activereach®

# HACKWATCHMAN™

Every year, hundreds of companies only find out that they have suffered a data breach when they are notified by a third party – often weeks or months after the initial infiltration. Even companies that spend millions of pounds on their security have no idea if malicious insiders are trawling for valuable data where they shouldn't be.

HackWatchman is a simple but effective managed detection service designed to instantly reveal the presence of malicious insiders on compromised networks.

## BREACH DETECTION: SERVICE OVERVIEW

An attacker, be that an individual hacker or malicious software, aims to gain a beachhead into a target network. Regardless of how they achieve that, once they have compromised one computing device, the most common next step is to identify other assets on the same local network and scan them for vulnerabilities that could be exploited, or use stolen credentials to try to login as a legitimate user.

**HackWatchman involves locating a number of tempting-looking computer assets on the local network segments next to devices you want to protect:**

- The Detector's sole job is to mimic other assets, and raise the alarm if anyone tries to access them
- The device is securely registered with activereach's management service (hosted in the EEA for GDPR purposes)
- The portal is configured to send real-time e-mail or SMS alerts whenever the detector is touched, with details of the suspect traffic, and where it came from
- HackWatchman is available as a 24x7x365 Managed Security Service

# HOW IT WORKS

activereach's Breach Detectors are small form factor appliances, powered by USB or AC power adaptor (included), which have a 100Mbps Ethernet port and require an IP address with outbound access to DNS services through any existing security layer.

As well as appliances, Breach Detectors are available as a virtual appliance (VMWare), and for AWS.

Once installed onto a network segment, the Breach Detectors are configured to mimic one of dozens of computing devices.

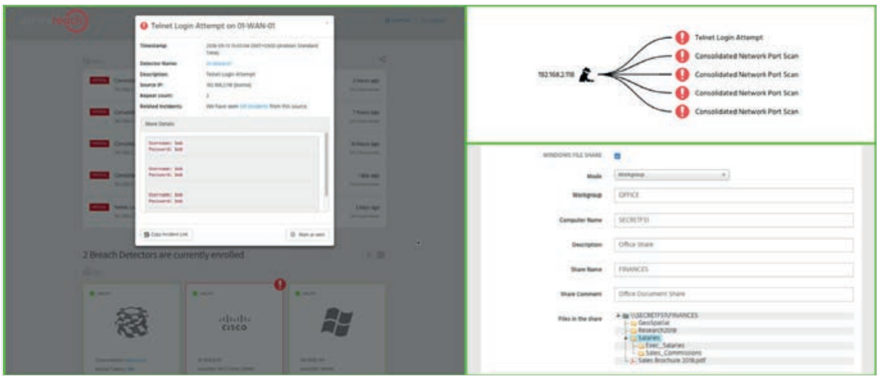
The devices are securely registered with a cloud service dedicated to the customer's collection of Breach Detectors and communicate using DNS protocols, with an encrypted payload.

Attackers who have breached your network, malicious insiders and other adversaries make themselves known by trying to access the Breach Detector.

If any of the devices are scanned, browsed, fingerprinted, or otherwise 'touched' by network traffic, even within the protected network segment, the Breach Detector signals an alarm.

Breach Incident
Shared File Opened.
Source:
192.169.103.59
Target: dc 104
(10.122.34.5) File:
"2016-Tender-Summary.pdf" User:
Guest

*SMS/E-Mail Alerting Service*



Telnet Login Attempt on 01-WAN-01

Description: Telnet Login Attempt

2 Breach Detectors are currently enrolled

192.168.2.118
Telnet Login Attempt
Consolidated Network Port Scan
Consolidated Network Port Scan
Consolidated Network Port Scan
Consolidated Network Port Scan
cisco

WINDOWS FILE SHARE ☑

Mode: Workgroup

Workgroup: OFFICE

Computer Name: SECRETFS1

Description: Office Share

Share Name: FINANCES

Share Comment: Office Document Share

Files in the share:
\\SECRETFS1\FINANCES
GeoSpatial
Research2018
Salaries
Exec_Salaries
Sales_Commissions
Sales Brochure 2018.pdf

