MANAGED ACCESS AND AUTHENTICATION

KEY SERVICE COMPONENTS

Device Access Management

- Ongoing management of device profiling policies adding visibility into the makes, models, versions and operating systems of devices on the network
- Custom device whitelist and blacklist creation and ongoing maintenance under change-control processes
- Ongoing policy management rerouting non-authorised devices into guest VLANs
- Where supported, federation of VPN mechanisms, device-access controls and next-generation firewalls allowing seamless user-identity pass through (requires User ID aware VPN capabilities on the firewall)
- Host checking functionality that ensures connecting devices comply with defined requirements

User Access Management

- Definition of access policies for authentication and authorisation to enforce user compliance with corporate policies and industry regulations
- Multiple profiles for different access methods for each user or user-group with their own access policy
- Layered profiles allowing access to different resources for users depending on user-type (employee or 3rd party), authentication mechanism, location or user-privilege status
- Where supported, application of security-contro policies enforcing Next-Generation Firewall capabilities such as Intrusion Detection, URL or Web Content filtering on a user-specific basis (requires user ID awareness on the firewall)

Multi-Factor Authentication Management

- Integration and ongoing management of a choice of Multi-Factor Authentication mechanisms
- Flexible single sign-on support allowing authenticated users automatic sign-on to back-end applications and services
- Ongoing management of RADIUS client integrations
- Management of self-serve platforms allowing users to regenerate locked AD accounts or forgotten passwords

SERVICE DESCRIPTION

With information security one of the key challenges is understanding which users are on the network, what devices are in use, where these devices are located and what their security posture is. A number of high profile attacks have shown that hackers target unprotected access & unpatched devices to become part of the network. Threat actors then use these devices as a springboard into the rest of the network. The questions that need to be answered are therefore who is on the network right now and are those users on the network permitted to access the data they are working with? Do the devices accessing the network represent a threat?

Maintaining visibility and control over the users and devices accessing hosted or on-premise infrastructure, discrete applications and privileged data is one of the cornerstones of cyber security. Organisation's requirements are thus:-

- to identify who the user is and verify their privileges to the data they are accessing
- to verify devices provisioned by the organisation are secure against spyware and not jail-broken
- to verify that data being accessed is contained within a private, secure environment on devices not provisioned by the organisation

Our Managed Access & Authentication service is designed to alleviate the burden of ongoing management of device-access, user-access, privileged-access and multifactor-access controls whether in use as point solutions or whether combined to provide a layer-based risk management strategy.

The service's aim is to increase visibility into the identity of the users and devices requesting access to an organisation's assets. The service further monitors the behaviour of the users and devices thereby enhancing the organisation's protection against breach and assists the organisations security team by controlling, via device and service policies, which user's and devices should be allowed to access the organisation's assets and data.

KEY BENEFITS & DELIVERABLES

- **Increased Visibility:** Awareness of users & devices accessing corporate resources
- Incident Alert: Identification and notification of issues related to device availability
- **Proactive Monitoring:** 24x7x365 pro-active monitoring of key device metrics
- **Help Desk Support:** 24x7x365 help-desk support to remediate issues in normal operation of scoped appliances
- **Patching, Updates & Upgrades:** Where performed remotely, full deployment of patches, updates and upgrades to the device specific software
- **Change Assessment:** Assessment of risk to business-as-usual by requested changes
- **Change Management**:
  a) In coordination with change processes and change windows specific to the customer business and,
  b) Assisting with the creation and implementation of changes

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com

SECDATA.COM

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com