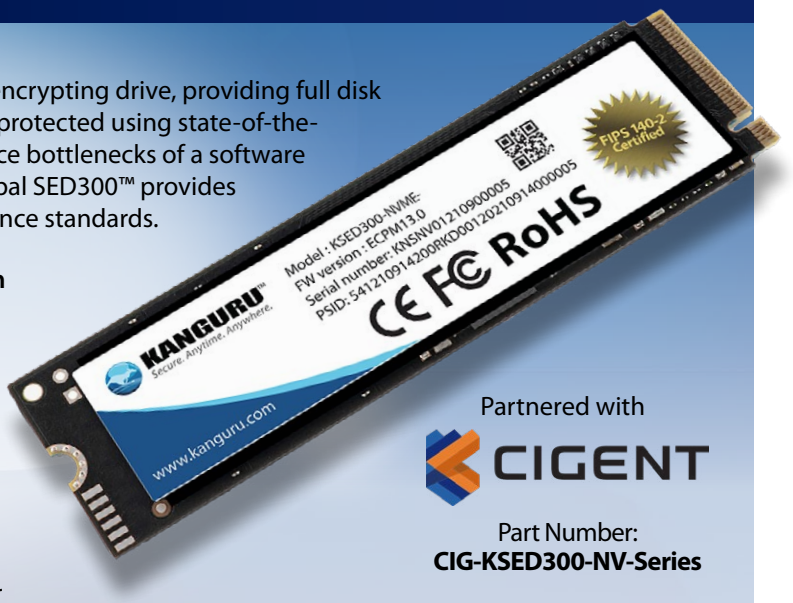
# Kanguru Defender® Opal SED300™

## FIPS 140-2 Certified, Self-Encrypting Internal NVMe SSD with Kanguru Data Defense™

The Kanguru Defender Opal SED300™ is a hardware-based self-encrypting drive, providing full disk data security at rest, keeping your operating system locked and protected using state-of-the-art, self-contained implementation, with none of the performance bottlenecks of a software based encryption platform. The FIPS 140-2 Certified Defender Opal SED300™ provides exceptional data security benefits to meet the toughest compliance standards.

- **Full Drive Hardware Encryption with Pre-Boot Authentication**
- **Comprehensive Dashboard for User-Friendly Experience**
- **Secure Firmware with Digital Signature**
- **Tamper-Resistant Epoxy Coating Cryptographic Controller and Flash Storage**




Partnered with CIGENT

Part Number:
**CIG-KSED300-NV-Series**

### Workforce Provisioning Tool

In addition, Kanguru's provisioning tools allow administrators to configure enforceable security policies for deployment to a global user workforce, which users must adhere to. Built on over 20 years of hardware security experience in the government certification world, users can be assured Kanguru is up to the task of keeping their organization's data assets safe.

**FIPS 140-2 Certified**

**TAA Compliant**

### BUNDLED with KANGURU DATA DEFENSE™

Kanguru has partnered with Cigent® to supply the Data Defense Security Suite. Cigent's advanced data protection and encryption technology are provided though a zero-trust security application to ensure only authorized users and processes have access to the data. Running Data Defense on the Kanguru SED300 provides Government-Certified Data at Rest and high levels of compliance with minimal interaction from the end user.

*Learn more about Data Defense Software Architecture - Page 2*

### FEATURES/BENEFITS

- FIPS 140-2 Certified, Level 2
- FIPS 197 Certified "Always On" 256-Bit AES Hardware Encryption
- TAA Compliant
- Internal NVMe PCIe M.2, 2280 NVMe
- Multi-Factor Authentication (MFA)
- High-Performance Solid State Drive Technology with Sequential Read up to 3000MB/s and Sequential Write up to 3000MB/s
- Includes Kanguru Data Defense™
- Available Capacities: 500G, 1T, 2T
- Zero-Trust Data Protection by Cigent®
- Verified Device Erasure: Ensures Every Block has Truly Been Wiped

### GOVERNMENT-CERTIFIED DATA AT REST PROTECTION

Self-Encrypting, Layered Protection. Defending Against All Data Attacks.

Government-Certified Data at Rest (DAR) protection that complies with FIPS, CC, and CSfC, protecting data on any O/S with full disk encryption, MFA, crypto erase, verified full drive erasure and on Windows OS makes data invisible, automatically responds to threats, and has immutable insider detection.

KANGURU™ Secure. Anytime. Anywhere. | CIGENT

FOR MORE INFORMATION, PLEASE CONTACT:

Kanguru Solutions
1-888-KANGURU
sales@kanguru.com
**www.kanguru.com**

© 2024 All Rights Reserved, Kanguru Solutions™ February 2024, Kanguru Defender SED300 NVMe - Cigent Sales Sheet

# Kanguru Defender® Opal SED300™

## FIPS 140-2 Certified, Self-Encrypting Internal NVMe SSD with Kanguru Data Defense™

## DATA DEFENSE SOFTWARE ARCHITECTURE

5

### Data Defense

Truly stop ransomware and data theft for all files on your endpoint devices with multi-factor authentication (MFA) for file access. Further make data invisible protected by non-recoverable keys on devices with secure storage. And keep data secure wherever it goes with file encryption and secure file sharing.

