Post event report

SECURING FINANCIAL SERVICES VR

The 2nd Securing Financial Services^{VR}

7th July 2021 | Online

Strategic Sponsors

DARKTRACE

ExtraHop

FORTINET

INTSIGHTS Democratizing Threat Intelligence™

proofpoint.

okta

Recorded Future®

Education Seminar Sponsors

BeyondTrust

Centrify

LogRhythm

MENLO SECURITY

OneTrust GRC INTEGRATED RISK MANAGEMENT

RANGEFORCE

RED SIFT

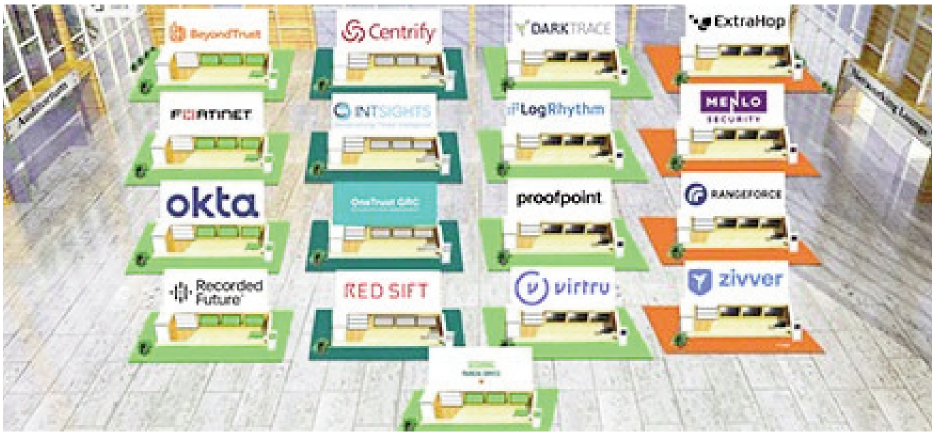
virtru

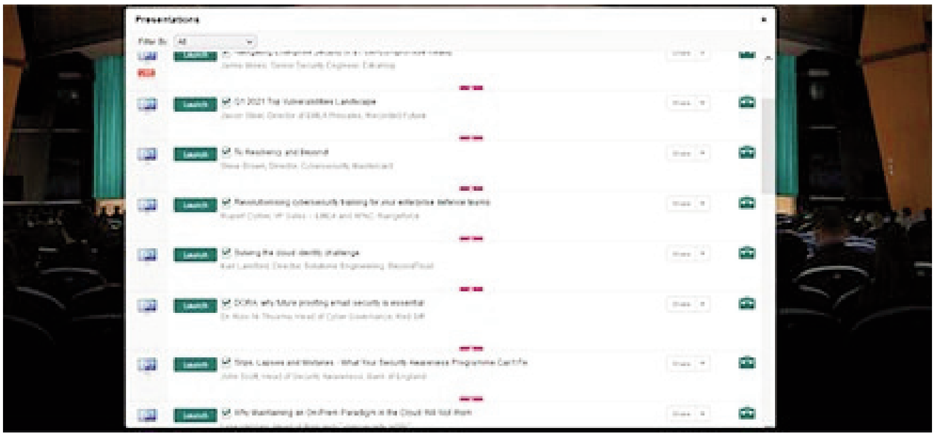
zivver

> “The online conference format was intuitive and an excellent user experience – I liked the ability to deal with a few matters arising between sessions and still get the whole session. The catering was excellent, all my food preferences taken care of, but service was a little sloppy I had to go to my kitchen to fetch my food.”
>
> **Identity and Access Management Specialist, Group Technology and Information, Sanlam**

> “The securing financial services forum was a great event, with some thought provoking presentations across the day and some good risk insights, I found the presentation covering differing approaches to risk appetite to be excellent and something that would help us here and ensure Board-level alignment and engagement on this key risk area.”
>
> **Chief Risk Officer, Monmouthshire Building Society**

Inside this report:





Presentations

Filter By: All

Jamie Moles, Senior Security Engineer, ExtraHop

Q1 2021 Top Vulnerabilities Landscape
Jason Steer, Director of EMEA Presales, Recorded Future

To Resiliency and Beyond
Steve Brown, Director, Cybersecurity, Mastercard

Revolutionising cybersecurity training for your enterprise defence teams
Rupert Collier, VP Sales – EMEA and APAC, RangeForce

Solving the cloud identity challenge
Karl Lankford, Director, Solutions Engineering, BeyondTrust

DORA: why future proofing email security is essential
Dr Rois Ni Thuama, Head of Cyber Governance, Red Sift

