MANAGED NEXT-GENERATION FIREWALLS

KEY BENEFITS & DELIVERABLES

- **Enhanced security:** Threat Prevention additions (Intrusion Detection/Prevention, Anti-Malware, Application Control, User Identity Awareness) assists prevention of malicious user- & application behaviour.
- **Reduced risk:** Intercepting and blocking at the application layer prevents breaches and avoids regulatory compliance violation.
- **Incident Alert:** Identification and notification of issues related to device availability
- **Proactive Monitoring:** Subject to contract, 24x7x365 proactive monitoring of key device metrics
- **Service-desk Support:** Subject to contract, 24x7x365 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 and management:**
  a) In coordination with change processes and change windows specific to the customer business and,
  b) Assistance with the creation and implementation of risk-assessed changes
- **Business continuity:** Weekly backups of device policies and hardware configuration

SERVICE DESCRIPTION

Considering that every company that has been breached has had firewalls in place indicates that traditional firewalls, often the first line of defence for a business, are incapable of combatting modern threats. The current dynamic threat landscape means firewalls now need to be application aware, inspect traffic content, intercept malware and offer intrusion detection/prevention capabilities.

Next-generation firewalls offer the additional layers of inspection and detection required to increase an organisation's resilience to an attack. These layers may comprise of:

- Anti-Virus/Anti-Malware
- Anti-Bot
- Application Visibility & Control
- User Identity Awareness
- Intrusion Prevention
- Web URL Filtering
- Web Content Filtering

While these additional features offer significantly better protection, they do create additional burden on resource-starved IT staff and add device management complexity to ensure they remain effective and deliver return on investment.

Our fully managed Next Generation Firewall service removes the complexity of continuous rule-base management allowing in-house IT teams to focus on the tasks the business needs.

The service also increases visibility into user behaviour, network- and application-layer traffic through Intrusion Detection & Prevention, extends protection against web-based attacks using Web Content and URL filtering and reduces the risk of malware infection through virus, malware and bot detection.

KEY SERVICE COMPONENTS

Managed Firewall

- Ongoing rule-base configuration mitigating against new & emerging threats
- Unlimited Site-to-Site VPN creation and configuration (device dependant)
- Site-to-Site VPN tunnel monitoring and performance-testing (subject to dedicated AffinitySECURE system being in place and device dependant)
- ISP failure monitoring for internet-facing gateways subject to access being enabled by the ISP

Managed Intrusion Detection & Prevention

- Initial application of one baseline policy to each device followed by finer tuning for a period of 30 days working with the customer to configure policies according to required actions and severity
- Ongoing fine-tuning of IDS/IPS policies and signatures as requested by the customer
- Signature updates deployed according to agreed customer schedule.

Managed Threat Prevention

- Anti-Virus, Anti-Malware & Anti-Bot signature database updates implemented as released by the vendor
- Emergency implementation of 'hotpatch' signatures, as per agreed BAU change process
- Maintenance of Threat Prevention exclusion lists

Managed Application Control & Identity Awareness

- Policy creation and management to identify, allow, block or limit usage of social networks, applications and features within applications
- Change management of user access to company resources and Internet applications
- Custom policy creation with centralised policy management

Managed URL- & Web Content Filtering

- IP address/domain signature database updates as released by the vendor
- Custom Proxy Auto-Config (PAC) and Whitelist/ Blacklist creation and maintenance (subject to scoping documents)
- Web content security policy and rule-base management

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