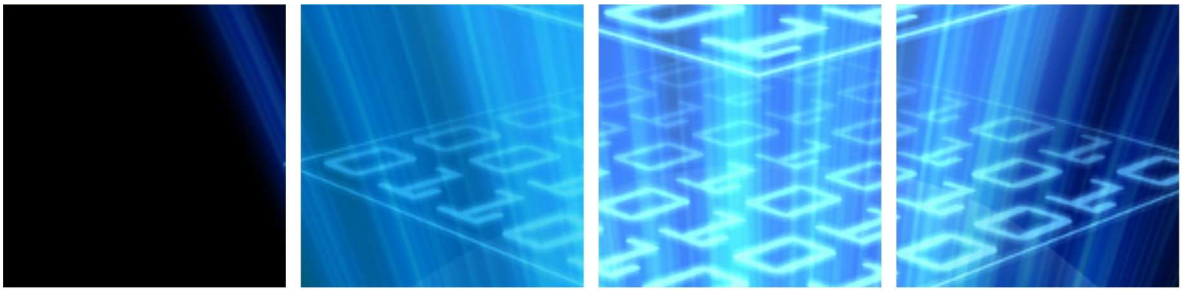
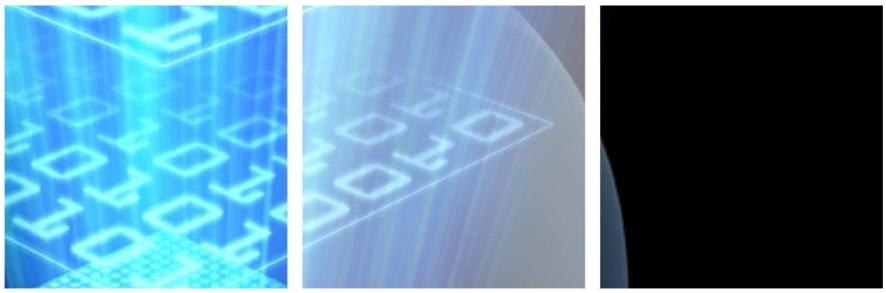
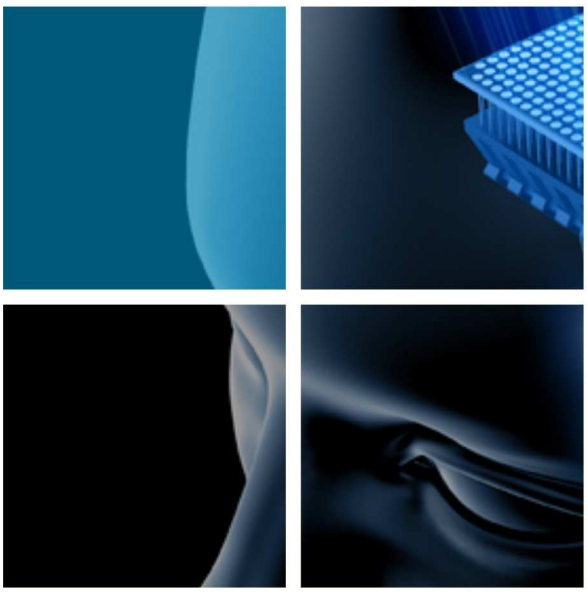


Cyberoam
virtual UTM
Appliances





Security in **Virtual Data Center**
Enterprise/MSSP **"Security-in-a-Box"**
Security in a Virtual Office or **"Office-in-a-Box"**

Take Control of Your Security Infrastructure!

Virtualization is taking organizations beyond the boundaries of their physical network infrastructure, empowering them to leverage their resources better and more flexibly, while quickly responding to the changing needs of their business. While higher efficiencies and lower total cost are few benefits of virtualization, security in virtual environments is an issue that organizations are struggling with, in the wake of virtualization!

Cyberoam Virtual UTM Appliances

Get complete control of your security infrastructure with Cyberoam virtual UTM appliances that offer industry-leading network security for your virtualized environments. Cyberoam virtual UTMs give you the flexibility to deploy a mix of physical and virtual appliances in your network, which can be managed centrally.

With the ability to scan all traffic in the virtual environment, Cyberoam virtual UTM protects virtual networks from attacks on hypervisor management console, hypervisor & Guest OS, virtualized web-facing applications and servers and allows organizations to secure Zero Trust Networks with its comprehensive security features in virtualized form.

Get a complete virtual security solution with Cyberoam virtual UTM, virtual Cyberoam Central Console and Cyberoam iView – Logging & Reporting software.

