DATA SHEET

Symantec Critical System Protection

Hardening Internet of Things & Operational Technology

Cyber-physical systems have become a part of day-to-day lives, bringing automation and intelligence to the physical things around us. But new threats are also evolving quickly to target this rich and extremely vulnerable new landscape.

With every industry embedding computing and connectivity into a wide variety of devices—cars, jet engines, factory robots, medical equipment, and industrial programmable logic controllers—the consequences of security vulnerabilities are increasingly serious.

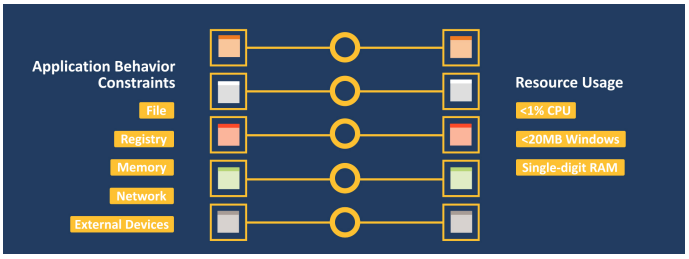
Complete IoT defense

Symantec Critical System Protection is a compact, behavioral security engine that provides comprehensive and in-depth security for your IoT devices. Based on the fixed-function and predictable nature of IoT devices, Critical System Protection can enact policies to define expected behavior of the system, allowing only non-malicious and hygienic operations.

Symantec secures more than 1 billion IoT devices.

Optimized for embedded systems and resource-constrained environments such as industrial control systems and operational technology, Critical System Protection can augment EOL/EOS and new operating systems without content, signature or any need for a cloud connection. It is qualified and interoperable with many automation vendors and robots today.

Whether your industrial control system is 20 years old or is brand-new machinery, Critical System Protection is compatible and securely protects it.

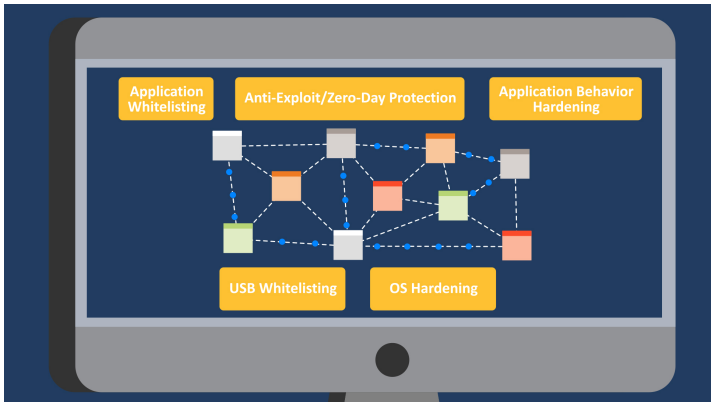


Critical System Protection features

Symantec Critical System Protection provides a host firewall, device and configuration control, file integrity monitoring, intrusion detection, operating system hardening, application whitelisting, automatic sandboxing, and many more features.

Compact size

A kernel-level protection engine, Critical System Protection requires about 20 MB RAM on a Windows® platform and uses less than 1 percent of a typical CPU.



Application containment

Using proprietary auto-isolation technology, Critical System Protection restricts applications to sandboxes that provide the least privilege access required on a per-application basis, without any code changes or functional limitations.

Application whitelisting

Critical System Protection provides the ability to whitelist applications within policies, allowing only named applications to run. In addition, you can specify policies for specific applications and application types. This ensures that even if an attacker obtains a compromised certificate, Critical System Protection will stop any attempt at an unapproved action. This highly granular control determines what any app can and can't do.

Intrusion detection

Critical System Protection policies provide thousands of prebuilt rules that monitor and harden the complete operating system and require minimal tuning. They monitor files, settings, events, logs, application behavior, and more, essentially covering the entire system. This ensures the immediate detection of any attempted malware actions.

Intrusion prevention

Critical System Protection prevents intrusions from causing damage. It has granular control over the entire operating system, blocking any attempts at unauthorized behavior and rendering attackers powerless.

Zero-day attack prevention

Zero-day exploits are security flaws that exist from the day of manufacturing, so they are already present when you purchase a device. Critical System Protection uses a prebuilt set of baseline policies to automatically confine known operating system components and restrict access only to required system resources. Additionally, the strategy of placing all unknown applications in least-privilege sandboxes prevents zero-day attacks from applications that are not known on the host machine.

Malware control in the network

Critical System Protection controls application access to networking. This is important because most malware tries to spread or download additional malware via the internet as soon as it is installed. Because Critical System Protection will not recognize malware, it will not provide network access.

Robust security

- **Auto sandboxing:** Jails processes, system, memory, OS, registry, Microsoft® PowerShell®, network, and other resources
- **Broad compatibility:** Supports any embedded/non-embedded/POSReady Windows OS since Windows NT, 2000, XP, 7, 8, 10, Linux®, and QNX®, managed or unmanaged mode
- **Complete protection:** Provides multistage zero-day prevention, and intrusion prevention system and intrusion detection system configurations
- **Automation Vendor Interoperability:** CSP is lightweight enough to easily protect, but not interfere with day-to-day operations of SCADA/DCS controllers, HMIs, and robot controllers.

More information

To learn more about Symantec Critical System Protection, visit **https://www.symantec.com/products/embedded-security**.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

SY-4015-IOT-CSP-Data-Sheet-D5