FlexPod®

Guard against intruders with a zero-trust framework

Most companies don't allocate enough resources for security until they've been hacked. In their defense, it's hard to know how many security mechanisms to establish and how to assess whether they are adequate. But ignoring the question can be fatal. Recovering from a ransomware attack often takes 15 days, and some companies don't recover at all once their data is lost and their customers no longer trust them.

The FlexPod® zero-trust framework is a tested and validated approach for deploying Cisco® and NetApp® technologies to build multi-tenant, secure infrastructure. Most applications run in virtualized environments, so, whatever your workload, this solution can help establish a comprehensive approach to security in your organization.

What if you addressed security holistically, before having an incident? We deliver a FlexPod solution that builds a zero-trust security framework for your infrastructure.

We start with a hardened set of systems from both Cisco and NetApp. Indeed, NetApp storage is the only enterprise platform approved to hold top-secret data. We integrate security as part of the architecture so that you can protect, detect, respond, and recover from attacks

Challenges

Today's threat environment has evolved to the point where every organization needs to consider its vulnerabilities.

Solution benefits

- Comprehensive security approach
- Greater visibility
- Reduced attack surface
- Improved compliance
- Rapid incident response
- Protection from internal and external threats

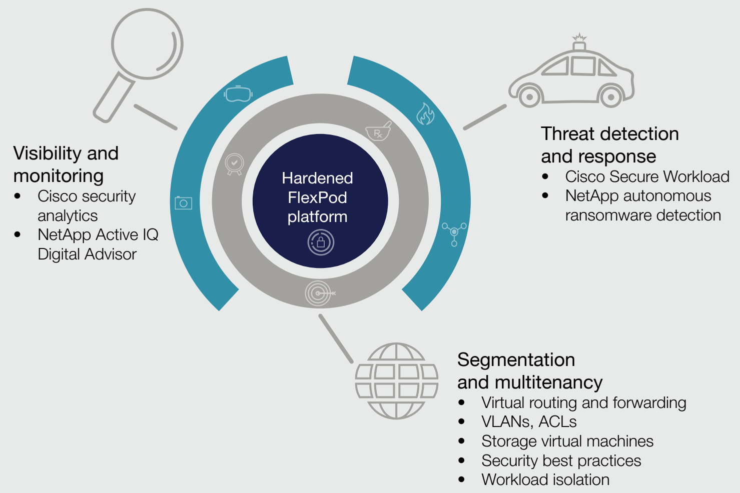
The data points to the need to establish a zero-trust environment in which you protect from both internal and external attacks, whether or not the actors have good intentions. The 2023 Verizon Data Breach Investigations Report finds that 74 percent of all breaches involve a human element through privilege misuse, stolen credentials, or social engineering. External actors were responsible for 83 percent of breaches with 95 percent of them were financially driven.

Ransomware is one of the top breaches and is responsible for 24 percent of them. While many incidents reported no loss, for those reporting losses, the 95th percentile cost ranged from $70 to $1.2 million. The bottom line: you need to build security into your infrastructure from the beginning.

How it works

FlexPod is trusted by thousands of customers across the globe. FlexPod unites components including innovative Cisco UCS® servers, NetApp storage, Cisco Nexus® and MDS networking, Cisco Intersight,® and NetApp ONTAP® storage management to accelerate the delivery of modern workloads future ready, and optimize resources to maximize efficiency.

Security is a key aspect of FlexPod, and it is designed as part of the architecture, from day one. A zero-trust FlexPod solution hardens the platform so every user and interaction are validated. The principles for such a framework include the following:



Hardened FlexPod platform
Visibility and monitoring
• Cisco security analytics
• NetApp Active IQ Digital Advisor
Threat detection and response
• Cisco Secure Workload
• NetApp autonomous ransomware detection
Segmentation and multitenancy
• Virtual routing and forwarding
• VLANs, ACLs
• Storage virtual machines
• Security best practices
• Workload isolation

Figure 1) FlexPod zero-trust framework is built on a hardened FlexPod with added Cisco and NetApp security products

- **Never assume trust:** always verify and enforce least-privilege access
- **Establish and enforce trust** on platforms through device and protocol hardening
- **Reduce the attack surface** using network segmentation and controlled traffic flow between segments
- **Provide complete visibility** of processes, devices, and workloads.
- **Quickly detect, block, and respond to threats,** then verify data integrity and implement loss-protection countermeasures

The zero-trust framework is built upon a secure foundation by hardening the native FlexPod solution (Figure 1). This includes activating and using best practices to deploy NetApp ONTAP features designed to protect your storage. The Cisco Intersight platform helps you build secure infrastructure stacks that include the latest firmware and software patches and best practices for deployment.

