), allowing for near-instantaneous recovery points. This means you can roll back to a moment before an attack, helping minimize data loss and downtime.

Detecting anomalous block-level encryption through both the B10000 and HPE Zerto provides additional layers of redundancy, helping ensure data protection and maintaining VM uptime, as shown in Figure 2. Alerts from the B10000 can be pushed to HPE Zerto through myriad methods. The synergy between B10000 and HPE Zerto helps ensure your data stays secure, and recovery processes remain robust and efficient.

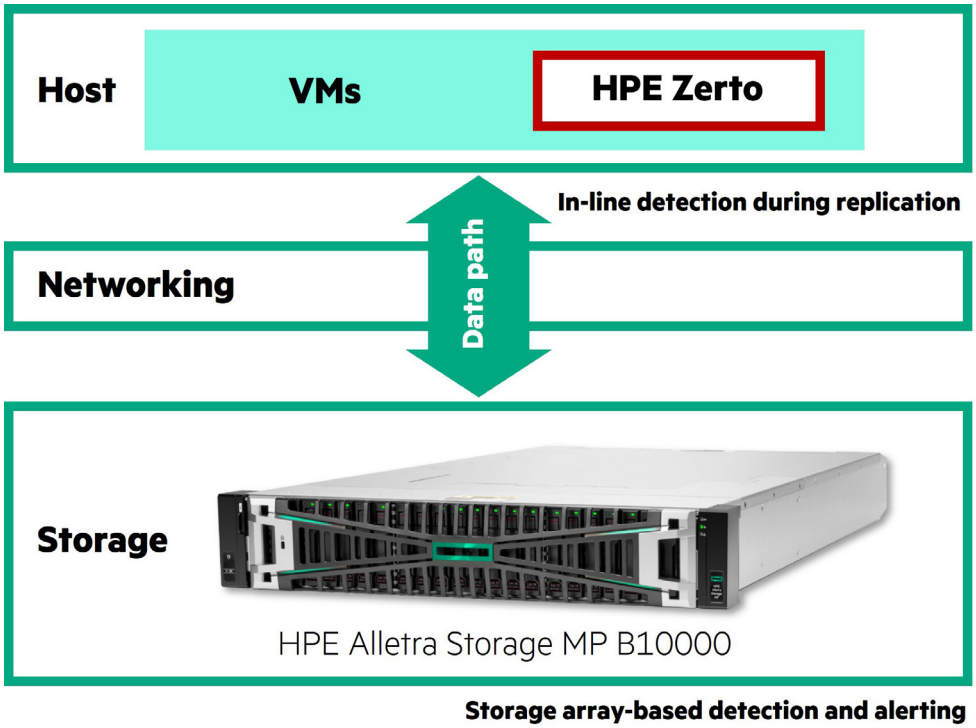

Figure 2. Dual-layered detection for ransomware protection

Evolve your cyber resilience strategy with HPE

To stay ahead of evolving ransomware threats, a comprehensive multilayered defense infrastructure is essential to protect your data. This includes protection for not only storage but also networking and compute layers. HPE is uniquely positioned to deliver an industry-leading, all-encompassing integrated cyber resilience strategy. HPE offers cutting-edge security technologies across its portfolio, including HPE ProLiant servers, HPE Aruba Networking, HPE Zerto, and HPE Alletra Storage MP B10000. Together, these solutions form the foundation of HPE's vision of delivering a fully integrated security stack for comprehensive cyber resiliency solutions across your IT infrastructure. Choose HPE as your partner to fortify your ransomware defenses for your critical data today and tomorrow.

Learn more at

HPE.com/se/en/Alletra-Storage-MP-B10000.html

Visit **HPE.com**

Chat now (sales)

a00146263ENW, Rev. 1

Hewlett Packard Enterprise | TD SYNNEX Public Sector | DLT