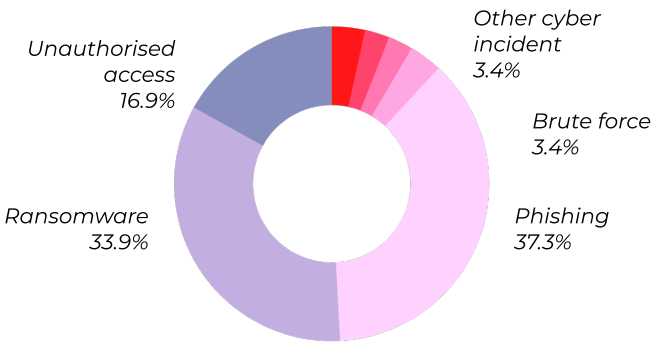
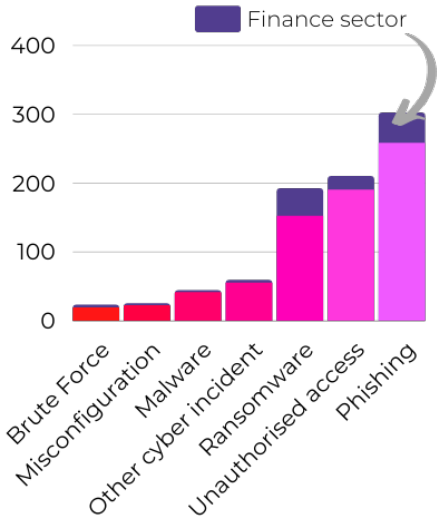
Overcoming the BYOD Challenge in Financial Services

YOU ARE A VALUABLE TARGET FOR CYBERCRIMINALS

As a Financial Service provider you are a gateway to vast amounts of sensitive PII (Personally Identifiable Information), making your employees a highly attractive target to attackers. The challenge for organisations is how to ensure that *every* endpoint is secure, that you have a view over the compliance status of your entire mobile workforce, without invading employee privacy.



The Finance Sector is particularly susceptible to **phishing** and **ransomware** [1]



Challenge: Protecting against evolving cyberthreats

Phishing attacks and ransomware are the prime causes of data loss for Financial Services. The vast amount of sensitive PII you hold makes every employee a valuable target for cybercriminals. Humans are the weakest link in the security chain, and despite regular employee training, employees regularly fall for scams, click links to malicious websites, connect to compromised WiFi networks, or install dangerous apps. You need to ensure every device is protected, including mobiles and tablets where small screens and distractions often cause security slip ups.

How to overcome it

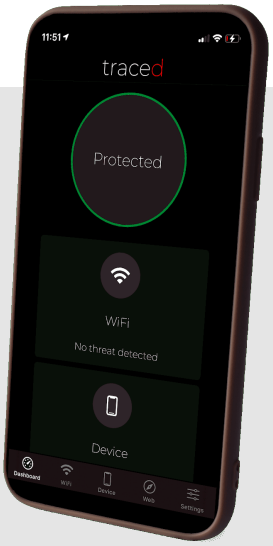
The Traced app uses our patented dynamic AI model, learning from hundreds of thousands of sample malware, malicious websites, phishing identifiers and app behaviours to protect devices against known and brand new threats. The Control platform gives your team a single-pane-of-glass view of incoming threats and whether the user has resolved them.

HOW DOES DATA BECOME COMPROMISED?