Then we layer in specific Cisco and NetApp security products to implement:

- **Segmentation and control** of the multitenant environment
- **Visibility and monitoring** to provide network and operating-system anomaly detection
- **Threat detection and response** to help protect against threats, including ransomware

The result is a combined solution that is the product of many hours of collaborative innovation between Cisco and NetApp engineers. The solution is provided in cookbook-like instructions in a Cisco Validated Design, and you can deploy it automatically using downloadable Ansible playbooks.

Segmentation and multitenancy

Segmentation is a key security mechanism that separates various application domains so that malicious actors—or compromised software—cannot do damage beyond a well-contained perimeter. Multitenancy is used so that a single FlexPod can host multiple clients, but also to isolate multiple tiers within individual applications. Imagine how an intrusion into a presentation tier could be prevented from gaining unauthorized access to a customer database.

- **Virtual networks** segment traffic through virtual routing and forwarding on the top-level Cisco Nexus 9000 Series Switches, through the Cisco UCS fabric interconnects, where the various networks are separated with virtual LANs (VLANs), and into specific virtual machines that are connected (Figure 2).
- **Traffic filtering** allows only authorized traffic to pass between application components and between the applications and the outside world. Cisco firewall, Cisco threat defense, and Cisco Secure Workload products enforce access-control policies through packet inspection; they also can delve into specific protocols to filter out malicious URLs.
- **Virtualization hardening** uses port groups in VMware vSphere to enforce virtual machine connectivity to VLANs, and consistency is enforced with role-based access control. Virtual machines are hardened using VMware best practices.
- **Storage virtual machines** (SVMs) are used on the NetApp controllers so that each tenant has its own instance of ONTAP, separating data between tenants and application tiers so that any intrusion that compromises a single SVM can access only a limited amount of data.

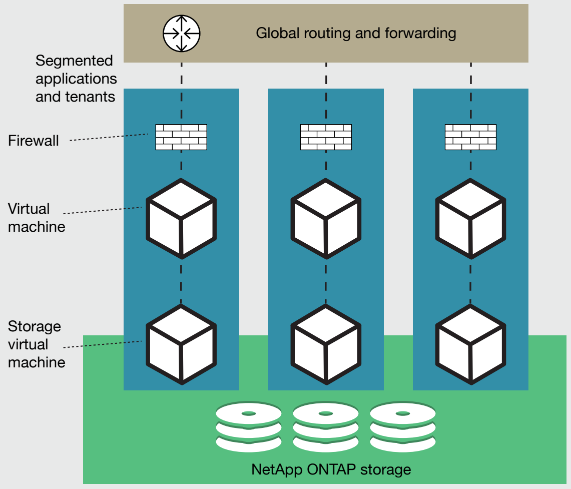


Figure 2) Segmentation puts each application, component, or tenant in its own space with its own virtual networks and storage virtual machines

Visibility for threat detection and analysis

You can't protect what you can't observe. To provide insight into the status of security threats in your data center, we watch for anomalies and defend specifically against ransomware attacks:

- **Anomaly detection** uses behavioral modeling to create a baseline of normal behavior, and then raise an alarm when anomalies or behavior changes occur. Cisco Security Analytics establishes a comprehensive set of agents that collect and analyze telemetry through your network. Cisco Netflow data from various sources in the network is processed and

> **“We used FlexPod to replace a conglomerate of different vendors and solutions—helping us reduce costs and complexity, while also better preparing us for future challenges.”**
>
> Head of platform services,
> Consulting and IT company
> From Forrester Report

sent into a behavioral engine to understand what traffic is normal, and then, once it has learned about your networks, it watches for anomalies or behavior changes and raises an alarm if it finds them (Figure 3).

- **Ransomware defense** has become necessary because of the severe consequences of a successful attack. These attacks are primarily against storage itself, so NetApp Active IQ Digital Advisor undertakes a set of prescriptive wellness checks that help protect against ransomware and recover quickly in the event of an intrusion. The software monitors the operation of NetApp ONTAP features that protect storage, including snapshot counts, retention, automatic deletion settings, and encryption.

