

White Paper:

Why Build a Service-Centric Security Strategy?

Bad actors are not limited to Hollywood. According to the 2019 Verison Data Breach Investigations Report, (DBIR) 59% of healthcare breaches exposing corporate data to an unauthorised 3rd party were caused by internal actors. This paper outlines how a CISO can plan and build a security defense against these bad actors.

The Healthcare industry stands out as a leader in securing data, because it is highly regulated and is required to report in more detail than most industries, but costly internal data breaches are seen across all industries. What is the bad actor insider threat?

An insider threat is a malicious threat or a well-intentioned employee error that originates within the targeted organisation for the purpose of negatively impacting the business.

These threats come from people such as employees, former disgruntled employees, contractors or business associates within the organisation who abuse data access and privileges.

Cost Optimisation

The focus here is on managing costs. Building on the foundations of structured ITAM, waste is identified with asset discovery, and actions put in place to cut it; recycling and reharvesting activities are in place data is shared with procurement to ensure contracts are right-sized and with finance to support budgeting.

Insights are provided on current use and to inform demand management, cost prediction, cost analysis, licensing options, application rationalisation and technology strategy decisions.

Compliance is Critical

Companies that deal with Protected Health Information (PHI) are required by The United States Health and Human Services (HHS) to develop a security strategy that has physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. Identifying and building a security defense against those attack vectors is difficult because of a number of reasons including:

- Networks containing electronic PHI (ePHI) are becoming more complex
- Adoption of hybrid cloud, virtualisation, containers and micro services
- Inheriting unknown IT assets from a merger or acquisition
















The Problem

Organisations fail to develop a mature security strategy because they have no idea how many assets are on their networks, where they are, who owns them and what role the assets play to deliver business critical services. The Verison 2019 report identified that out of 41,686 security incidents across all industries 34% involved internal actors.

Consider a Service-Centric Security Approach

The Service-Centric approach enables an IT professional to take a methodical step-by-step approach to this problem and continually, assess, improve, and mature over time.

ITAM Maturity Model

Level 0	Level 1	Level 2	Level 3	Level 4
Nothing	Asset Discovery & CMDB/ITSM Integration	Infrastrucutre and Service Dependency Mapping	Infrastructure Monitoring	Business Service Mangement
Risk 	Risk 	Risk 	Risk 	Risk 
Cost 	Cost 	Cost 	Cost 	Cost 
Effort 	Effort 	Effort 	Effort 	Effort 

Level 1: Asset Discovery & CMDB/ITSM Integration

Building a mission critical security defense strategy starts with a strong foundation of accurately identifying all assets on the network at all times. Using a combination of passive and active discovery methods is essential so you are able to discover, identify and sync assets (devices) in realtime with CMDB and ITSM solutions for faster incident resolution; ensuring higher availability and customer satisfaction.

FireScope Delivers: All Assets are identified, catalogued and accounted for, as well federated to the CMDB.

Level 2: Map Devices & Dependencies that Deliver Business Services

A mapping tool would need to passively listen to the network flow traffic and discover all the servers and devices that are communicating in an application or service. Then automatically discover and suggest service groupings without prior knowledge or input by the user. Establishing a baseline then allows for the detection of real-time changes and threats.

FireScope Delivers: All Business Services mapped, clearly identifying device dependencies and communications among assets.

Level 3: Monitor Performance Avoid Service Disruptions

Now monitor the health and availability of servers, applications, storage, network devices, and more to proactively avoid service disruptions due to suspicious activity, authorized or unauthorized changes and device failures. Then if an application or asset diverges from that baseline an alert can be generated and sent to whatever standard tool or workflow the enterprise has in place.

FireScope Delivers: Baseline and policies are established and monitoring is in place to alert on deviations.

Level 4: Align IT with Business Objectives

The last phase is to ensure that going forward the health and performance of business-critical services supported are aligned to business objectives to reduce risk, secure your services, plan successful cloud migrations and avoid costly service disruptions.

FireScope Delivers: Service-centric security strategy is in place as well as ongoing monitoring and exception workflows.

FireScope stands ready to assist you with this service-centric approach and deliver the right platform and expertise to remove the risk and exposure of bad actors. FireScope delivers:

- Augmented perimeter security controls by baselining business services and detecting authorised and unauthorised changes.
- Change detection of new network communications including threats targeted at systems and services with ePHI data and integrate with SIEM tools.
- A virtual internal security perimeter around your business services that detects changes in real-time.

Contact us today for a complimentary, Service-centric Security Strategy assessment.

Tel: +44 (0)118 324 0620
info@pinkelephant.co.uk
www.pinkelephant.co.uk
Twitter:@PinkElephantUK

Pink Elephant EMEA
9 Castle Street
Reading
RG1 7SB
United Kingdom



PINK Expect more.
Expect Pink.

www.pinkelephant.co.uk