BORDERPOINT PROTECTIVE MONITORING

A dedicated managed cyber security service that monitors your IT infrastructure, detects vulnerabilities and threats, intrusion attempts, security anomalies, badly configured applications and unauthorised user activities.

Systems driven alerts are investigated by CSA security analysts who escalate identified threats and provide guidance on remedial actions required to mitigate those threats.

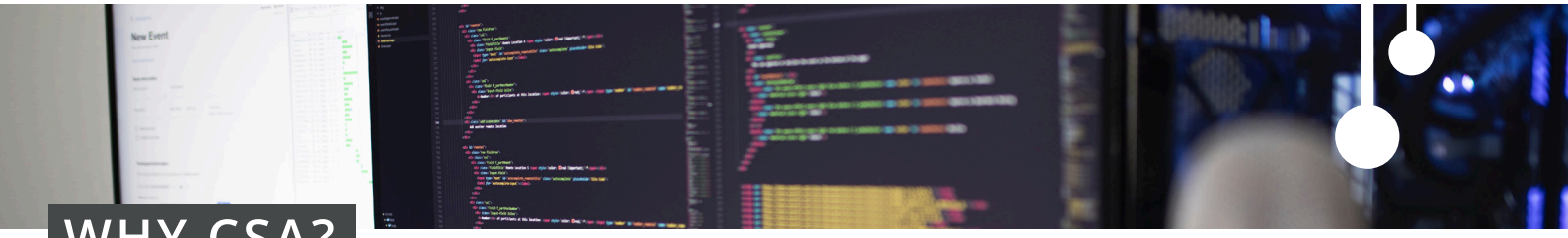
THE ISSUE

'Investigating unreliable alerts wastes two-thirds of staff time while actual breaches go undetected an average of 146 days.You must be on constant lookout for security threats lurking in your network traffic – managed detection and response gives you actionable insight when it counts.'

Gartner's 2018 Intrusion Detection and Prevention Systems Magic Quadrant

Cyber criminals are getting more sophisticated with attackers conducting in-depth reconnaissance to find vulnerabilities before launching their attack. Firewalls, anti-virus and patching are often not resilient enough to protect your IT from being compromised. As illustrated above, often once a breach occurs cyber criminals have access to a network for long periods of time without the breach being discovered.

To combat this increased level of threat larger companies, have been deploying managed detection and response capabilities. This is achieved by either operating an in-house SOC (security operations centre) which is expensive to set up and operate or by commissioning a managed service like BORDERPOINT which has been designed and built by CSA to offer an affordable solution to businesses of all sizes.



WHY CSA?

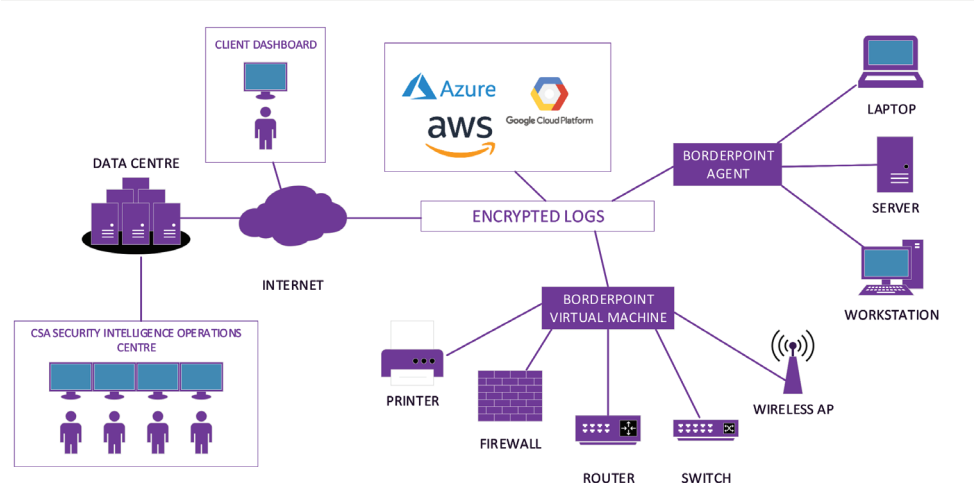
CSA's UK based SOC is operated by experienced cyber security analysts overseen by James Griffiths and Dave Woodfine; both of whom have extensive experience in setting up and operating SOC monitoring services for large corporate organisations including the MOD and the Bank of England.

The BORDERPOINT service has been designed and built by CSA based on experience gathered working for organisations where the highest standards of security are demanded.

INCIDENT DETECTION & RESPONSE

Activity and Security Analysis

BORDERPOINT collects system and security data from your IT devices (on-site or cloud) and then forwards it securely to CSA. This data is indexed and analysed against bespoke rule-sets and a threat intelligence database to identify potential threats, behavioural anomalies and to detect intrusions.



Intrusion Detection

BORDERPOINT provides real-time scanning that looks for cyber threats and suspicious anomalies at the host level. This enables the CSA Analyst to investigate and respond to advanced threats and attacks against your IT. BORDERPOINT can uncover more complex exploit processes, used to bypass Anti-Virus systems, through the integration of the CSA Threat Intelligence database to identify indicators of compromise.

Flexible Incident Response

BORDERPOINT can provide an optional automated active response service that can be used to block a network attack, stop a malicious process or quarantine a specific user or file. This tailored service will be developed to meet an organisations individual automated response requirement.

