Nutanix Extends Ransomware Protections to Help Secure Customers' IT Environments

Hybrid and Multicloud Leader Strengthens Networking, Storage and Virtualisation Services

Sydney, Australia. February 23, 2021 - Nutanix (NASDAQ: NTNX), a leader in private, hybrid and multicloud computing, today announced additional ransomware protections in the company's cloud platform. These include new threat monitoring and detection, as well as more granular data replication and robust access controls - all natively built into the Nutanix stack. These new capabilities build on Nutanix's rich data services for network security, files and objects storage, virtualisation, and business continuity to help enterprises prevent, detect and recover against ransomware attacks across multiple cloud environments. At a time when attacks are becoming even more common due to the rise of remote work, these capabilities make it easier to implement security and business continuity best practices at the infrastructure level, rather than rely on a complex matrix of bolt-on security products.

A recent Gartner report[1] shared that, "in 2020, in particular, there have been swift changes to threats with increased remote work and targeted malware campaigns that take advantage of worldwide events, such as COVID-19. Ransomware has evolved beyond the commodity, widespread attacks intended to infect a single endpoint to include more advanced techniques, such as fileless malware and data exfiltration [...]. These new strains of ransomware make prevention and planning more important than ever to prevent ransomware attacks." Organisations, especially those with large remote user populations or hybrid work environments, can no longer rely on a single action or tool to protect themselves. They need to ensure their IT infrastructure allows them to best respond to these incidents.

Detect and Recover Network and Data Threats

The Nutanix cloud platform now delivers anomaly detection based on machine learning and IP reputation services with the company's security networking operations and monitoring solution, Flow Security Central, a feature with Nutanix Flow. Flow Security Central helps identify known attack vectors, including potential ransomware, at the network level before reaching the application and data layers. Specifically, Flow Security Central now monitors networks for anomalies, malicious behaviour, as well as common network attacks that propagate by searching for additional vulnerable targets. Flow Security Central also monitors endpoints to identify traffic coming from disreputable locations, something especially helpful for defending Virtual Desktop Infrastructure (VDI) deployments that are prime targets for initial ransomware infection and spread.

Closer to the application layer, the Nutanix cloud platform now also includes native ransomware detection to its file storage services within Nutanix Files. File analytics, which is a feature included with Files, now detects abnormal and suspicious access patterns and identifies known ransomware signatures to block data access in real-time. To help ensure snapshots are available when needed, Nutanix Files analytics now identifies file shares where replication and snapshots have not been configured appropriately and alerts IT administrators to this potential risk. Nutanix Files also provides immutable snapshots preventing tampering and deletion which are common attacks in ransomware payloads to hinder recovery attempts. Recovery is accelerated via native snapshot capabilities when enabled on file shares. With these capabilities natively integrated into Nutanix Files, IT professionals can not only detect but also quickly recover from ransomware attacks using native tools.

Protect Data and Applications

To further protect application data from ransomware attacks, the Nutanix cloud platform now includes new features in its object storage solution, Nutanix Objects. Objects includes more granular permissions to access objects data for primary and secondary storage. Specifically, Nutanix Objects now offers the ability to configure Write Once Read Many (WORM) policies for individual files and objects selected by an IT team to help guard against unauthorised deletion or encryption of data, thwarting many common ransomware attacks. These WORM protections can be automated by simply classifying data under a "legal hold" to prevent tampering or malicious destruction. Additionally Objects' locking features were reviewed and attested by Cohasset Associates as meeting the non-rewritable, and non-erasable storage requirements for electronic records as specified under the relevant SEC, FINRA, and CFTC regulations.

Objects now also provides data access permissions at a granular bucket level so administrators can better secure multi-tenant environments. Lastly, the Nutanix platform now delivers support for Microsoft Windows Credential Guard for virtual machines and virtual desktops running on the AHV hypervisor. Credential guard adds operating system (OS) protection from malware using credential theft attacks on Microsoft OS environments, a common vector used by ransomware to gain administrative privileges.

Ensure Business Continuity

While detection and prevention are both key aspects of an effective strategy to protect against malware and ransomware, all companies should have a plan to ensure business continuity in the event of an attack. Nutanix Mine, the company's secondary storage solution, now provides direct backup to Objects when using Mine in conjunction solutions from partner HYCU Inc. This means all ransomware protection natively available in Objects will also be applied to secondary storage, such as immutability and WORM, will also be applied to this secondary storage solutions. Additionally, Nutanix has obtained new interoperability qualifications, including Veeam® Object Immutability as well as certifications with other leading backup vendors, to extend ransomware protections to secondary storage.

"CIOs and CISOs know that there is no one solution that provides 100% protection against ransomware or other types of malware attacks, and the current remote and hybrid work models widen an enterprise's attack surface," said Rajiv Mirani, Chief Technology Officer at Nutanix. "Enterprises need a defence in depth approach to security, starting with their IT infrastructure. However, the right security tools need to also be simple and seamless to implement. Nutanix delivers a strengthened cloud platform out of the box, with an even richer set of ransomware protections available now."

All new features are currently available to customers. More information on how Nutanix can help protect against ransomware is available here.

[1] Gartner, Inc "How to Respond to the 2020 Threat Landscape," 17 June, 2020, John Watts

Contacts

Harvey Ferle
02 9929 7533
mailto:
Oisin O'Callaghan
0431612386
mailto:
Chloe Curby
+61 2 9929 7533
mailto: chloe.curby@watterson.com.au