activeDEFENCE™ DNS Security - Enterprise Threat Protector

The enterprise threat landscape is fast evolving. Targeted threats such as malware, ransomware, data exfiltration, and phishing are increasing in volume, and malicious actors are becoming more adept at circumventing traditional security approaches. Combined with the adoption of SaaS, Cloud, and IoT in the enterprise, more sophisticated threat delivery has introduced new visibility challenges, controlpoint complications, and security gaps. Powered by unique global insights into Internet and Domain Name System (DNS) traffic, Enterprise Threat Protector enables security teams to proactively block and mitigate targeted threats and enforce an acceptable use policy across the enterprise.

Enterprise Threat Protector

Built on X carrier-grade recursive DNS, Enterprise Threat Protector (ETP) is a quick-to-configure and easy-to-deploy cloud solution that requires no hardware or software to deploy or maintain.

Enterprise Threat Protector leverages real-time Cloud Security Intelligence and our partner's proven, globally distributed recursive DNS platform to proactively identify and block targeted threats such as malware, ransomware, DNS data exfiltration, and phishing. The cloud portal enables security teams to centrally manage and enforce unified security and acceptable use policies in minutes for all employees.

How It Works

The Domain Name System (DNS) is the foundation for all Internet services, yet many malicious domains — including sites hosting malware and ransomware, and the associated command and control (CnC) servers — use recursive DNS for attacks.

When an enterprise's external recursive DNS traffic is directed to Enterprise Threat Protector, requested domains are checked against our real-time domain risk scoring threat intelligence, and enterprises can proactively block employees from accessing malicious domains and services. As this validation happens before the IP connection is made, threats are stopped earlier in the security kill chain, i.e., farther away from an enterprise's perimeter. In addition, DNS is effective across all ports and protocols, thus protecting against malware that does not use standard web ports and protocols.

Domains can also be checked to determine the type of content an employee is attempting to access and blocked if the content breaches the enterprise's Acceptable Use Policy (AUP).

Enterprise Threat Protector easily integrates with other security products and reporting tools — including Secure Web Gateways, Next Generation Firewalls, and SIEMs, as well as external threat intelligence feeds — allowing companies to maximize their investments across all layers of their security stack.

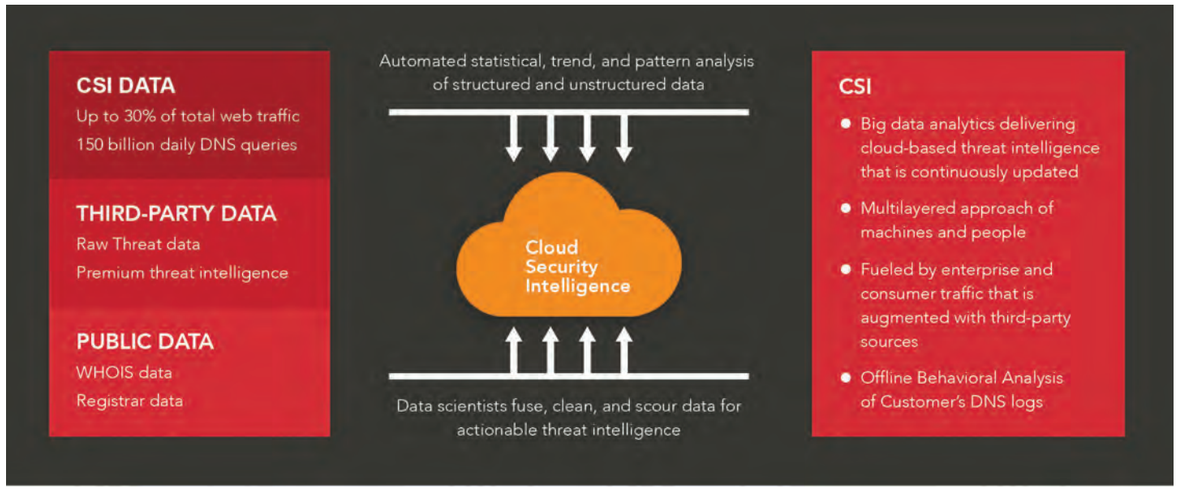
Recursive DNS Servers

The Recursive DNS Servers, which are distributed globally and deployed on our partner's Intelligent Platform, are responsible for resolving all of an enterprise's external DNS requests and provide exceptionally reliable and scalable recursive DNS service.

