Data sheet

BT Assure Log Retention

Addressing the compliance & incident response challenge

Meeting the challenge of compliance

Maintaining network logs will meet data retention requirements for a wide range of compliance mandates.

Government and industry regulatory compliance mandates have created a growing need for data privacy and compliance auditing. Organizations of all sizes are obliged to store the majority of IT system logs. They must also be able to provide immediate and historical evidence of access, activity and configuration changes for applications, servers and network devices.

The challenge of archiving an entire history of network activity and system logs can become a costly and time consuming burden. BT Assure Log Retention (ALR) repositories are indexed and searchable using the ALR user interface, as well as providing charts and reports for a visual view of data.

A managed approach to network logging

With BT managing your security, archiving and compliance requirements, your entire downtime and compliance history can be fully mapped and available for audit reporting on demand.

BT’s ALR service is part of the Assure Intelligence portfolio and may be used alone or with other BT managed security services. The ALR service is a fully managed log repository solution designed to assist with requirements to retain log files for a fixed period of time.

The ALR service enables the preservation of logs from supported networked devices.

These logs are stored on ALR purpose built appliances, which are deployed on client’s premise.

BT Assure Log Retention

Our managed log retention service can combine log management, real-time event correlation and alerting, remediation, and reporting in a high performance solution that simplifies the time-consuming task of monitoring and managing for compliance and security risks that can affect your business operations.

With BT you have a data storage solution that protects your intellectual property, financial data and business plans with BT able to collect all of your organisation’s logs from connected data sources, including built-in support for over 1,000 devices and applications with an easy device integration tool.

BT’s ALR service gives you rapid access to centralised log data for incident response, forensics, discovery and access to reporting packs for all major regulatory compliance standards.

Capabilities

- **Event logging and storage**

  Enables rapid incident investigation and convenient access to all audit and incident data by stored raw logs and correlated events on the same device.

  The storage capacity for raw logs and correlated events is configurable. Depending on your requirements, between 19TB - 269TB of compressed raw logs can be stored, enabling long-term, fully accessible, data retention.

- **Rapid drill-downs and incident summaries**

  Incident information is accessible from nearly all screens within the user interface. Details on incidents are immediately available with a minimum of clicks.

  Users can quickly investigate all incident-related information and see who was involved in an incident, what systems were affected, and how the attack occurred.

- **Real-time Incident Identification**

  A fast engine normalises parses and correlates incoming messages in near real-time. Administrators can see threats and attacks the second they are reported, allowing time to secure systems and prevent an attack from negatively impacting the network and connected assets.

- **Security and Compliance Reporting**

  Delivers detailed reports to aid in investigating incidents, comparing new threats against historical data, and preparing for compliance and corporate audits. Users can gain a better understanding of how an incident occurred, if there has been previous related activity, and what systems might have been affected.

  The reporting system enables fast, easy searches of raw logs based on a wide-range of criteria. Pre-configured reports specific to a variety of compliance regulations include PCI, SOX, HIPAA, GLBA, FISMA and ISO.

  These and other basic reports are available and automatically generated right out of the box. Additionally, individual reports specific to business needs can be created easily and quickly.

- **Extensive Device Support**

  Includes out-of-the box integration support for over one thousand devices, systems and applications. And an integrated device-builder tool lets you quickly and easily add support for other data sources.

Benefits

- **Incident Investigation**

  Supports incident response and forensics efforts by providing access to historic asset log data.

- **Automated Integrity**

  Raw log data is compressed in hashed archive files and indexed to meet data retention regulations.

- **Audit & Compliance Reporting**

  High volumes of raw log content can be summarized in reports or available for ad hoc audit reporting.

- **Device management**

  BT manages the log retention appliance and applies patches and updates, enabling the IT department to focus on core business functions, while still maintaining compliance with log retention requirements.

Service Features

- Purpose built appliance
- Installation, management and ongoing support
- Easy to use and intuitive user Interface
- Supports over 130 security devices
- With the default compression ratio of 10:1, up to 269TB of raw log retention on an enterprise class machine
- Ability to handle up to 115,000 messages per second
- Monitored and managed 24x7x365 by BT Security Operations Centre
- Optional encryption and Assure Threat Monitoring integration
- On-demand security and compliance reporting
- Optional professional services retainer

Achieve Optimal Results

When you combine our ALR service with our leading Assure Threat Monitoring service you also get:

A comprehensive correlation engine

- BT's proprietary correlation engine, matches your unique network information in order to identify threats, attack signatures, patterns and known vulnerabilities
- Eliminates false readings and identifies real threats faster than other DIY SIEM's
- Responds to threats with immediate and precise recommendations

24/7 compliance monitoring

- 24/7 incident response
- Integrity and presentation of data is legally admissible
- User access to programs and data constantly monitored and reviewed
- All logs are collected to BT secure facilities
- A subset of critical devices are monitored

The quick and easy way to a healthy network

BT can monitor devices across your networks, from intrusion detection systems, intrusion prevention systems, firewalls and routers, to servers, applications, mainframes and PCs.

We combine this monitoring with a database of identified threat situations and a worldwide team of experts to protect your infrastructure. We also offer you the option of outsourcing all aspects of the management to us - simplifying the process.

The solution enables BT to detect internal and external attacks on your network as they happen and halt these attacks before damage is done. This eliminates the expensive and time- consuming clean-up costs required following network attacks

> "Security and compliance requires specialized expertise, and it makes more sense to outsource that so my staff can stay focused on the core business objectives... BT can survey all the potential threats worldwide. They can provide a much wider, more current view of the threats. That's something we can't do as efficiently, given our current staff levels."
>
> *John Lambeth, CISSP,CISA*
> *VP Information Technology, Blackboard, Inc*

Trouble-free implementation

As soon as your data sources have been integrated, we can begin monitoring your network 24/7. We will alert you immediately to any anomalous behavior and when an incident occurs, you will receive ongoing assistance until the issue has been resolved.

You can see your network status at any time via a web portal. You can depend on timely assistance from our SOC analysts around the clock.

Why BT

Key role of human intelligence

Our philosophy is underpinned by a belief in the importance of human intelligence. No matter how advanced a technology, there will always be an attack that will get around it. This is where people enter the equation. No-one has more experienced and qualified security analysts who are able to recognise the bigger picture in the data than BT.

Security Operations Centres (SOCs)

BT has a network of 14 SOCs at different locations around the world, where customer devices are managed and monitored, and where our security analysts are on hand to provide real time support and response services to protect your networks. To provide the assurance of the highest quality of service, the SOCs are accredited and audited variously to ISO27001, SSAE16 and ISAE3402 and where appropriate to Government information assurance standards.

Breadth and depth of experience

Trust is one of the core values that drive BT's own business culture, and we believe it is fundamental to the choice of security partner for any organisation. We are one of the world's leading and most trusted security brands, derived from a set of credentials that have been earned over decades of experience in the field:

- We are one of the largest security and business continuity practices in the world, with over 2000 security professionals globally
- Our secure networking experience includes monitoring more than 335,000 customer devices from our Security Operations Centres around the world
- We have global analyst recognition for our achievement in delivering outstanding managed security services globally to customers.

www.bt.com/globalservices

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000