Secure Kernel

SecureOS utilizes a hardened kernel that protects servers from zero-day exploits, giving administrators the flexibility to deploy patches during planned maintenance windows. The kernel protects user space applications from memory corruption exploits such as buffer overflows and protects the kernel itself, preventing many privilege escalation exploits and other attacks.

Some of the protections offered by the secure kernel include:

- Enhanced ASLR (address space layout randomization) compared to stock kernels, which significantly raises the bar for exploits
- Hardened userland-to-kernel copies that protect kernel objects from being modified
- The KERNEXEC feature that prevents the kernel from executing userland code in the event of memory corruption
- Enhanced userland memory permissions that prevent injected code from being executable

These protections completely eliminate entire classes of attacks that can result in critical vulnerabilities in traditional operating systems and can greatly limit the severity of other classes of attacks. It is a proactive approach to security, unlike solutions that only protect from old, well-known vulnerabilities.

Minimal Attack Surface

Many attack vectors come from services running on the system that are not necessary for the appliance's operation. By removing unneeded utilities and services, SecureOS limits the possible attack vectors for the appliance, allowing the administrator to focus on just the services the system needs to provide without worrying about firewall rules and policies to block unwanted services.

Role-based Access

A key aspect of system security is ensuring only authorized users can change specific system settings. SecureOS uses advanced file access controls and privilege escalation lists to limit users' ability to modify the system. User abilities are based on roles to which they are assigned, thus limiting access.

While security is enhanced by the role-based access, users still have access to the best of Linux, including standard editors, the bash shell with scripting and command completion, job control, and a full set of system tools. In addition to standard Linux commands, a set of customer commands allows users to interact with the system with simple, intuitive commands for the most commonly needed operations.

Built-in DDoS Protection

Secure64 products are known for featuring flexible, built-in, and proprietary Distributed Denial of Service (DDoS protections. SecureOS implements these protections through low-level kernel modules that intercept network packets as soon as they arrive at the system and process them according to rules that the user defines. These rules allow administrators to:

- Rate-limit, temporarily blacklist, or drop packets from clients that exceed user defined thresholds
- Process traffic based upon any combination of network protocol, network port (for UDP and TCP), or DNS resource record type
- Process traffic on the basis of packets, overall bandwidth consumed, or both
- Combine rules using logical "or" and "and" operators

In addition to these user-configurable rules, SecureOS automatically blocks improperly formed packets without any user intervention required.

Full insight into what actions the system has taken is provided through a detailed defense report that the user can request, as well as through syslog alerts and SNMP traps. Rules and actions can be changed and reloaded on the running system, and started or stopped completely as necessary.

Because it uses a simple rule syntax and engages in the kernel itself, the SecureOS DDos mitigation offers simplicity and scalability to handle large scale attacks that is unmatched by competing solutions.