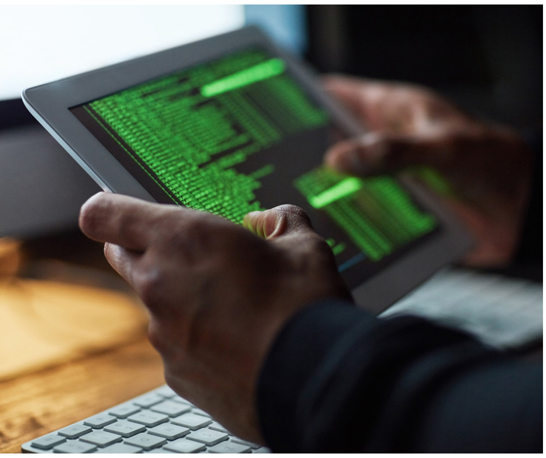
Hewlett Packard Enterprise | XYPRO

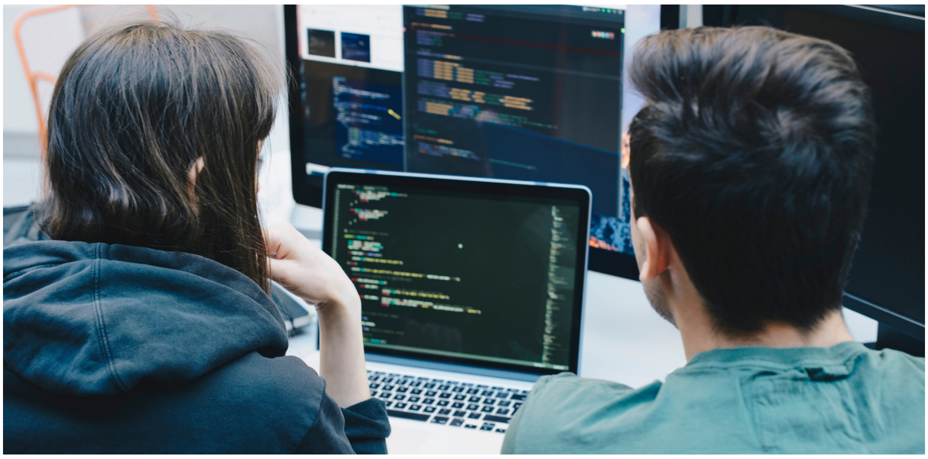
Data sheet

Check if the document is available in the language of your choice.

XYGATE OBJECT SECURITY FOR HPE NONSTOP

Enforcing object-based security for HPE NonStop





Key benefits

- Is simple to use
- Reduces administration costs
- Increases productivity
- Offers powerful security controls

Compliance, government legislation, and other regulations mandate that HPE NonStop resources be properly secured to prevent unauthorized access from data breaches, from both inside and outside the organization. Safeguard provides tightly restricted access to Guardian resources. Operational support system (OSS) resources can be secured with standard UNIX® "rwx" security or with POSIX ACLs. However, implementing access control to protect against real-world scenarios may require sophisticated setups and command procedures.

DYNAMIC RULES

XYGATE Object Security (XOS) protects all aspects of your HPE NonStop system, covering both Guardian and OSS environments. Rather than managing with static, reactive Safeguard mechanisms, XOS uses dynamic rules that adapt to the characteristics of each access attempt. For example, if OPER.BACKUP is attempting to read a file while running BACKUP, XOS grants access, but if OPER.BACKUP attempts to read the same file using EDIT, XOS would deny access. These extremely powerful dynamic access rules are applied to volumes, subvolumes, files, devices, subdevices, processes, and subprocesses.

EXTENDED SECURITY VECTORS

XOS extends both Guardian and Safeguard security vector parameters to include "Rename" (RN), "Give" (G), "License/ Revoke" (L), and "ProgID ON/OFF" (PR) providing additional granularity and features for your security implementation. No other HPE NonStop security solution can do this.