The use of Anycast routing ensures load balancing and optimal performance for the service.

Cloud Security Intelligence (CSI)

Enterprise Threat Protector is powered by our partner's Cloud Security Intelligence (CSI), which delivers up-to-date intelligence about malicious domains and the risk these domains present to companies.



This threat intelligence is built using insights gathered continuously from our Intelligent Platform, including up to 30% of global web traffic and up to 150 billion daily DNS queries. This data is enhanced with external threat feeds, and the combined data set is then analyzed using advanced real-time behavioral analysis and proprietary algorithms.

As new threats are identified, they are immediately added to the ETP service, delivering instant protection for companies and their employees.

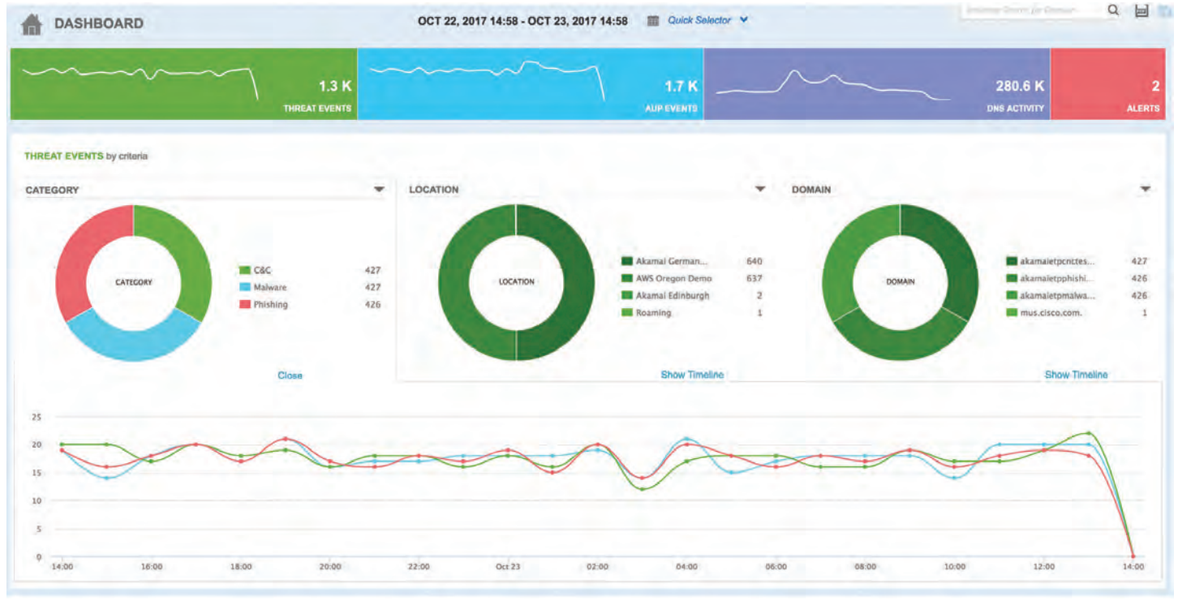
In addition, CSI also uses offline behavioral analysis of customers' DNS logs to identify if they may have been impacted by newly discovered threats. This helps reduce the identification time for new threats.

This combination of real-time and offline behavioral analysis techniques provides exceptional levels of threat protection.

Cloud-Based Management Portal

All configuration and ongoing management of ETP is done through our cloud-based Luna Portal, enabling management to be done from any location at any time.

Policy management is quick and easy, and changes can be pushed out globally in minutes to ensure that all of an enterprise's locations and employees are protected instantly. Email alerts can be configured to alert security teams about critical policy events so that immediate remediation steps can be taken to quickly identify and resolve potential threats.



A real-time dashboard provides an instant overview of ETP, and detailed information on any activity can be achieved by drilling down into individual dashboard elements. This detailed information provides a valuable resource for analysis and remediation of security incidents.

All portal functionality can be accessed via APIs, and data logs can be exported to a SIEM, allowing ETP to easily and effectively integrate with other security solutions.

Deployment And Configuration

There is no hardware or software to install, so configuration and deployment of ETP is simple and straightforward, and can typically be completed in less than 30 minutes. For most enterprises, all that is needed is to change their recursive DNS IP addresses to point to our ETP service.

Most typically, the existing recursive DNS resolution will be provided by an on-premise Recursive DNS Server such as Infoblox or Microsoft Active Directory, or through the enterprise's ISP.