*activereach Breach Detector: Management Dashboard*

# TYPICAL DEPLOYMENT CONFIGURATIONS

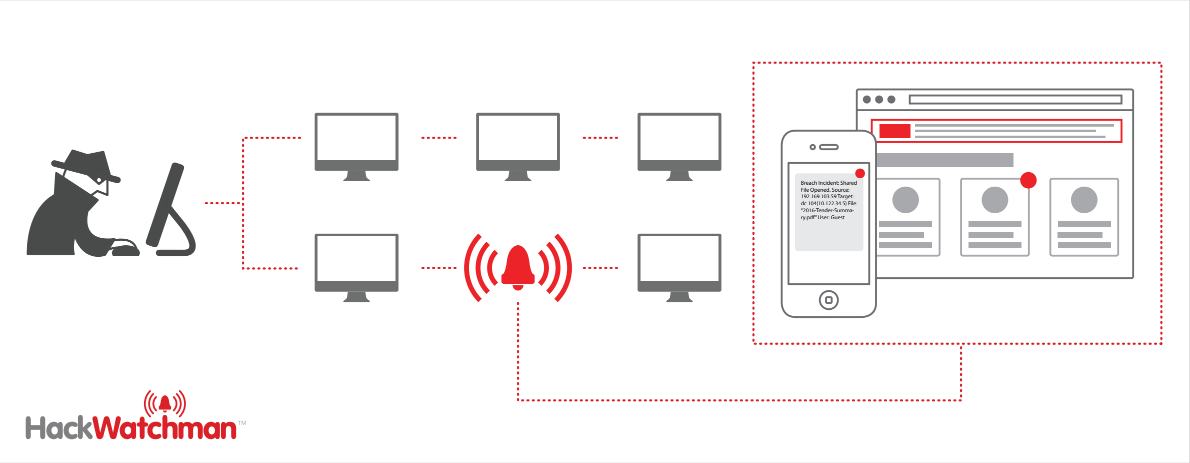
Breach Detectors are deployed all over the world. The possible OS, service and port permutations number in the thousands. The Breach Detectors are supplied with a host of default "personalities" including several flavours of Windows, Linux, routers, switches and SCADA equipment (programmable logic controllers).

What matters, of course, is where you place the Breach Detectors. If you are a large financial organization, and place a "Dell Switch" in the CEO's office, it may get tripped over by a really clumsy attacker, but there are several spots on your networks where attackers are likely to show up. activereach can advise on optimal location of your Breach Detectors on one of your DMZs, database segments or your VOIP network, etc.

**Typical deployments include the set-up of the Breach Detector to mimic:**

- Web application servers or SQL servers in a DMZ network segment
- Endpoints of managers or executives on internal networks
- Cisco routers that seem to be connected to third parties such as banks, or data centres
- Sensitive file servers in an AD domain, even SCADA systems

There is no need to purchase additional licenses e.g. to mimic a Windows device.



Breach Incident: Shared File Opened. Source: 192.169.103.59 Target: dc 104(10.122.34.5) File: "2016-Tender-Summary.pdf" User: Guest

*Attackers immediately reveal their presence by interacting with the activereach Breach Detectors*

## DECOY PERSONALITIES

Appliances can be configured to mimic other computing devices from this list:

- Windows 2012/2008/2000
- Windows Sharepoint 2010
- Windows 8/10/XP Desktop
- Diskstation NAS
- VMWare ESXi server
- HP iLO Server
- Joomla Server
- CUPS Server
- JBOSS Server
- Dell Switch
- Cisco Router
- Standard Linux Server
- Linux Database Server
- Linux Proxy Server
- Rockwell Automation PLC
- Siemens Simatic PLC

Custom configurations and behaviours are available at an additional charge based on complexity.

## ONGOING SUPPORT

HackWatchman comes with our basic support service (UK working hours 9-5pm), with a number of support cases that can be requested by the customer (default is three per Breach Detector). Each case can either be a remote reconfiguration of a Breach Detector to adopt a new configuration, or assistance in understanding, diagnosing, and resolving an alarm where the customer needs additional assurance.

Enhanced support services that extend the operating hours, and provide proactive incident response, managed security integration and/or managed SOC services are separately available.

