SOLUTION BRIEF

Enhancing Security Visibility with Pure Storage and Cisco

Optimizing cyber resilience through enhanced storage visibility

In today's data-driven world, security and simplicity are critical. Data storage systems containing sensitive information face constant threats due to the valuable data they hold. The cybersecurity threat landscape is evolving rapidly in both speed and scope, making it challenging for security teams to keep pace with emerging threats using their available resources. This makes it essential to have a security solution that is both automated and easy to set up, ensuring that critical data is protected against real-time threats.

The integration of Pure Storage® and Cisco XDR enhances data security by combining efficient storage solutions from Pure Storage with Cisco's robust threat detection. Together, they offer a unified approach to safeguarding critical assets, ensuring data remains secure and accessible against evolving threats.

Solution Overview

The integration of Pure Storage FlashArray™ and FlashBlade® with Cisco XDR leverages advanced threat intelligence to significantly enhance security visibility across the storage infrastructure. This collaboration enables comprehensive aggregation and analysis of security data from storage components. This powerful combination improves threat detection and response times, leading to robust security and more efficient cyber threat management. Ultimately, it fortifies your defenses against the ever-evolving landscape of cyber threats, ensuring a secure and resilient infrastructure.

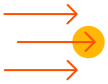
This integration offers a suite of automated workflows triggered by alerts or incidents based on automation rules. These rules can be defined by administrators to customize rules to fit specific security needs. Cisco XDR uses advanced analytics and AI to evaluate threat severity and initiate appropriate response measures through these workflows, ensuring swift and effective mitigation of potential threats.

Protection

Safeguard critical data with automated responses that use SafeMode™ Snapshots.

Simplify

Streamline security deployment for on-premises FlashArray and FlashBlade appliances



Enhance

Boost threat detection with Unified Storage Insights to gain instant visibility into storage events and potential threats across your infrastructure

Cisco XDR Integration with Pure Storage FlashArray and FlashBlade

Cisco Automation Remote is an on-premises virtual appliance designed to bridge communication between your workflows and resources within your private network. Many on-premises devices are isolated from the public internet; Automation Remote enables these devices to participate in your workflows by securely linking them with cloud services.

Set up is simple: Set up a remote server in Cisco XDR, download the configuration file, and deploy the Automation Remote virtual appliance using VMware vSphere. Once the appliance is powered on, verify that its status changes to "Connected" on the Remotes page in the Cisco XDR portal. This connection allows you to initiate action scripts through Cisco XDR workflows, seamlessly integrating your isolated on-premises devices into your automated processes.

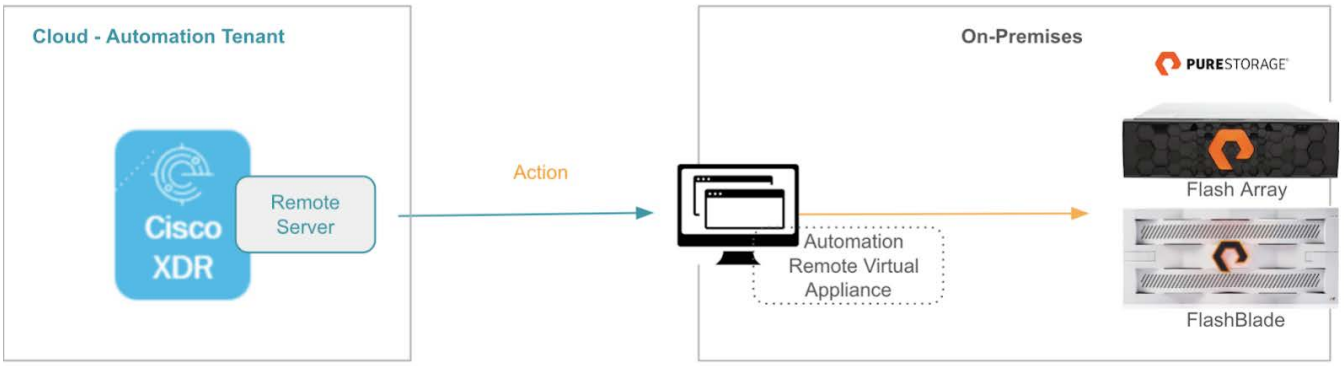


FIGURE 1 Cisco XDR Integration with Pure Storage FlashArray and FlashBlade

How Automated Threat Response Works

Cisco XDR streamlines security operations through automation and guided response recommendations, effectively addressing threats across all relevant control points. This cloud-based solution enhances detection capabilities, accelerates response times, and boosts productivity by seamlessly integrating with Cisco's extensive security portfolio and select third-party offerings. Cisco XDR collects and correlates data and telemetry across multiple sources—including network, cloud, endpoint, email, identity, and applications—to provide unified visibility and deep context into advanced threats while reducing time-consuming false positives.