In addition, ETP can interoperate with a Secure Web Gateway or Next Generation Firewall by configuring the product to forward DNS requests to the ETP service.

Deployment	Configuration Changes Required
DNS set by DCHP (i.e., guest Wi-Fi)	Set the DHCP DNS server to point to ETP
Set the DHCP DNS server to point to ETP	Set the DHCP DNS server to point to ETP
On-premise DNS appliance (i.e., Infoblox)	Also a simple forwarder
On-premise Secure Web Gateway or NGFW	Configure the SWG to forward DNS requests to the activereach ETP service

Configuration

The configuration of ETP is simple and straightforward and consists of the following steps.

1. **Create one or more locations:** A location identifies where the DNS requests originate from. This is achieved by using the public-facing source IP address of the DNS traffic — most typically this will be the external IP address of the router, but could also be the IP address of the on-site recursive DNS server if that has a public-facing IP address.

   Each location can have one or more IP addresses associated with it.

   Three Separate Locations
   Boston Office – 194.71.97.31
   London Office – 194.88.65.38
   Tokyo Office – 194.92.72.12

   One Single Location with Three Offices
   Global offices – 194.71.97.31, 194.88.65.38, 194.92.72.12
   A location can also be identified by using CIDR notation.

2. **Create a policy and attach the policy to one or more locations.**
   An ETP Policy consists of the following components:

Item	Description
Security Lists	These are the frequently updated security lists that are maintained by activereach. The lists contain domains and resolved IP addresses covering the following threats: • **Malware –** domains or IP addresses that are known to serve up malware or ransomware binaries. • **Phishing –** domains or IP addresses have been known to be used to host phishing pages. • **CnC -** domains or IP addresses that have been known to be used by malware to communicate with to retrieve commands and control requests from adversaries. Each threat type list contains known and suspected domains and IP addresses that can be configured separately. Each list can be configured with a policy action: • **Block Page:** the DNS request is redirected to a customizable error page that indicates access is prohibited to the domain. • **Deny:** the DNS request is denied, and the user is redirected to a browser-specific error message. • **Sinkhole:** the DNS request is redirected to the IP address of a security device that can be used to collect information about suspicious traffic. The sinkhole can either be the activereach Security Connector or a customer sinkhole. • **Monitor:** the DNS request resolves as expected, but the event is logged. An email alert can be configured for each threat type. A policy can be attached to one or more locations, but each location can only have one policy attached to it.
Custom Lists	Custom Lists allow you to use your own threat intelligence resources in Enterprise Threat Protector either manually or through an API. You can create an unlimited number of Custom Lists, but there is a limit of 200,000 entries across all your lists. Lists have the same parameters as the activereach Security Lists. All Custom Lists are attached to all policies, but you can modify the policy action and list order in each policy.
Acceptable Use Policy (AUP)	AUP allows you to restrict the categories of web content that users can access. If the action for a category is set to Block Page, a user will receive a customizable block page if they attempt to access a domain listed in that category.

3. **Create a Quick list (optional):** Quick lists are global allow and deny lists that are effective across all policies. Domains and IP addresses can be added to the list and a maximum of 2,000 entries can be included.

4. **Deploy:** The configuration is pushed out globally, typically in less than 30 seconds. However, if Custom Lists are used, these can take up to 60 minutes to be deployed.