4

### Kanguru Defender SED300

- FIPS 140-2 Certified, AES 256-Bit Hardware-based Encryption
- Pre-Boot Authentication
- User-Friendly Dashboard (Opal Commander)
- Secure Firmware with Digital Signature
- Tamper-Resistant Epoxy Coating Cryptographic Controller and Flash Storage

3

### Cigent Windows Software

- Invisible Data
- MFA for File Access
- Verified Device Erasure
- Automated Threat Response
- Immutable Insider Detection

2

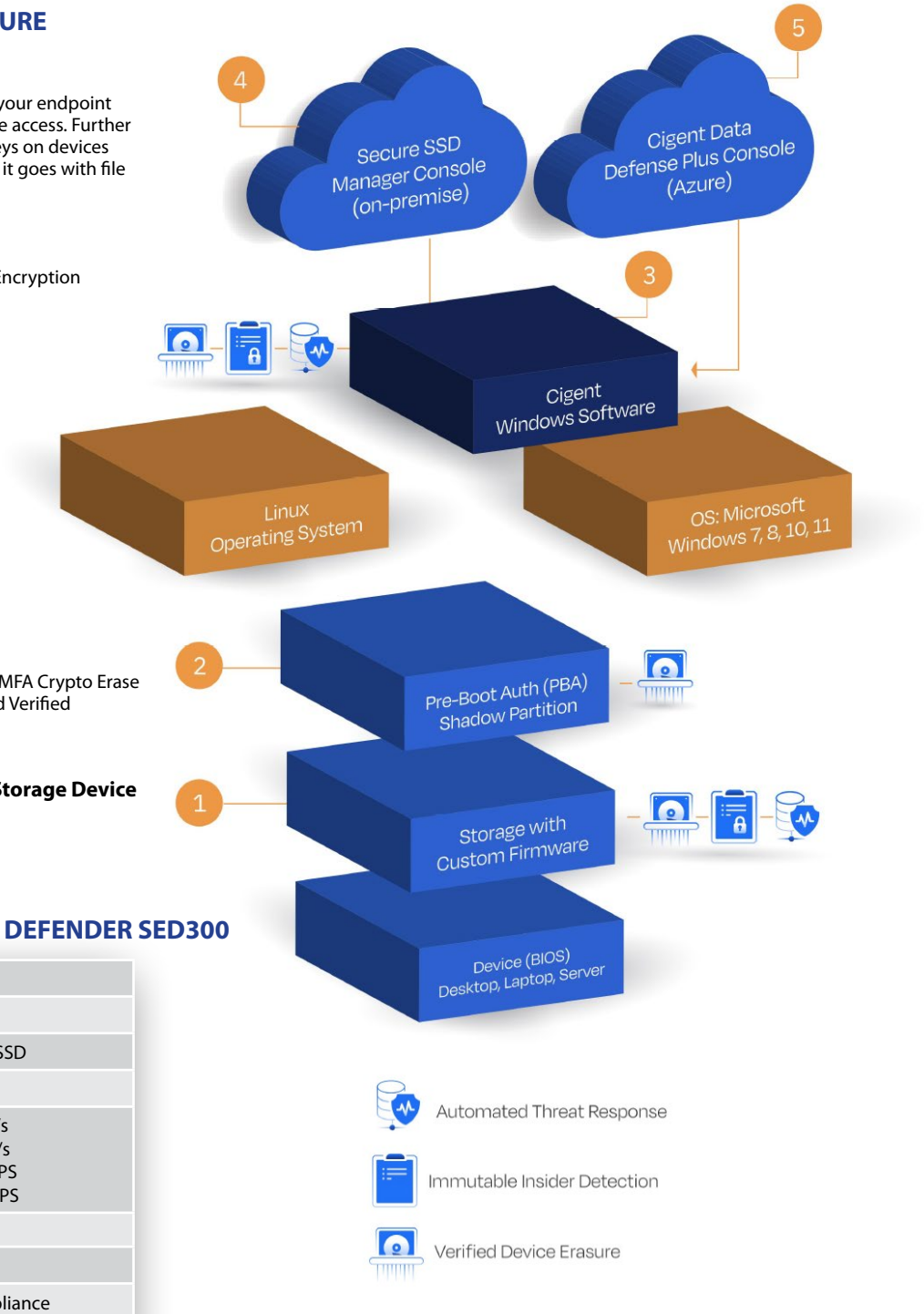
### Pre-Boot Auth (PBA) Shadow Partition

- OS agnostic Full Disk Encryption
- Pre-Boot auth with password, CAC/PIV, or both for MFA Crypto Erase
- Full NVMe Drive Erasure Verified by Firmware Based Verified Device Erasure

1

### Firmware-Level Capabilities Built-In to the Storage Device

- Automated Threat Response
- Verified Device Erasure
- Immutable Insider Detection




## TECH SPECIFICATIONS FOR KANGURU DEFENDER SED300

| | |
|---|---|
| **PART NUMBER** | CIG-KSED300-NV-Series |
| **CAPACITY** | 500G, 1T, 2T |
| **DEVICE TYPE** | Self-Encrypting Internal NVMe SSD |
| **FORM FACTOR** | M.2 2280 |
| **PERFORMANCE** | Sequential Read up to 3300MB/s<br>Sequential Write up to 3000MB/s<br>4K Random Read up to 700K IOPS<br>4K Random Write up to 680K IOPS |
| **PRODUCT WEIGHT** | 14 g |
| **WARRANTY** | 3 Years |
| **CERTIFICATIONS** | FIPS 140-2, FIPS 197, TAA Compliance |
| **COMPATIBILITY** | Windows and Linux |

KANGURU™ Secure. Anytime. Anywhere. | CIGENT


FOR MORE INFORMATION, PLEASE CONTACT:

Kanguru Solutions
1-888-KANGURU
sales@kanguru.com
**www.kanguru.com**


© 2024 All Rights Reserved, Kanguru Solutions™ February 2024, Kanguru Defender SED300 NVMe - Cigent Sales Sheet