SECURITY HEALTH & MONITORING

Software Audit

BORDERPOINT will conduct a full software audit every 12 hours on each monitored device. This inventory check will provide a detailed list of all software installed including patching status. This near real-time service will provide assurance that you understand what software has been legitimately installed on your devices and will be used to inform the BORDERPOINT vulnerability assessment service.

Vulnerability Assessment

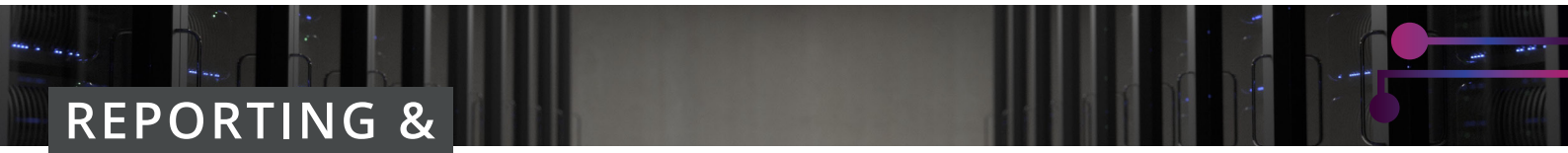
The automated vulnerability assessment feature helps to find the weak spots in your IT. BORDERPOINT uses the output from the software audit to provide a continual vulnerability assessment for each monitored device. BORDERPOINT achieves this by comparing the results against the latest CVE (Critical Vulnerability and Exposure) database of known vulnerabilities to identify weaknesses that need be addressed.

File Integrity Monitoring

BORDERPOINT monitors selected files to identify changes in content, permissions and attributes of the files that are important to an organisation such as files that a hacker or malware would target or those containing sensitive financial information or personal data in HR records. BORDERPOINT will generate an alert if it detects that a file has been changed or modified and can identify the user(s) involved. File Integrity Monitoring will also provide inputs into the BORDERPOINT regulatory compliance service.

Security Configuration Assessment

BORDERPOINT monitors operating system and application configuration settings to identify where areas of potential attack can be reduced. BORDERPOINT will detect and alert against common system misconfigurations that may be present on monitored devices. Each device will have a security configuration assessment score that will be available through the user dashboard. These scores can be benchmarked and tailored against an organisations security policy.



REPORTING & COMPLIANCE

Regulatory Compliance

BORDERPOINT alerts and reports against compliance with some of the mandatory security controls for various industry standards and regulations. BORDERPOINT is configured and mapped to the technical controls of the PCI DSS (Payment Card Industry Data Security Standard), GDPR, NIST and HIPPA. Additionally CSA are working on the technical controls for the Cyber Essentials accreditation and ISO 27001.

User Dashboards

BORDERPOINT has been designed with its own unique user accessible dashboard. Each dashboard is pre-configured to display the core features of BORDERPOINT and can be tailored to meet the individual needs and requirements of each client. This single interface provides a real-time view of your monitored IT infrastructure that some clients will appreciate while others will just want to be alerted when there is a real issue that has been identified as part of the CSA managed service.

FAST & SIMPLE DEPLOYMENT

BORDERPOINT provides a fast and easy deployment straight onto your IT. For windows, BORDERPOINT can be automatically deployed through group policy deployment or the CSA installer for singular hosts. For Linux and MacOSX a simple installer script is provided. As part of the installation process our deployed agent will register with the BORDERPOINT management server ensuring the BORDERPOINT service is up and running straight away without the need for license keys or software downloads.

For log sources where the BORDERPOINT endpoint agent can't be installed (firewalls, routers, switches) the BORDERPOINT on-premise pre-configured Virtual Machine can be deployed onto your infrastructure. Once the Virtual machine is up
and running then any remaining devices will also be monitored. All you need to do is to install and power on and let BORDERPOINT do the rest.

TECHNICAL SPECIFICATION

AIX 5,6 and 7
Amazon Linux, Amazon Linux 2
CentOS 5,6 and 7
Debian 7 and above
Fedora 22 or above
HP-UX 11.31
MacOSX Sierra or above
OpenSUSE
Oracle Linux 5,6 and 7
Solaris 10 and 11 - i386 / sparc
Suse 11 and 12
Ubuntu 12.04 and above
Windows XP Service Pack 2 and above
Windows Server 2003 and above

Encryption

All BORDERPOINT logs are sent from the monitored device to the procesing manager using AES 256 bit encryption via either UDP or TCP.

Installation

The BORDERPOINT agent can be installed using both .msi for Windows based operating systems and .sh command line script for *nix based operating systems. A full installation guide is provided if required. The agent install is fully automated and will automatically register with the BORDERPOINT service.

CONTACT CSA:

If you would like more information or would like to request a demonstration of the BORDERPOINT managed service then please contact us via:

Website: www.csa.limited
Telephone: +44 (0)1452 886982
Email: info@csa.limited

ADDITIONAL CSA SERVICES

Providing around the clock managed cyber services from the CSA SIOC from a team of Cyber professionals.

Our range of security assessments cover both technical and operational aspects for any business.

CSA produces its own and re-sells a number of specialist cyber products.

Your expert information security partner

CSA provides a range of cyber training services designed to meet an organisations needs.

Our crisis response service is run through the CSA SIOC providing a number of services to help companies when something goes wrong.

The Senior Team at CSA provide a range of cyber consultancy services to assist companies understand cyber security.

+44 (0)1452 886982 | UNIT 11, WHEATSTONE COURT, WATERWELLS BUSINESS PARK, GL2 2AQ | W: CSA.LIMITED

CYBERSECURITY Associates

BORDERPOINT PROTECTIVE MONITORING