MANAGED NEXT-GENERATION ENDPOINT SECURITY

KEY BENEFITS & DELIVERABLES

- **Enhanced endpoint security:** Non-signature based malware detection profiles malicious behaviour without relying on lists of white-listed or blacklisted executables
- **Reduced risk:** Intercepting and blocking previously unknown malware 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:** 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) Assistance with the creation and implementation of changes
- **Business continuity:** Weekly backups of device policies and hardware configuration

SERVICE DESCRIPTION

With the latest cybersecurity attacks and breaches it has become evident that the endpoint has become the latest battleground. Desktops and mobile devices face increasingly complex and numerous attacks by malicious software (malware) authors attempting to gain an entry point into the network to exfiltrate data or, through ransomware, for financial benefit. Attackers are not only attacking vulnerabilities in endpoints but are exploiting features within well-known applications. Recent research from SensePost has shown that exploiting features within common Microsoft Office applications have a close to 100% success rate.

Legacy antivirus products, though having evolved through the addition of host intrusion detection and/or behavioural heuristic analysis, still rely heavily on detecting malicious files by matching the file against a database of known bad signatures which leaves a considerable window of opportunity for ‘zero-day’ malware to take hold and proliferate across the network if there is no signature for it.

Next-Generation anti-malware defences have entered the marketplace to work in tandem with, or replace, signature-based detection . Known variously as sandboxing, containerisation, threat emulation and threat extraction these products seek to fill in the gap between known-bad and known-good by intercepting the execution of the file, profiling the file’s metrics and intended actions and then preventing the file’s execution based on the probability that it will perform malicious actions.

Our fully managed Next Generation Endpoint Security service removes the complexity of continuous rule-base management allowing in-house IT teams to focus on the tasks the business needs. By monitoring and managing the endpoint-management server or appliance, SecureData’s service offers businesses peace of mind that their endpoints are under constant supervision and have fully updated malware detection mechanisms in place. The service also increases visibility into user behaviour and extends protection against email attachment and web-based attacks to reduce the risk of infection by zero-day

KEY SERVICE COMPONENTS

- Initial application of ‘detect-only’ policies to the endpoint management server or appliance followed by finer tuning for a period of 30 days working with the customer to configure policies according to required actions and severity
- Creation of initial whitelists and blacklists to allow or deny execution of files
- Ongoing fine-tuning of endpoint- or user-based policies and signatures on a monthly basis
- Creation of additional policies or amending existing policies as part of the business’s change control process
- Signature updates deployed according to agreed customer schedule. (Due to updates being automated the agreed schedule should include customer resource allocation to test critical applications)
- Reports detailing the top 50 events detected, along with key related metrics including, for example: Top malware blocked, Top malware detected, Top infected endpoints

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