FlexPod®

FlexPod and today's threat landscape

Zero Trust framework, security hardening, ransomware protection, and recovery guides

FlexPod

FlexPod® is a converged infrastructure solution jointly developed by Cisco and NetApp that integrates computing, networking, and storage resources into a unified architecture. It combines Cisco Unified Computing System (UCS) for compute, NetApp® storage solutions for data storage, and Cisco Nexus switches for networking. Certified and validated by both Cisco and NetApp, FlexPod enhances interoperability and support for customers seeking a reliable, integrated infrastructure solution.

Threat landscape

In recent years, the threat landscape has evolved significantly, presenting formidable challenges across numerous fronts Ransomware stands out as one of the most pervasive and financially damaging threats. Cybercriminals deploy sophisticated ransomware tactics, encrypting sensitive data and demanding exorbitant sums for decryption keys. These attacks disrupt operations and also pose severe financial repercussions for businesses and organizations of all sizes.

Insider threats are another significant concern in the cybersecurity landscape, because malicious actors in an organization can exploit their access to sensitive information for personal gain or to inflict harm. These threats may come from disgruntled employees, contractors, or inadvertent actions by well-meaning staff. Organizations must adopt robust insider threat detection and prevention mechanisms, including stringent access controls and continuous monitoring of user activity to safeguard against internal threats.

State-sponsored cyberattacks pose yet another layer of complexity to the threat landscape, with nation-states employing their resources and capabilities to conduct espionage, sabotage, or geopolitical maneuvers in cyberspace. These attacks are often highly sophisticated, targeting critical infrastructure, government agencies, defense contractors, and multinational corporations. State-sponsored threat actors employ advanced techniques and coordinated campaigns aimed at achieving strategic objectives.

Zero Trust framework

The Zero Trust security framework is a comprehensive strategy for network security that operates on the premise of distrust, requiring thorough verification for every access request, regardless of its source or location. This approach, encapsulated by the motto "never trust, always verify," aims to fortify digital environments by employing tactics such as network segmentation, Layer 7 threat

prevention, and precise user-access control. When implemented within a FlexPod infrastructure, additional benefits include:

- Heightened security through risk reduction
- Heightened visibility into network activities for swift anomaly detection and response
- Minimized attack surfaces via least privilege access and microsegmentation
- Improved compliance with data protection regulations
- Streamlined incident response capabilities
- Protection against both external and internal threats

This integration incorporates supplementary security elements from Cisco and NetApp such as Cisco Secure Firewall Threat Defense, Cisco Secure Network Analytics, Cisco Secure Workload, and NetApp Ransomware Protection, further enhancing the security posture of the FlexPod solution.

Security hardening

In response to the escalating threat of security breaches, especially prominent instances like ransomware attacks that cause significant disruptions and financial losses for enterprises, robust security measures has become imperative. Attackers not only cause operational disruptions, they also pilfer sensitive customer data. The repercussions can tarnish the enterprise's reputation and customers' trust.

Given the rising frequency and severity of such attacks, enterprises must fortify their existing security measures and also explore and integrate new, inherently secure solutions. Recognizing the foundational role of FlexPod in enterprise infrastructures worldwide, prioritizing security best practices, and leveraging built-in tools and technologies in FlexPod solutions is crucial.

This technical report discusses securing FlexPod components, spanning compute, network, storage, and virtualization layers, offering insights, examples, and guidance to bolster overall security.

Emphasizing continual vigilance, the report advises staying abreast of evolving threats and vulnerabilities, advocating for regular updates of software and firmware to mitigate known vulnerabilities, and incorporating new security features to enhance solution security. It also recommends leveraging additional resources from NetApp, Cisco, and VMware to continuously enhance the enterprise's security posture.

Autonomous Ransomware Protection and Recovery

The NetApp ONTAP Autonomous Ransomware Protection (ARP) feature is designed to preemptively detect and alert abnormal in-file activities that indicate ransomware attacks in NAS (NFS and SMB) environments. Through workload analysis, ARP correlates volume encryption events with user activities to pinpoint potentially malicious users, implements predefined response policies such as NetApp Snapshot™ creation and user access blocking, and offers forensic capabilities for data breach investigations and recovery.

Enabling ARP involves configuring ARP-enabled volumes via NetApp ONTAP System Manager or CLI, operating initially in learning mode to establish baseline values for file entropy, extensions, and IOPs, which are then used to assess ransomware threats in active mode. Administrators can adjust detection parameters for improved accuracy based on volume workload requirements. When suspicious activity is detected, ARP generates alerts and notifications, allowing administrators to mark suspected files as false positives or potential ransomware threats and take appropriate actions via System Manager or CLI commands. Overall, ARP provides a proactive defense mechanism against ransomware attacks, enhancing security posture and facilitating swift response and mitigation efforts.

To recover from a ransomware attack and restore data to its pre-incident state, organizations often need access to decryption keys held by attackers. Recovery typically involves paying ransom with no guarantee of receiving the key or decryption as promised, thereby incentivizing further attacks.

Having a ransomware recovery plan is crucial, covering preparation, handling ongoing attacks, and recovery procedures. Instant data recovery without addressing root causes risks reinfection and prolonged downtime. Proper remediation involves containing the outbreak, cleaning infected systems, applying patches, and then recovering data.

Regularly backing up critical data minimizes loss, with timely backups reducing impact post-attack. Features like ONTAP Volume Snapshot Restore and NetApp SnapCenter® plug-ins can greatly aid recovery efforts, providing tools for Snapshot management, VM-consistent backups, and application-specific recovery, bolstering defenses against ransomware threats. The SnapCenter centralized framework supports various applications, databases, and file systems, offering scalability, performance, and enhanced security features like role-based access control and comprehensive reporting, for robust data protection across diverse environments without additional licensing costs.

Defense in depth

First, deploy FlexPod in accordance with the FlexPod Datacenter Zero Trust Framework Design Guide to implement a security posture of "never trust, always verify."

Next, use the guidelines found in FlexPod Security Hardening (TR-4984) to further secure your FlexPod environment.

Finally, use FlexPod Ransomware Protection & Recovery with NetApp Cloud Insights and SnapCenter (TR-4961) to complete your defense-in-depth strategy.