Monitoring

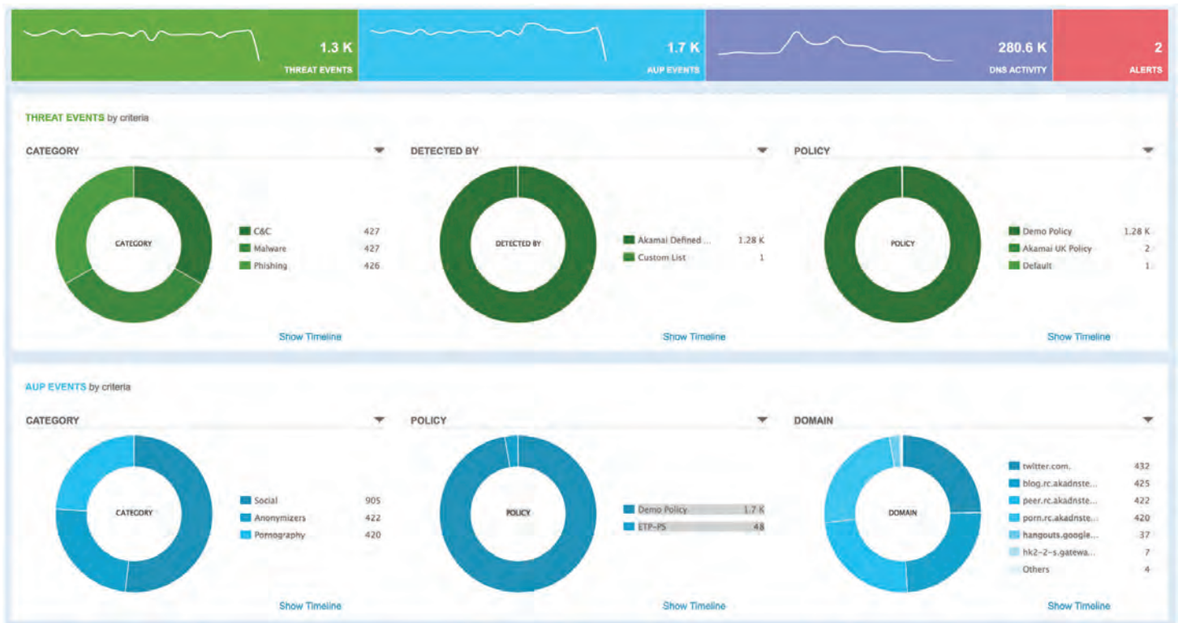
Monitoring provides a comprehensive high-level view and detailed information about ETP and consists of three parts:

- **Dashboard:** Provides an overview of ETP, and of the threat and AUP events over the past 24 hours, week, or month.
- **Events:** Provides deeper detail on threat and AUP events.
- **DNS Activity:** Provides an overview of DNS traffic.

DNS Logs are retained for 30 days, and SIEM integration can be done via a JSON API.

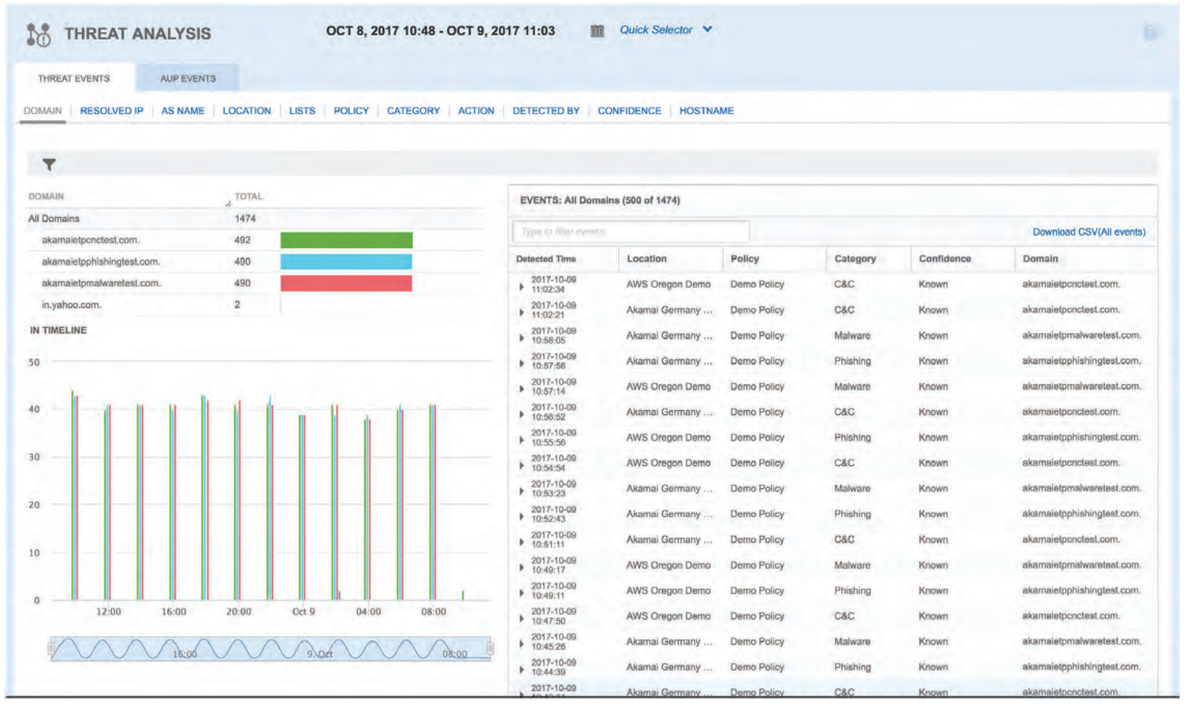
Dashboard

This provides an overall view of ETP activity over the last 24 hours/week/month or a specified date or date range. The dashboard view can be customized to show different criteria and to display a timeline of events.