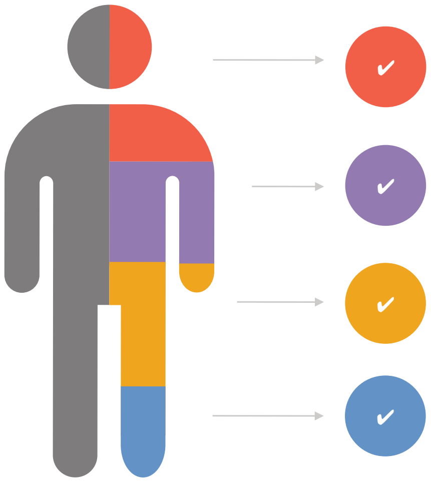
Slips, Lapses and Mistakes - What Your Security Awareness Programme Can't Fix
John Scott, Head of Security Awareness, Bank of England

Why Maintaining an On-Prem Paradigm in the Cloud Will Not Work

Key themes

- Building a secure multi-Cloud strategy
- Frictionless security: the customer challenge
- Staffing Cloud security
- Vulnerability monitoring
- Identity & access management in the Cloud
- Is hybrid Cloud the answer to security worries?
- SaaS, IaaS, PaaS
- Securing data in transit
- The security challenges of Cloud Native
- Solving the Cloud visibility problem
- Keeping regulators happy
- Ensuring consistent control

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Matt Bailey, Platform Specialist, Okta