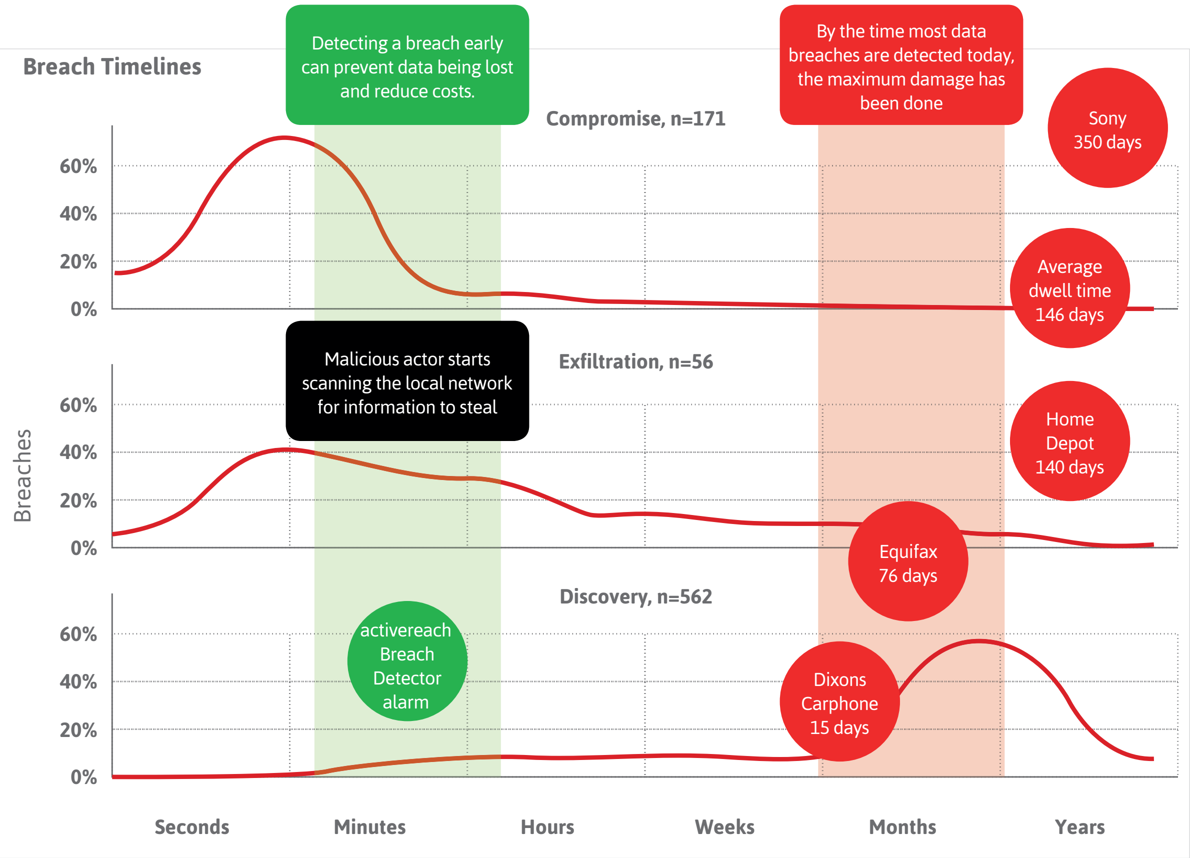
## CUSTOMER REQUIREMENTS

- Each appliance needs a USB port or UK AC power socket for power (5V, 2A).
- Each appliance needs a Cat5 or similar cable for Ethernet connection to switch LAN port.
- Each appliance needs an IP address from the subnet it will be installed on.
- Small form factor appliances are also available as a VMware appliance or cloud service.
  Call for details.

# THE CASE FOR BREACH DETECTION

The elapsed time between a threat actor gaining control of a device inside your network, and that breach being detected, is called the dwell time. An attacker, with an abundance of time, can systematically exfiltrate databases of credit cards and personal information with stealth, and may even be able to escape undetected.

Data breaches are a fact of life in modern information technology, but the mean dwell time is increasing each year, rather than decreasing. If we could reduce the dwell time, from the current average of 146 days, to hours, or even minutes, then we can reduce the number of data records removed, reduce the risks to the data subjects, and avoid subsequent compensation claims and reduce any regulatory fines for breaches of data protection.



*The activereach Breach Detection Service can reduce the mean dwell time from months to minutes*

Note: activereach is a data processor under EU GDPR for this service, which may involve the transfer of IP addresses, and storing e-mail addresses, which are sometimes personal information.

## Reduce Your Breach Detection Time - Call: 0845 625 9025 or Email: contactus@activereach.net

### About activereach

activereach® is a leading technology integrator providing bespoke IT solutions and professional services to customers in the areas of Security 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™ and activeDEFENCE™ technology divisions, activereach is headquartered near London, UK.

**activereach Ltd.**
4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks HP12 3YZ
Tel: 0845 625 9025 | Email: contactus@activereach.net | Web: www. activereach.net