When a potential threat is detected, Cisco XDR activates a suite of automated workflows triggered by alerts or incidents based on predefined rules. Utilizing machine learning and artificial intelligence, the system evaluates threat severity and initiates appropriate response measures through the Cisco XDR workflows.

For instance, if suspicious activity is detected on any endpoint and identified within the Cisco XDR workspace, an alert is generated, prompting an incident response via the respective Cisco XDR workflows. To safeguard against potential data loss, corruption, encryption, or other threats posed by ransomware, an immutable snapshot of the relevant protection groups or volumes can be captured. Immutable Pure Storage SafeMode™ snapshots ensure critical data remains protected from deletion, modification, or encryption by ransomware, thus maintaining data integrity and security without requiring complicated setup or professional services engagement.

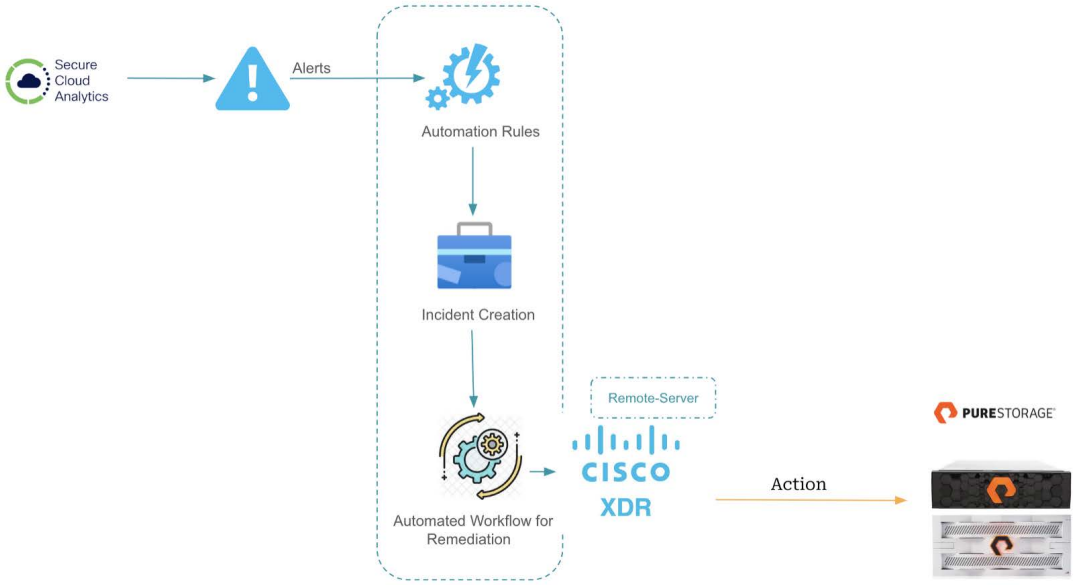


FIGURE 2 Cisco XDR threat response

Use Case Scenarios

The following table lists common use case scenarios.

Target	Action	Description	Use Case
FlashArray	Take protection group snapshot	Creates a snapshot of all volumes within a protection group	An attack is detected and a SafeMode protected snapshot is taken to secure critical data.
	Take volume snapshots	Creates a snapshot of the volume	An attack is detected and a SafeMode protected snapshot is taken to secure critical data. Note: Volume level snapshots are only protected by SafeMode if SafeMode is enabled array-wide.
	Remove local user	Removes a local user from FlashArray.	A user account has been compromised and is trying to dump or delete critical data.
FlashBlade	Take file system snapshots	Creates a snapshot of the fIle systems of FlashBlade	An attack is detected and a file system snapshot is taken to secure critical data.

About Cisco XDR

Cisco has changed the way security teams approach Threat Detection, Investigation, and Response (TDIR). Our cloud-based extended detection and response (XDR) solution is the fastest, easiest way to integrate TDIR into your security posture and simplify security operations, providing a streamlined approach to quickly detect, prioritize, and respond to sophisticated threats.

About Pure Storage

Pure Storage offers a cloud experience that empowers every organization to maximize their data's potential while minimizing the complexity and cost of managing the underlying infrastructure. Our commitment to providing true storage as-a-service enables customers to adapt to evolving data needs rapidly and efficiently, whether deploying traditional workloads, modern applications, containers, or more.

We believe we can significantly reduce data center emissions worldwide through our environmental sustainability initiatives, which include designing products and solutions that help customers decrease their carbon and energy footprint. With a certified customer satisfaction score in the top one percent of B2B companies, our continuously growing list of customers ranks among the most satisfied in the world.

Additional Resources

- Discover Pure Storage data protection solutions.
- Learn how SafeMode secures data from ransomware attacks.
- Pure Storage and Cisco XDR marketplace.
- Explore five ways to experience XDR.
- Read why Cisco XDR Matters.

PS2687-01-en 10/24