ENDPOINT PRIVILEGE MANAGEMENT SERVICE

THE PRIVILEGE CHALLENGE

Protection against external threats (e.g. anti-malware) can reduce cyber risk, but it doesn't address security breaches resulting from user-related activity within the organisation.

As perimeter security becomes stronger, end user devices are heavily targeted by threat actors using social engineering techniques via email phishing. If a user has local admin rights when they open an infected attachment or link, the payload can execute using their privileges, giving the hacker control of the machine by silently installing backdoors and reconfiguring (or disabling) other security controls. Even when an external threat actor is not involved, elevated users privileges poses a high level of risk - either from a malicious user or just from human error when they are no users restrictions.

Endpoint privilege management (EPM) prevents users from gaining access to software or functionality they don't actually require. EPM follows the principle of least privilege to minimise the attack surface, by eliminating unnecessary administrator accounts.

Zero Trust Security and EPM

The zero trust security model states "never trust, always verify." This approach relevant as technologies like the cloud, virtualisation and IoT have blurred the idea of a traditional firewalled network. These risks are further increased in an environment with users who work from home and use their own devices. EPM technology helps organisations to achieve zero trust goals by enforcing adaptive, least privilege control for all access.

Endpoint Privilege Management Service

CSI helps clients to deploy, manage, optimise and leverage the right technology to mitigate the risk linked to uncontrolled user permissions and to achieve zero trust security goals. This service is supported by Privilege Management products and services from BeyondTrust.

BENEFITS OF EPM WITH CSI

1. **Remove administrator rights** without compromising productivity.
2. **Assign necessary privileges to applications** using their standard account but invisible to the end-user when app launches.
3. **Ensure application control** by configuring policies to whitelist approved apps or block unauthorised applications (installers and scripts).
4. **Ease of deployment** using CSI's predefined rules and playbooks. Pre-configured scenarios make it possible to cover the various needs of your users and reduce deployment costs.

GROW SAVE INNOVATE PROTECT

Endpoint Privilege Management (EPM) Service

SERVICE DELIVERABLES	
QS Policy Configuration	New Application Definitions Add/modify custom discovered applications that are being used within environment
Trusted Application Protection (TAP)	TAP enhances security against malware—including ransomware--and phishing attacks by adding context that stops attack chain tools that may exploit commonly used and legitimate applications. allowing restriction of common attack chain tools, such as PowerShell and Wscript that are spawned from commonly used applications, such as browsers or document handlers (Word, PowerPoint, Excel)
Exception Handling	Adds, remove changes - to allow users to request access to an application when it has been blocked or requires authorisation from the support team
Reporting & Configuration Reporting Analytics	Identification/Triage of Windows Security events, Discover shadow IT, Applications launched
File Integrity Monitoring	Custom Concepts, monitors and detects file changes that could be indicative of a cyberattack
ServiceNow integration	Can allow for users to create a ticket in ServiceNow as part of the application request
Virus Total Integration	Integrate reported events with Virus Total, to provide reputational information on applications that are being run within the customers environment

SERVICE ELEMENTS SUPPORTED	
Service Desk – 24x7 for P1 incidents	✓
Incident Management	✓
Security Operations Support	✓
Cadence Calls *	Monthly
EPM Reports	Monthly
Service Level Agreement	✓
Service Delivery Manager	Optional
* A remote meeting with a SOC analyst to present findings and analysis of the previous month's activity. Cadence calls will typically include discussion of threat events, devices added, license count review and agent update rollouts.	

Additional Cyber Resilience Services from CSI

- Managed Web Filtering
- Managed Endpoint Protection
- Managed Phishing Defence
- Managed Detection and Response
- Vulnerability Assessment
- Extended Detection and Response

CSI Ltd Head Office

CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

CONTACT
+44 (0) 800 1088301
info@csiltd.co.uk
www.csiltd.co.uk