

Checkmarq BOS Series

BORDER OFFICE SECURITY

The Checkmarq BOS appliance delivers powerful protection against internet and network security threats to SMB offices.

Failure is not an option

Each year dramatic financial losses are the result of cyber crimes and security holes. Cyber crime is not only a risk from the internet, but internal attacks happen as well. Research teaches us that 80% of all damage is done by attacks coming from within the network. In the 2005 CSI/FBI Computer Crime and Security Survey, "software vulnerability exploits", "unauthorized access", "Distributed Denial of Service" are listed as the top "Dollar Amount Losses". Since existing infrastructure in many organizations is no longer sufficient to protect against the increasing intelligence of vulnerability based and high-volume attacks which interrupt business operations, Checkmarq delivers state-of-the-art bi-directional Intrusion Prevention Appliances that can not only stop internet-initiated attacks, but also prevents internal users from attacking the network, or even getting infected through unknown malware situations. Some users just do not have the knowledge about security issues and need to be protected against their own browsing rituals.

Cost efficiency

Checkmarq delivers high-end Intrusion Prevention Services to SMB offices, completing the existing functionality of basic security, i.e. firewalls. As prevention reduces the costs of failure, Checkmarq IPS solutions are cost-efficient.

Rule-based IPS

Running on CMQ firmware, Checkmarq IPS appliances offer rule-based intrusion prevention through the world's largest database of rules. These rules are continuously monitored for additions and make no exception towards Operating Systems or applications. By using this set of rules, Checkmarq IPS offers protection against buffer overflows, CGI attacks, NetBIOS queries, HTTP-based attacks, RPC anomalies, telnet negotiation code anomalies, ARP spoofing, polymorphic, shell code and Unicode irregularities, and many other network intrusion attacks.

Bi-directional Intrusion Prevention

Unrestricted employee internet access allows employees to browse the internet freely and gather automated internet attacks. Current IPS appliances only support prevention that is initiated from Internet. Checkmarq Border Office Security range prevents internally initiated attacks as well by checking the data traffic in a bi/directional manor. If an internal user initiates a session then the reply data will also be checked. This stops malware that has been installed on Internet sites worldwide with the intention of infecting systems that just visit the site.

Since the Checkmarq BOS IPS solutions cover bi-directional prevention on all anomalous or malicious traffic on the network, it works as a powerful add-on to a firewall and is there for an addition to all network security solutions.

Checkmarq Vulnerability Definitions Feed (CVDF)

Border Office Security Range products can be equipped with the Checkmarq Vulnerability Definitions Feed (CVDF) for instant threat protection against hackers, worms, malware and zero-day vulnerability exploits. The Online Management Centre gives network administrators a simplified insight of the network security. Based on real-time reporting, attacks directed towards network vulnerabilities can be made visible in a clear report. This is all possible because Checkmarq uses self-made real-time deep packet inspection filters.

Malware

An increasing problem within network security is malware. Malware is software that is put on Internet in places that people browse to, in order to upload unwanted software without the user knowing about it. Spyware is well known example of malicious software that is uploaded without warning. By inspecting data traffic bi-directional Checkmarq is able to filter known malware from the line and warn the users about sites that provide these kinds of attacks. By adding this protection Checkmarq adds an extra level of security that is often forgotten.

Ensuring Business Continuity

With the Checkmarq BOS Intrusion Prevention appliance in your network, risks and losses are minimized by:

- Reduction in maintenance because of network infections by viruses, worms, and Spyware
- Reduction of downtime from DDoS attacks and Zombie threats
- Protection against theft of intellectual property due to undesired access
- Regulatory compliance through protection of confidential data
- Pro-active protection from threats while patches are being tested and deployed
- Improved security posture through acceptable application usage enforcement



*office security
sophisticated
powerful*

Checkmarq delivers high-end SMB security solutions at an affordable price. 100% customer satisfaction is a guarantee!

Call us! Learn more about how Checkmarq BOS Series can not only secure your network but bring you peace of mind as well.