Key features

- Guardian and OSS
- Simple, powerful RBAC rules
- Dynamic user groups
- Powerful wild card means greater applicability of rules without adding complexity
- Verification of configuration before deployment
- Dynamic rules adapt to the type of access attempt
- Objects protected before they exist
- Alias support
- Remote access control to files in OSS

SAVE TIME AND EFFORT

XOS uses dynamic functional groups of users (ACLGROUPS) that allow or deny access to an object. Use ACLGROUPs wherever you would use user IDs in security rules. Create an ACLGROUP that includes all these user IDs and use the ACLGROUP in the rules protecting the files, rather than having to list the users or user groups individually in each rule. If one or more user's roles change, you only need to modify the ACLGROUP and not all the individual rules.

REDUCE THE NUMBER OF RULES

Each XOS rule can have multiple masks. This technology greatly reduces the number of rules required to protect the system. If the same users are granted the same pattern of access to a set of files, then all the files can be included in one rule.

POWERFUL WILD CARD

XOS groups' object access records that contain wild card policies are applied consistently regardless of the existence of the secured objects at the time your security policy is defined. This means you can create security rules for objects that don't even exist yet! Users can't create objects that don't follow the rules, and the rules are in place to protect those objects from the moment they're created, even dynamically adapting the security over time. **It can't be emphasized enough the power of this technology to protect your environment**.

ANY OBJECT ATTRIBUTE

Traditional security ACLs are applied against objects based on the object name alone. This is limiting and does not factor many other attributes of an object that may be relevant to applying security. XOS protects SQL tables and applies security based on the age of a file, enabling the security to change along with the object.

Using XOS, objects can be protected by name or any other object attribute, alone or in combination. For example, authorization to purge save abend files could be given to users based on multiple criteria (object name, age, and type).

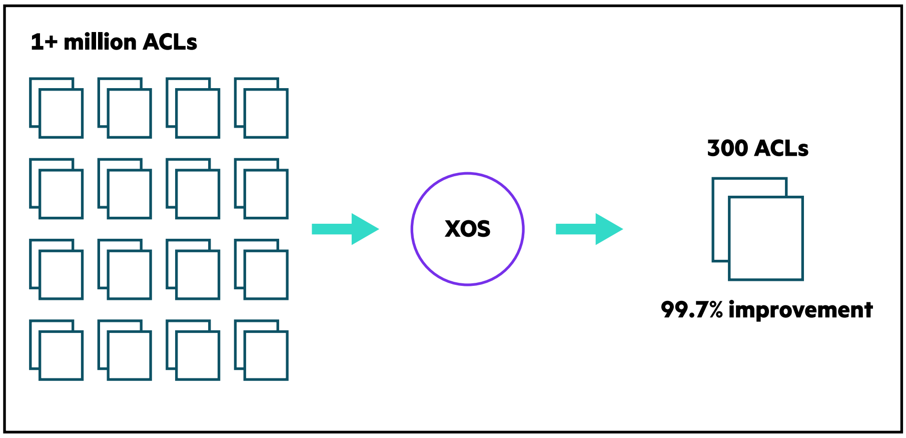


FIGURE 1. Visible benefits of using XOS for HPE NonStop[1]

[1] Actual customer data: Large global credit card company manages entire network of HPE NonStop servers with XOS, with less than 300 role-based access control rules. Before XOS, over a million Safeguard ACLs were used for the same purpose

ORDERING INFORMATION

XYGATE Object Security for HPE NonStop can be ordered using the product IDs (PIDs) listed in the following table:

Product	Product ID (L-Series)	Product ID (J-Series)
HPE NonStop XYGATE Object Security	BE246AC	QXOS

LEARN MORE AT

hpe.com/info/nonstop

xypro.com

Make the right purchase decision.
Contact our presales specialists.

Chat Email Call

Get updates

Hewlett Packard
Enterprise

a50004628ENW, August 2021