Based on the Linux open source operating system to meet cloud, web and virtualised application access requirements, providing a secure and resilient browser-based and lightweight application environment.

**Paradox Variant descriptions**

**Paradox** – Flagship product version, fully featured except custom secure boot keys and custom boot screen animation.

**Paradox SE** – Mandates custom secure boot keys, 2FA with smartcards and ethernet only network connections.

**Paradox L** – Optimised for constrained and legacy hardware platforms.

**System Requirements**

**Minimum system requirements:**
- x64 Processor, 2GB RAM, 16GB Disk
  (For minimum spec machines Paradox L is recommended)

**Recommended system requirements:**
- Intel Core i3 or higher. Or AMD equivalent. 4GB of RAM or more
- 16GB of HDD disk space or more. Ideally SSD, SSD with NVMe is perfect
- TPM1.2 or 2.0 recommended but not mandatory

**Additional Requirements for Paradox SE:**
- UEFI Mandatory (no BIOS support)
- Hardware must support custom secure boot keys
- TPM 1.2 or 2.0 mandatory. Ideally a discreet (physical TPM) but Intel PTT TPMS are supported
- Yubikey or PIV2 smartcard for authentication

**Security Features**

**Device Identity & Health**
- Trusted Platform Module (TPM) as hardware root of trust. TPM based encryption key and system measurements protection
- Secure Boot with support for custom keys
- Measured Software Execution extends to application layer
- Remote Attestation provides device identity management and controlled access to protected services
- Cryptographically signed updates and device policies

**Device Protection**
- Read-only system image
- Built-in (compile time) user and application models prevent unauthorised privilege escalation
- Encrypted configuration partition for user preferences
- Optional TPM-backed encrypted data partition
- Compile-time source minimisation for reduced attack surface
- AppArmor profiles for all in built and Becrypt supplied apps
- Fine-grained USB device control

**The Security Principles of Paradox**

- Maintain trust in the identity and integrity of a device through its lifetime
- Ensure only authorised Apps and Updates can be installed
- Ensure confidentiality of services and data of authorised users

**Network Protection & Monitoring**
- 802.1x for WiFi connections
- FileBeat integration for runtime integrity monitoring and real-time alerting to ELK base SOCs
- Global network proxies

**Authentication**
- Two-factor authentication and single sign-on support
- Azure AD authentication integration
- Okta and OpenAM OAuth based authentication integration
- Web App based SSO with policy control
- NHS smartcard integration

**Standard Client Application Support**
Examples of typically installed and configured applications include:
- Chrome, Firefox
- VMware, Citrix, Amazon Workspaces and multiple RDP clients
- Cisco and OpenSwan VPN Clients
- Libra Office
- Rocket Chat

**Standard Configuration Options**
- Low Touch automated deployment configuration
- KIOSK mode with configurable T&Cs page
- Application auto-launching based on configurable conditions
- Centralised printer configuration
- Smartcard pin reset application
- Managed browser extensions
- Guest mode
- Samba shares for mounting network drives via BEM policy settings
- Browser bookmarks
- Audio settings
- Display settings
- Keyboard & mouse settings
- Accessibility settings
- Language settings
- WiFi settings
- Application settings

#becrypt
Smart Card Support
Paradox supports PIV compliant smartcards for 2FA to the device. FIPS 201 (Federal Information Processing Standard Publication 201) is a United States federal government standard (NIST) that specifies Personal Identity Verification (PIV). It is now a commonly adopted standard across many of the major smartcard vendors such as Yubico, HID, Gemalto and Entrust. The Yubikey 5 range by Yubico is widely used because it is a USB form factor that doesn’t require an additional Smartcard Reader device. Becrypt can also provide Yubikey programming and recovery tools integrated to the solution with certificate lifecycle management.

System Customisation
Becrypt can offer customer specific customisations to Paradox for specialist applications or personalisations that are not to be included as standard functions within the base. Additionally the base Paradox Linux OS may not contain drivers for some unusual or closed source devices, or VPNs. For these circumstances we use a type of Union file system called OverlayFS to make additions to the file system in a way that can maintain our boot time integrity checks. There are two types of Overlay, System Level Extension (SLEs) for VPNs and Drivers and Platform Customisation Layers (PCLs) for personalisations. Both can be provided by Becrypt on request and are uploaded alongside OS updates to BEM (Becrypt Enterprise Manager).