If you are an MSSP, reduce your operational and capital expenditure, and serve your customers better and at reduced costs, by having elastic network infrastructure utilization with virtualization.

If you are an SMB with virtual infrastructure, you can now extend your existing infrastructure to include security for your network without the need to add hardware security appliances, thus saving cost and time.

Cyberoam®
Securing You

Benefits

- Security for dynamic virtual environments and Cloud
- Choice of individual or mixed virtual and physical network infrastructure
- Single virtual appliance to deploy and manage for comprehensive network security and single vendor to contact
- Easy scale-up of security infrastructure as business grows
- Deployment flexibility with licensing based on number of vCPUs
- Management and display of regulatory compliance

UTM Security features

- Stateful Inspection Firewall
- Gateway Anti-Virus and Anti-spyware
- Intrusion Prevention System
- Gateway Anti-spam
- Web Filtering
- Application Visibility & Control
- Web Application Firewall
- Virtual Private Network (VPN)
- IM Archiving & Controls
- Bandwidth Management
- On-Appliance Reporting
- Identity-based Security

Take control of what you want, how much you want, how you want it, with Cyberoam virtual UTMs!

WHAT you want

Virtual Security solution: Cyberoam virtual UTM appliances give complete control of security in virtual data-centers, Security-in-a-Box and Office-in-a-Box set-ups to organizations. Get comprehensive security in virtualized environments without the need for deploying a hardware security appliance anymore.

Support for infrastructure scale-up as the business grows: By providing a virtual network security solution to organizations and MSSPs, Cyberoam virtual UTMs allow security in virtual networks to be scaled up as the business needs of organizations/MSSP customers grow.

HOW MUCH you want

Easy Upgrade: Cyberoam virtual UTM appliances can be upgraded in no time and with maximum ease, using a simple activation key, to match the growing business needs of organizations/MSSP customers.

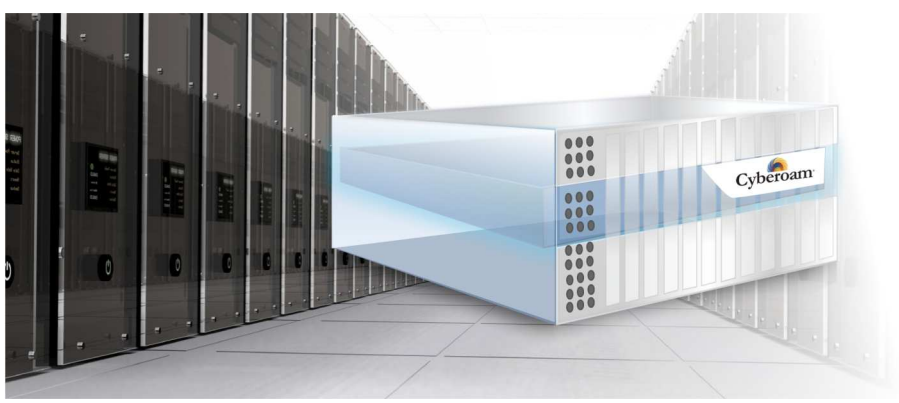
Benefit of shared infrastructure: By capitalizing on lean and peak periods of activities in the networks, organizations and MSSPs can optimize the resource utilization in their own/customer networks, using Cyberoam's security in virtualized form.

HOW you want

Choice of Virtual and Physical Infrastructure: Organizations and MSSPs get the flexibility to choose between individual and a mix of physical and virtualized environments without worrying about security, with Cyberoam's security solution for both physical and virtualized environments.

Deployment Flexibility: The licensing model for Cyberoam virtual UTM appliances is based on the number of vCPUs, giving deployment flexibility to organizations and MSSPs, unlike most competitor models that are based on concurrent sessions and number of users. Cyberoam virtual UTMs allow organizations to get maximum benefits of Cyberoam's multi-core processing architecture by flexibly allotting vCPUs from the virtual infrastructure to the virtual UTM appliance.

No Hard Limits on Usage: If the number of network users in organizations or MSSP customer networks increase beyond the recommended number for a given model, Cyberoam virtual UTMs continue to secure these networks, allowing organizations and MSSPs to upgrade to a higher model only when they want to.