Events

Events provides deeper insights into Threat and AUP events. Views can be customized and filtered.



For Threat events, you can view these by:

- Domain
- Resolved IP
- AS Name
- Location
- Lists
- Policy
- Category
- Action
- Detected By
- Confidence
- Hostname

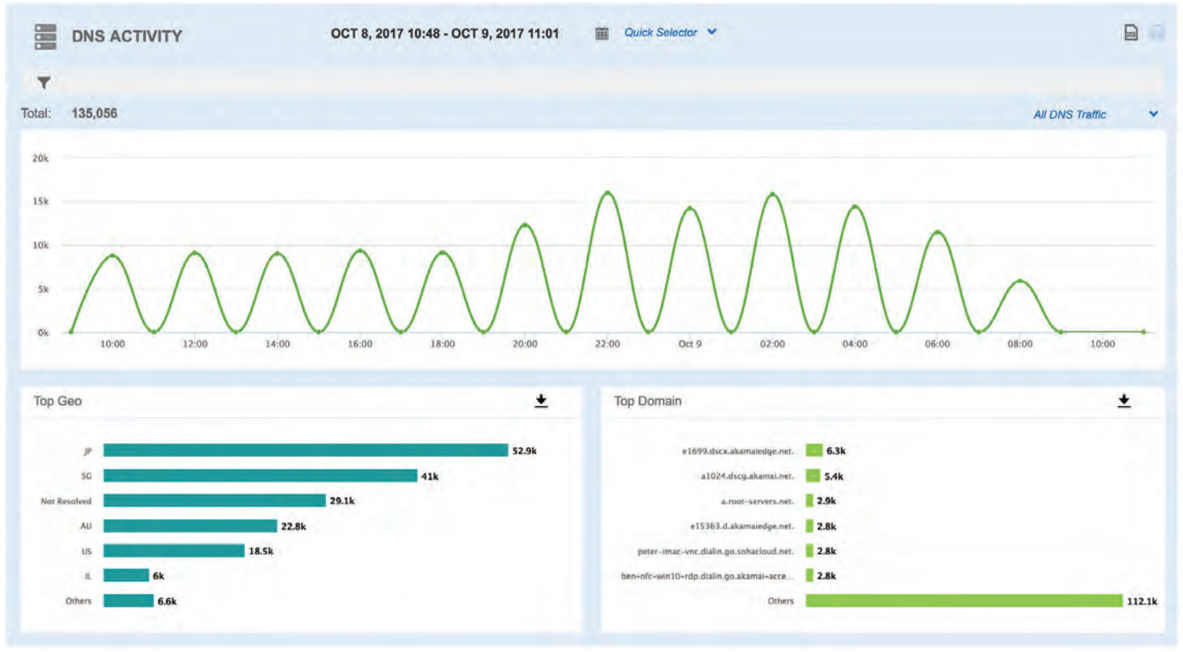
For AUP events, you can view these by:

- Category
- Domain
- Policy
- Location

Threat and AUP events can be downloaded as a CSV file for further analysis or integrated into a SIEM via a JSON API.