Security Architecture Overview

Secure Boot
Paradox implements a standard secure boot process for bootloader validation, firmware integrity validation and validation of initial operating system components. Paradox SE allows the customer to sign their specific Paradox SE build providing assurance that only their own version of Paradox will boot on their hardware.

Measured Execution
Measured execution extends trust from the initial Secure Boot process. Paradox implements a scheme referred to as “dm-verity” (Device Mapper Verity), which validates system reads at a block device level using a cryptographic hash tree. For every block (typically 4k), there is a SHA256 hash. The hash values are stored in a tree of pages, only the top-level “root” hash must be trusted to verify the rest of the tree. For Paradox, the top-level hash is protected by the Secure Boot process, ensuring a continuation of trust from the early boot process through all system files including 3rd-party drivers.

Policy and Application Signing
Paradox system updates involves replacing the entire system image using a process which is secure, safe and can be mandated and automated. A Public Key Infrastructure (PKI) based scheme is used to cryptographically sign system updates, applications and policies delivered via an encrypted and authenticated client-server communication channel with the Becrypt Enterprise Manager (BEM) server. This methodology ensures that:

- Only applications specifically packaged and signed for the system image can run on the Paradox client, preventing application side loading or the injection of unapproved applications. This process extends the trust boundary from the measured execution process.
- Only the specific updates and policies configured within the BEM server can be applied to the Paradox clients, preventing malicious attempts to subvert the endpoint.

Read-only System Image
Paradox uses a non-persistent system partition to prevent sensitive data from being written to persistent storage on the device, as well as providing significant mitigation against malware persistence.

Encrypted Data and User Profiles
Paradox is typically required to store some data locally such as the Device Policy and Certificates. To protect this information from offline attacks, Paradox encrypts the Configuration Data Partition using AES and a 256 bit key (DEK) which is itself encrypted by a Key Encryption Key stored in the TPM and sealed by the TPM on the local device.
Two Factor Authentication
Paradox integrates with a number of the most common smartcards available today. The system will also perform a CRL check against the certificate on every login to ensure it has not been centrally revoked.

External Interface Protection
The Paradox centrally managed device policy can define strict white-lists of allowed peripheral devices at a device manufacturer, model or instance level (PID\VID).

802.1X and 802.1AE
Paradox supports both variants of the IEEE standard for port-based Network Access Control. MACSEC (802.1AE) encrypts network packets from the device to the local switch.

Integration with SIEM systems
Paradox can be configured to output detailed system logs directly to SIEM systems through Syslog or the output can be distributed to the SIEM system from the Becrypt Enterprise Manager Server. Paradox supports RELP (Reliable Event Logging Protocol).

Memory wipe
Paradox implements memory erasure functionality that runs automatically on device shutdown, combating data retention exploits.

Management
Paradox is centrally managed by the Becrypt Enterprise Manager (BEM), a mobile device management system. BEM is scalable from a single server to fully resilient multiple servers with split roles and an SQL clustered back end for EUD deployments in the tens of thousands. BEM can also be configured with secure multi-tenancy for cloud based SaaS deployments.

To install and run BEM Web, you will need:

Servers
- For the BEM Web Server, a machine running Windows 2012 or 2016 with IIS and .NET framework
- For the BEM Web Database, SQL Server 2012, 2014 or 2016
Why
#becrypt

With a heritage of creating National Cyber Security Centre certified products, Becrypt is a trusted provider of endpoint cybersecurity software solutions. Becrypt helps the most security conscious organisations to protect their customer, employee and intellectual property data. It has an established client base which includes governments (central and defence), wider public sector, critical national infrastructure organisations and SMEs.

As one of the early pioneers in disk encryption software to today being first to market with a unique desktop operating system, Becrypt continues to bring innovation to endpoint cyber security technology. A recognised cyber security supplier to the UK government, Becrypt's software also meets other internationally accredited security standards. Through its extensive domain and technical expertise, Becrypt helps organisations optimise the use of new cyber security technologies and its flagship security solution Paradox delivers a highly secure platform for the modern age.

Paradox is available as a cloud hosted managed service:

Paradox Edge provides a desktop-as-a-service option for Paradox customers. With the Paradox management platform pre-built and hosted within a secure cloud environment, organisations can rapidly deploy secure endpoints outsourcing patch management and security monitoring to reduce internal IT resource requirements, and leverage scale for ongoing cost reduction.

Get in Touch
If you would like to find out more about Paradox please contact us on

0845 838 2080
info@becrypt.com

View us on: becrypt.com
Follow us on: @Becrypt
Support us on: Becrypt