Cyberoam Offers

1.Protection for Virtualized networks

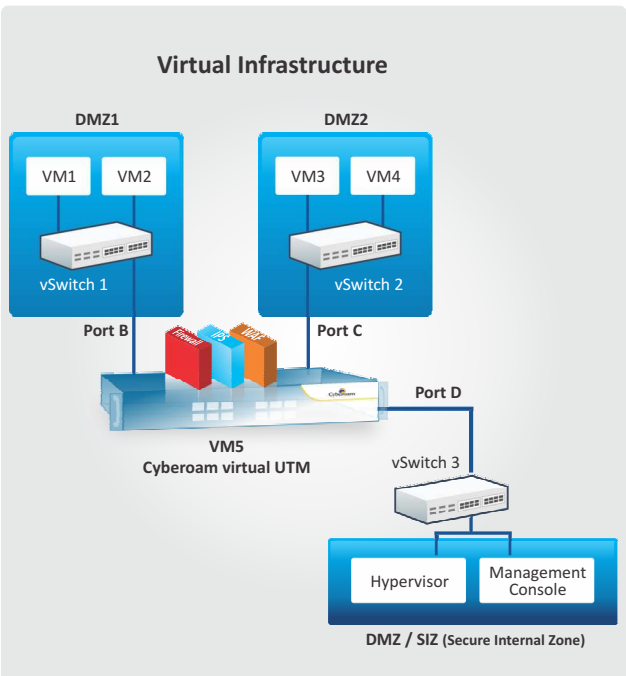
Inter-VM traffic scanning

External hardware security devices are incapable of scanning inter-VM traffic, creating blind spots in traffic within the virtualized environments. With their ability to scan Inter-VM traffic, Cyberoam virtual UTMs remove the network blind spots and allow granular firewall and security policies over inter-VM traffic.

Hyperjacking & Hypervisor vulnerabilities

In cases where the hypervisor management console is placed in live production virtual environment due to lack of segmentation within virtual environments, the virtual networks are prone to attacks that exploit vulnerabilities on software layers like the hypervisor management console, hypervisor & Guest OS, putting the security of entire virtual network at risk.

Cyberoam virtual UTMs enable administrators to segment the hypervisor management console in DMZ and route all traffic through Cyberoam virtual UTM appliances. The Intrusion Prevention System on Cyberoam virtual UTMs scans Inter-VM traffic, VM to hypervisor traffic and ensures threat-free traffic. Web Application Firewall protection on Cyberoam virtual UTM blocks attacks that exploit vulnerabilities in the virtualized web applications.



Separation of duties

In case of external network security solutions, a level of Separation Of Duties (SOD) is achieved by default because the functions are hosted on separate physical systems that are managed and configured by separate teams. However, in case of collapsed DMZ, loss of SOD by default between security/network security and operations leads to security risks and potential conflict of interest between the roles.

Role-based administrator controls in Cyberoam virtual UTM allow separation of administrator duties. Cyberoam offers logs of administrator events and audit trails with its Layer 8 identity-based security and on-appliance reporting.

Zero Trust Networks

In an office-in-a-box setup, since the virtual infrastructure hosts the entire user workgroup, User-Identity based control and visibility becomes even more important.

Cyberoam's Layer 8 Identity-based security policies over user authentication, service authorization and reporting (AAA) secure the Zero Trust virtual networks. Deployed at the perimeter or within the virtual infrastructure, Cyberoam virtual UTMs offer visibility and user-based access control in the virtualized environment. Ensure consistent security policy across your network – virtual and physical, with Cyberoam.

2.Comprehensive security:

Cyberoam virtual UTMs simplify the security for your virtual environments by consolidating multiple security functions in a single virtual appliance. Get all security features found in Cyberoam's hardware appliances, viz. firewall, VPN, Gateway Anti-Spam, Gateway Anti-Virus, IPS, Web Application Firewall, Web Filtering, Application Visibility & Control and much more, to make your virtualized environments as secure as your physical network infrastructure.

3.Easy to deploy

Cyberoam virtual UTMs are easy to deploy with a licensing model that provides the flexibility to allot the number of vCPUs for Cyberoam virtual UTM based on your requirements. A simple key activation to upgrade to higher models and no hard limits on crossing recommended usage limits make Cyberoam virtual UTMs easy to deploy in your virtualized set-ups.

4.Compliance Management

In case of collapsed DMZs that hold sensitive information and office-in-a-box setup, compliance and privacy requirements become difficult to achieve, especially in a virtual environment. By segregating and securing traffic and data between and around your virtual entities, Cyberoam virtual UTMs help you stay regulatory compliant. The integrated logging and reporting feature offers in-depth reports of activities in your virtual infrastructure to support your organization to display compliance.

5.Centralized Management of Hardware and Virtual appliances

Centrally manage your physical and virtual infrastructure using a single interface with Cyberoam Central Console, available in hardware and virtual forms. Reduce the expense of separate management consoles for your physical and virtual environment needs as well as ensure centralized, consistent and quick security actions across your network.