Datasheet ControlGuard

Prevents information leakage and unauthorized access to any device or interface.

ControlGuard is an enterprise-grade solution that offers a proven technology to protect your company from the risks of data loss from both insiders and external threats. By implementing policy-based control of endpoint access to portable devices and removable media, ATROG's ControlGuard solution effectively prevents unauthorized use of enterprise data.

ControlGuard allows security administrators to define policies that are automatically distributed to the endpoints. These policies are enforced by the Agents and all relevant events are monitored and communicated back to the Management Server providing real time notifications, alerts and reports. The Agents are intelligent and independent modules that remain active even when the endpoint is not connected to the network.

ControlGuard integrates with directory services, enterprise management systems, application infrastructure and distribution systems enabling easy deployment and minimal administration overhead.

Key Features

- Real-time notifications
- Audit logs stored in corporate databases
- Customized web-based reports
- Control and monitor how information is downloaded to the endpoints
- Location based policies (online/offline/VPN)

ControlGuard allows security administrators to define policies that are automatically distributed to the endpoints.

Benefits

Intelligent and Granular Policies

ControlGuard Manager allows you to authorize specific devices, media and interfaces for particular PCs and users leveraging directory services. The policies are communicated to the endpoints in real-time and immediately enforced by the endpoint Agents. Administrators can grant temporary permissions for on-line and mobile users. Location-based policies are also possible, enabling different policies depending on whether the Agent is online, offline or using VPN.

Hot-Plug Support

ControlGuard monitors Plug-and-Play device drivers that are installed on the endpoint. Based on the policy of that endpoint, the Agent will report the newly installed device to the Management Server and enforce the appropriate access permissions.

Mobile Users Support

Mobile user endpoints are monitored and protected. The Agent continues to enforce the policy even when the endpoint is not connected to the network. It may apply different access permissions to interfaces (like wifi)
when the endpoint is off the network. Security administrators can temporarily grant mobile users access to a removable device that needs to be used.

Real-Time Notifications and Auditing

All I/O activities of the managed endpoints are notified in realtime to the Management Server and logged in a database. The events are displayed on the Management Console and communicated to security administrators in a variety of formats such as popup messages and email. The events are also made available to enterprise management systems in SNMP traps.

Advanced Security Agent

ControlGuard Agent is protected against attacks from processes, drivers, services and malicious code on your endpoint. It cannot be bypassed even by users who have administrative privileges.

Intelligent Distribution

ControlGuard Agents are distributed and installed seamlessly and efficiently across your network. The Agents can also be distributed by common enterprise software distribution tools such as Microsoft System Management Server.

Enterprise Management Systems Integration

ControlGuard is well integrated with enterprise management systems such as CA Enterprise Management solution, CA SIM/SOC system, IBM Tivoli and HP Openview. This enables administrators to leverage existing Management infrastructure and consolidate endpoint security events in unified logs and existing management consoles. eDevice records all endpoint I/O events in an SQL database. A flexible and intuitive reporting module allows administrators to submit customized queries and generate comprehensive reports on endpoint and end user activities.

Directory Integration

ControlGuard is well integrated with enterprise directory infrastructure such as Microsoft Active Directory and Novell eDirectory. This enables administrators to leverage the existing organizational logical layout of objects and groups. It also allows dynamic discovery of new objects added to the network, and optionally installing an agent on any new endpoint.

I/O devices

- Internal Modems Camcorders
- External Modems Digital Cameras
- PDAs Scanners
- Network Printers IPods
- Local Printers Optical Devices
- MP3 Players Smart Phones
- Tape Devices Floppy Disks
- Biotech Devices Mass Storage
- CD/DVDs, Burners SD Cards
- Memory Sticks Zip/Jazz
- LAN Adapters Drives

The events are also made available to enterprise management systems in SNMP traps.

ControlGuard Agents are distributed and installed seamlessly and efficiently across your network.