#becrypt

High Assurance Endpoints

Secure Thin Clients for elevated threat environments

A Becrypt Whitepaper

Introduction

Security features and functionality offered by the popular desktop operating systems have improved considerably over the last decade. Development standards are more rigorous, hardware support for software integrity and isolation is now pervasive, and once specialist endpoint protection capabilities are now commodity. If organisations correctly configure and manage standard desktop environments, they are today well protected from the commodity attacks that represent the vast majority of cyber-criminal activity.

But for some environments within some organisations, even these improved standards are insufficient. Operating systems and applications will always have vulnerabilities that may be successfully targeted where there is the will and the expertise to do so. Organisations that are high value targets for well-funded organised cyber criminals, such as those within government and the Critical National Infrastructure, face the need to protect against elevated threats and targeted attack, while maintaining competitive advantage through increased adoption of evolving technologies.

Examples of assets that face elevated threats include:

- Management or administrative endpoints (Privileged Access Workstations);
- Devices connecting to government classified networks;
- Devices remotely accessing critical systems;
- Un-managed endpoints accessing critical systems (e.g. Supply Chain)

Within the UK, the National Cyber Security Centre (NCSC) has lead a number of initiatives to develop the standards used by the High Assurance products and services that are designed specifically to protect against elevated threats. One area to benefit from this work is endpoint security, where architectures have been defined and deployed across government and the CNI to better protect both endpoint devices and the online services they access.

Emerging High Assurance technologies combine improved threat protection, detection and isolation for defence in depth architectures to support improved organisational cyber resilience.

High Assurance defined

The NCSC High Assurance principles stress that for protecting against elevated threats, products should be sourced from trusted suppliers with proven high threat domain knowledge, that adhere to accepted good practice processes and standards.

A key factor that separates High Assurance products from much of the broader cyber security and technology market, is the inclusion of clearly defined security functionality supported by systematic, independent and evidence-based assessment, ensuring that products always operate as intended, and remain in a trusted state.

The move to Secure Thin Clients

The increased use of public, private and hybrid cloud services has allowed endpoint platforms to be lighter-weight, providing the potential for a significantly reduced attack surface compared to common desktop operating systems. However, a key factor behind the move to Thin (or thinner) clients is that the protection of Data at Rest (DAR) on commodity endpoint hardware has become increasingly difficult in the face of evolving threat.

As a result, many security conscious organisations have moved to architectures with multiple trust domains, in which core systems have a higher level of trust than distributed endpoints. Within such architectures, data typically resides in better protected environments behind High Assurance gateways, removing or reducing the endpoint DAR challenge with a Thin Client model.

Historically, the deployment of Thin Clients has often reduced focus on endpoint security, however, within elevated threat environments, the security properties of the client device still need to be considered, as anything that is acting as a Thin or even Zero Client endpoint, is executing code that is subject to vulnerability or tampering.

Data at rest may still be a consideration for Thin Clients, as many devices may retain data in the form of user or application settings. As a result, Secure Thin Clients should implement low-level encryption utilising hardware-backed key storage (i.e. Trusted Platform Module) for local data protection.

Device Health Measurements

Targeting a Thin Client or Zero Client device is a more specialist activity than standard desktop environments, but many such devices have far less scrutiny of their codebase, fewer inherent security controls, and once compromised, any exploit may be far more challenging to detect.

As a minimum, Secure Thin Client devices should support secure boot, to protect both firmware and boot process integrity, however, validating the integrity of the entire system becomes relevant for elevated threat environments. A research project initiated by NCSC referred to as CloudClient, demonstrated how on a Thin Client platform, device health measurements initiated within secure boot may be extended to measure and validate the integrity of all endpoint software. The *Measured Execution* architecture provides confidence in the health of the device when powered up, using cryptographic measurements of all software components based on a hardware root of trust.

This architecture is viable for Thin Client devices, given their relatively small software image. Limited image size also allows the operating system to be mounted as read-only, providing additional protection against system modification. This non-persistence combined with Measured Execution of all software components provides significant advantage over the more limited Health Measurement functionality of general-purpose operating systems.

Device Authentication

NCSC End User Device principles stress the importance of 'device to service' authentication to complement user authentication. Additionally, the increased focus on Zero Trust Architectures as the preferred model for cloud environments, emphasises the need to combine device identity and device health signals as part of authentication and authorisation processes that control access to protected services.

Secure Thin Client devices should use a hardware root of trust, such as a TPM, to form the basis of strong device identity, as well as Measured Execution to validate device health. Standards-based protocols, such as a Remote Attestation protocol, may then be used to complement service access control policies.

Threat Isolation

Enterprise management platforms and directory services are high-value targets for adversaries, given the concentration of information and privilege they represent. Ideally, within a multi-domain architecture, a degree of separation will exist between management platforms, and managed endpoints, through the use of cross domain gateways or web application firewalls. Strictly enforced isolation is difficult to achieve for typical endpoints, given the complexity of client and management server protocols. Within an appropriately designed and configured Secure Thin Client environment, simpler management traffic protocols may be routed via gateways for network isolation, and network packet validation, significantly reducing the opportunity for compromise of core networks by remote systems.

Summary

Secure Thin Clients deployed in elevated threat environments will typically include additional security functionality to that outlined above, including privileged escalation control, application and policy enforcement, simplified patch management and extensive security monitoring.

However, the central High Assurance product requirements of operating as intended and remaining in a known good state, can be met through robust device health measurements, and device identity management and management domain isolation. A number of UK government departments have now successfully deployed Secure Thin Client environments to enhance cyber resilience, resulting in technologies and standards now available to the wider Critical National Infrastructure.

About Becrypt

Becrypt is an agile London-based UK SME with 20 years cyber security expertise, established through the development and delivery of cloud, mobile and endpoint platforms. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services - from funded research, to commercially available products and flexible managed services. Becrypt have worked with UK Government and platform vendors to pioneer and deploy device health identity management products and services, based on the NCSC CloudClient Architecture.

https://www.becrypt.com/uk/products/paradox/

Becrypt Ltd
Artillery House
11-19 Artillery Row
London SW1P 1RT
UK Company Number 4328430
Tel: 0845 838 2050