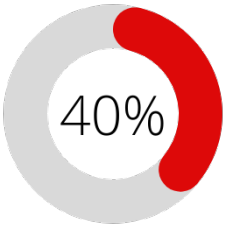
Network threats
- Man-in-the-Middle attacks
- Phishing
- Malicious proxies
- Unsecured WiFi
- Weak WiFi security

Device threats
- OS exploits
- Vulnerable configuration

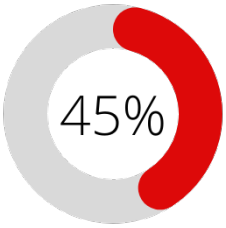
App threats
- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse



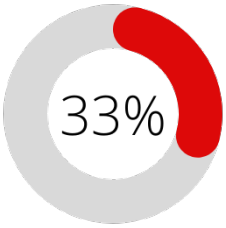
An Ivanti survey of 400 CISOs across Europe asked the question: What are your top IT security challenges? [2]



employees using their own devices to access corporate data



using unsecured Wi-Fi to access business resources



employees using unauthorized apps to access corporate data

Challenge: Ensuring compliance across the organisation

Regulatory compliance is mandatory and keeping up with changing policies and new ways of working is a difficult and thankless task. To meet the guidance of GDPR, PCI-DSS, the FCA, and other standards you need to demonstrate appropriate security measures across your organisation, protecting every endpoint and network. With more employees working from home, outside your network perimeter, and using shadow devices to access sensitive PII that you are responsible for, it's more important than ever to ensure there is an additional layer of security on employee mobile phones and tablets.

How to overcome it

With Traced Mobile Threat Defence you are ensuring that both company- and personally-owned mobile devices are protected against data loss and theft, significantly reducing the risk of financial and reputational damage. The Control dashboard enables you to see at a glance which devices are out of compliance, so you can take immediate steps to remedy it.

The threat landscape has been forever changed by widespread remote working and increasing integrations with third parties.

As threats evolve and attacks become more sophisticated it is vital that every employee has the training and tools to identify and remediate cyberattacks and data breaches.

Challenge: Full, frictionless employee adoption

Employees want to be productive at work, and that means that the distinction between designated personal and work devices has become blurred. BYOD strategies are great for efficiency and productivity, but come with significant challenges for the security team. Staff will find their ideal way of working, so instead of trying to stop them, pave the cow-paths and make it easy to use personal devices at work.

Traced respects employee privacy

Your business remains protected against mobile threats without tracking employees. Web browsing, photos, videos, calls, contact, emails and messages stay completely private.

How to overcome it

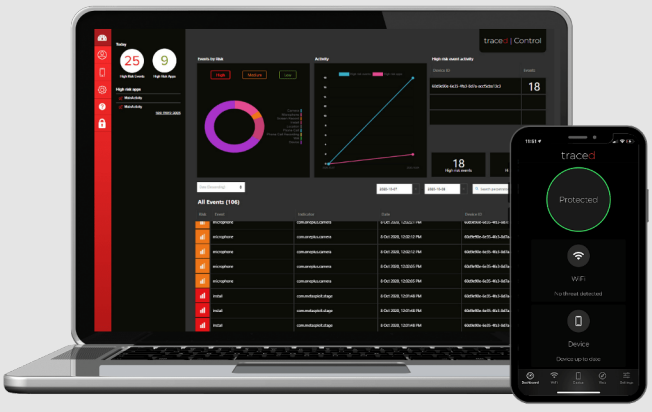
You can invite every employee to install the Traced app on multiple personal phones and tablets. Set up is simple and quick, the app is intuitive and lightweight - and most importantly, employee privacy is at the heart of Traced. And if this isn't enough to stimulate full employee adoption, you can see at a glance if any devices have not yet been enrolled into Control or if they've not been set up correctly. Peace of mind for you, knowing your entire organisation is protected.

traced | Control

MOBILE SECURITY MADE SIMPLE

A robust, low-cost MTD to guard against data loss and regulatory fines.

- See which devices are enrolled and protected
- Comply with data protection regulations
- High-level view ensures employee privacy
- Identify threats and remediate straight away



Sources

[1] Types of cyber incidents reported to the ICO from organisations in Q2, FY20-21
[2] Ivanti, EMEA CISO Survey: How the pandemic has shifted CISO priorities, 2021

https://traced.app
Oxford, UK