Threat detection and protection

Building upon network and virtual machine segmentation, and visibility into network and storage activity, a layer of threat-detection and protection software actively protects workloads:

- **Securing workloads:** Cisco Secure Workload controls east-west traffic that otherwise may not be inspected by a firewall (see Figure 4 on next page). It establishes agents within virtual machines that set up micro-perimeters around workloads through microsegmentation policies. It analyzes communication within applications, and prohibits, for example, inappropriate communication between layers, or unexpected applications running in a virtual machine. It detects common vulnerabilities with dynamic mitigation and maintains a threat-based quarantine.
- **Data governance:** while Cisco Secure Workload protects at the OS, application, and network level, NetApp BlueXP provides governance at the data level. It helps you understand where your most important data is, whether on-premises or in the cloud. It deeply scans your data estate, giving visibility into unsecured data and providing AI-driven guidance for instant problem resolution.
- **Protecting against ransomware:** because it has become such a formidable threat, and has such serious consequences, we include ransomware protection as a special case. We protect against the main feature of ransomware, which is making data unavailable to the organization. We implement standard policies in NetApp ONTAP through FPolicy settings, then enable NetApp autonomous ransomware protection that learns patterns

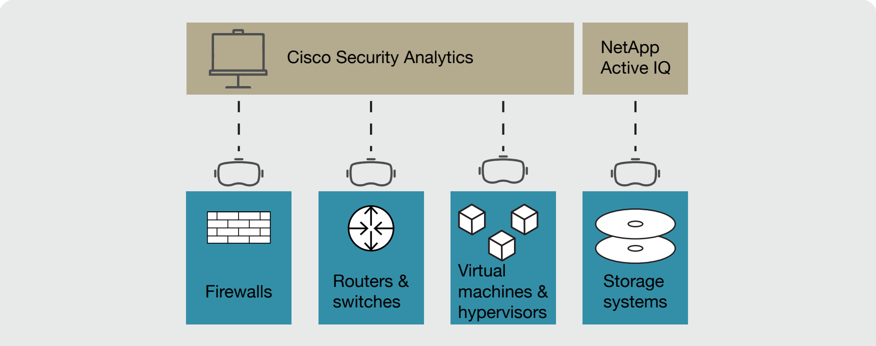


Figure 3) The solution provides visibility into the security status of infrastructure components.

and then protects against anomalous behavior. It does not disrupt I/O; it takes a snapshot and alerts administrators. While this protection works on the storage device itself, NetApp Cloud Insights storage workload security adds protection at the user level, and can operate on premises and in the cloud.

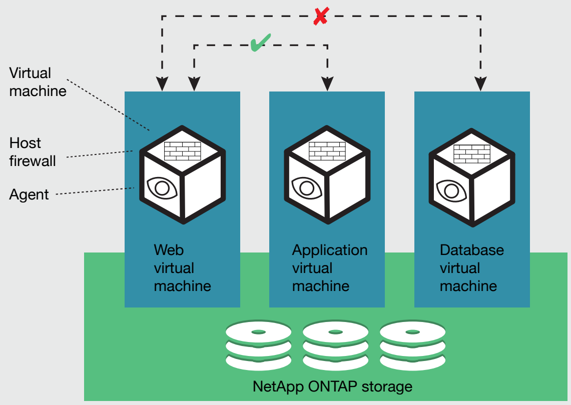


Figure 4) Cisco Secure Workload controls east-west traffic to prohibit inappropriate communication between layers

Automated deployment

As with all of our solutions based on Cisco Validated Designs, we provide a GitHub repository of Ansible playbooks so that you can accurately and quickly deploy this solution with the confidence that no step is left undone. We provide playbooks to support both day-0 and day-1 operations, including:

- **Initial setup:** through a combination of Ansible playbooks and manual steps, you can deploy and verify the infrastructure.
- **Security enablement:** these playbooks enable security best practices at the hypervisor, compute, network, and storage layers, enabling the tools that this solution brief describes.
- **Tenant onboarding:** once your FlexPod zero-trust infrastructure is set up, playbooks automate tenant deployment on all of the devices when bringing on a new tenant or application tier.

Data is changing IT requirements

Data is changing IT requirements, driving new applications, business, and consumption models. The degree to which data has become the focal point of business operations has exposed the reality that it is the primary vulnerability from a security perspective.

The FlexPod zero-trust framework establishes a solid foundation for data-lifecycle security from the core, to the cloud, to the edge. It is smart infrastructure that will grow with you and provide the flexibility to adapt as your business needs change

Security is more than just a single feature that can be turned on or off. The diversity of attacks against your data and infrastructure dictate security that needs to be built into a platform. Indeed, since its inception, FlexPod has been built on security, with secure multitenancy designed as a key use case. This FlexPod solution simplifies security by making it straightforward to integrate the platform and security practices into your business.

Explore FlexPod

Learn more about FlexPod solutions at cisco.com/go/flexpod

Download the Security CVD design guide or view all Cisco Validated Designs for FlexPod