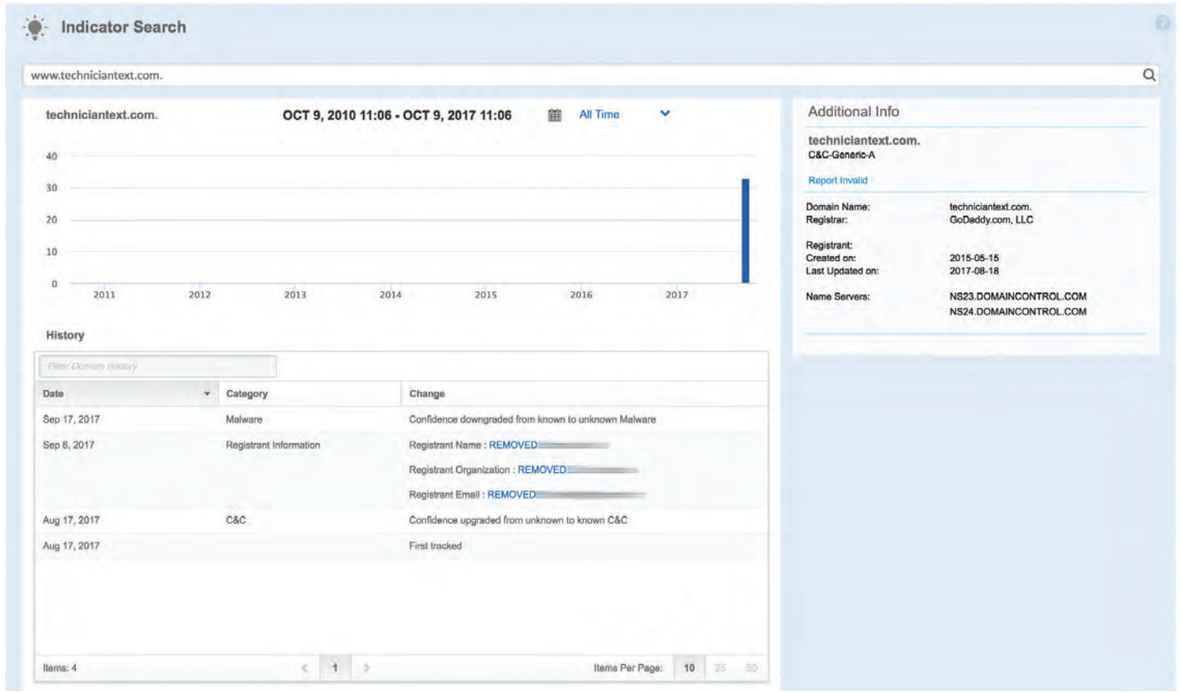
DNS Activity

DNS Activity provides an overview of all DNS traffic by AS Name, Domain, Geography, Location, Query Type, and AUP.



Intelligence

This allows you to obtain a summary of the intelligence that we hold about the domain in its Threat Intelligence List. You can either enter a domain directly or click on the link in the events page.



Operating Systems Supported

- Microsoft Windows: 10 and 7
- Apple OS X: OS X 10.12 (Sierra), OS X 10.11 (El Capitan), OS X 10.10 (Yosemite)

Specifications

	Download Size	Installed Disk Space	Memory Used
OSX	<3 Mb	<7 Mb	Daemon: <3 Mb UI: <20 Mb
Windows	<7 Mb	<7 Mb	Service: <16 Mb UI: <20 Mb

Identifying Endpoint Devices With The Enterprise Security Connector

The Enterprise Security Connector is a Virtual Machine that you can deploy on your internal network to receive malicious traffic so that you can identify the IP addresses of the device or devices. DNS requests are sent to the Security Connector when a policy action is set to Sinkhole.

Requirements

To deploy the ETP Security Connector, the following requirements apply:

- You must deploy the ETP Security Connector on VMware ESXi version 5.5 or later
- Ensure that the virtual machine meets the following resource requirements:

  - RAM: 1 GB - Disk Space: 30 GB - CPU: 2 cores

The Security Connector is supplied as an OVA file.

Protecting Laptops With The Enterprise Client Connector

The Enterprise Security Connector is a lightweight client that can be installed on Windows and OS X laptops to provide improved protection when users are off-network and not connected to the VPN.

About activereach®

activereach® is a leading technology integrator providing bespoke IT solutions and professional services to customers in the areas of Security, Collaboration and Connectivity. Our independent consultative approach helps organizations maximise business value from their technology investments, providing a platform for businesses to grow, reinvent and transform.

Working in partnership with many of the world's leading technology vendors and software providers, we offer the most innovative hosted, on-premise and cloud based services. Our consultancy, technology and services have transformed hundreds of businesses across the UK, Europe & Middle East – ranging from FTSE 500 enterprises to corporates and SMEs. Operating across our activeNETWORKS™, activeDEFENCE™ and activeCONNECT™ technology divisions, activereach is headquartered near London, UK.

activeDEFENCE™
END TO END SECURITY

activereach Ltd.
4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks. HP12 3YZ.
Tel: 0845 625 9025 / Fax 01494 980 255 / Email: contactus@activereach.net

Ref: ETP2018.1
www.activereach.net