Rob Bolton, Sr Director Intl at Information Protection, Proofpoint

Steve Brown, Director, Cybersecurity, Mastercard

Nick Colin, Regional Sales Director – EMEA, UK&I, Centrify

Rupert Collier, VP Sales – EMEA and APAC, RangeForce

Simon Collins, Director, Head of Cybersecurity, Allianz Global Investors

Brian Cooke, CISO, PermanentTSB

Daniel Crossley, Sales Engineering Manager, LogRhythm

Philip Edwards, Director, Global Head of Security, Revolut

Rick Goud, CIO, Zivver

Luke Hebbes, Head of Risk and Cybersecurity, HSBC

Martin Ingram, Product Owner, Identity and Access Management, NatWest Group

Karl Lankford, Director, Solutions Engineering, BeyondTrust

Rob McDonald, SVP of Platform, Virtru

Tom McVey, Solution Architect, Menlo Security

Jamie Moles, Senior Security Engineer, ExtraHop

Nick Pavlichek, Product Manager, OneTrust

Mariana Pereira, Director of Email Security Products, Darktrace

Dr. Rois Ni Thuama, Head of Cyber Governance, Red Sift

Joe Robertson, EMEA CISO, Fortinet

Tiago Rosado, Head of Cybersecurity, Curve

John Scott, Head of Security Awareness, Bank of England

Jason Steer, Director of EMEA Presales, Recorded Future

Chris Strand, Chief Compliance Officer, IntSights

Jerome Walter, CISO, Digital Venture, Standard Chartered Bank

Mark Williams, Customer Success, EMEA, Virtru

Laure Zicry, Head of Cyber Insurance Western Europe, Willis Towers Watson

Agenda

08:00	Breakfast networking
08:55	Chairman's welcome
09:00	**Two cases for measuring cyber-risk appetite** **Simon Collins,** Director, Head of Cybersecurity, Allianz Global Investors, and **Brian Cooke,** CISO, Permanent TSB • Join this session to hear two alternative approaches to measuring cyber-risk appetite • One approach will focus on the sophistication of the attackers, the other will be based on key risk indicators • Both approaches will be explored, followed by a discussion of the strengths and challenges of each
09:20	**Navigating enterprise security in a post-compromise reality** **Jamie Moles,** Senior Security Engineer, ExtraHop • Every organisation gets compromised – it's how fast you detect and respond to an incident that counts • This is especially important when you look at trends like the overnight move to remote work, the rise in encrypted traffic and acceleration of cloud adoption, as well as the proliferation of enterprise IoT that have expanded the attack surface and complicated the job of security professionals • We'll explore those trends and the opportunity that lay ahead for security teams post-compromise to prevent an event that results in an outage or an incident from becoming a full-scale data breach
09:40	**Q1 2021 Top vulnerabilities landscape** **Jason Steer,** Director of EMEA Presales, Recorded Future • Why Q1 2021 had the highest high-risk vulnerabilities since our report began • Why your supply chain is your achilles heel • Why COVID continues to shape the vulnerability landscape
10:00	**To resiliency and beyond!** **Steve Brown,** Director, Cybersecurity, Mastercard • Increasingly complex networks of business relationships are exposing participants to systemic operation risk • As a result, our national security, public safety and economic growth are being exposed to major disruption • In this session, see how Mastercard is delivering trust through an approach that quantifies, automates and prioritises risk to build cyber-resilience and trust throughout the connected digital economy
10:20	**Education Seminars | Session 1** **BeyondTrust** **Solving the cloud identity challenge** **Karl Lankford,** Director, Solutions Engineering, BeyondTrust **RangeForce** **Revolutionising cybersecurity training for your enterprise defence teams** **Rupert Collier,** VP Sales – EMEA and APAC, RangeForce **Red Sift** **DORA: why future proofing email security is essential** **Dr. Rois Ni Thuama,** Head of Cyber Governance, Red Sift
10:50	Break and networking
11:20	**Delegates will be able to choose from the following topics:** **Slips, lapses and mistakes – what your security awareness programme can't fix** **John Scott,** Head of Security Awareness, Bank of England • Everyone knows by now not to click a suspicious email or to open a dodgy looking attachment. So why does it keep happening? • This session will draw on the fields of health and safety and behavioural psychology to understand why teaching people what to do doesn't always help, and what you can do to make your awareness programme more effective **Why maintaining an on-prem paradigm in the cloud will not work** **Luke Hebbes,** Head of Risk and Cybersecurity, HSBC • Banks used to be about the safe storage of your money and valuables, with physical safes and cash. Now the vast majority of transactions are electronic and banks (and other FS companies) are primarily technology companies. This was a different approach and requires a different mindset • The technology isn't the same and the models don't work: addressing the switch from on-prem to the cloud • Rapid adoption of SaaS and cloud can cause issues with unstructured data. How do you provide data integrity and full lifecycle data management in the cloud and prove it to the regulators/auditors? • What in your threat model that indicates managing your own keys for a SaaS system is significantly reducing your risk? • Addressing issues that appear when moving from a quarterly release cycle to cloud technologies and agile development with multiple intra-day releases
11:40	**Identity focused security: Why start with identity when mitigating risks** **Matt Bailey,** Platform Specialist, Okta • Identity focused security and how identity is foundational to the financial services industry • Why you should start with identity when mitigating security risks • Key challenges we face today from remote working to the rise in bad actors

Agenda

12:00	**Cyber-intelligence empowering IT security audit for financial systems** **Chris Strand,** Chief Compliance Officer, IntSights • What is Cyber Threat Intelligence (CTI) and why is it important to the financial services industry • How to use CTI to prioritise financial system security gaps and enhance security posture • How your business digital footprint can help predict targeted threat patterns • Understand how to use CTI findings to accelerate risk assessment and data privacy adherence through real examples from the field
12:20	**Avoid playing whack-a-mole with your cloud security** **Joe Robertson,** EMEA CISO, Fortinet • Cybersecurity for financial institutions in the new normal must solve an equation with multiple variables, lots of unknowns, and adversaries that can pop up anywhere • Users and customers can pop up anywhere too – in a branch, in an office, at home, on the go • Ditto applications: they can move from the data centre to a cloud to another cloud, and a single query can bounce around like a pinball • This session will cover what is needed for a flexible cybersecurity strategy and how an agile and consistent multi-cloud strategy can protect you today and tomorrow
12:40	**Education Seminars | Session 2** **Centrify** **Privileged access management challenges when moving to the cloud** **Nick Colin,** Regional Sales Director – EMEA, UK&I, Centrify **LogRhythm** **Detection and response strategies for cloud security incidents** **Daniel Crossley,** Sales Engineering Manager, LogRhythm **Zivver** **How the financial services sector can benefit from secure digital communication** **Rick Goud,** CIO, Zivver
13:10	Lunch and networking
14:00	**Cybersecurity isn't just doom and gloom** **Jerome Walter,** CISO, Digital Venture, Standard Chartered Bank • Over the last 10 years, the transformation brought about by Agile development, cloud technologies and DevOps has created a number of opportunities for security to rethink and implement new cyber-hygiene strategies without slowing down the enterprise • See how the IDEAS architecture framework helps reconcile security and innovation • Exploring key metrics that help drive better organisational outcomes • How new practices are emerging to enable continuous verification and collective learnings
14:20	**Insider risk: A CISO imperative** **Rob Bolton,** Sr Director Intl at Information Protection, Proofpoint • Data doesn't lose itself. People's actions whether negligent, compromised, or malicious are #1 cause of data related breaches • Legacy tools miss early signs of data and insider risks and can't provide granular user context yet cause alert fatigue – costing firms $11.45m annually • Drawing insights from past breaches, we will explore effective pragmatic practices to mitigate exposure and insider risk across your organisation
14:40	**Banking on cyber-AI: Neutralising threats before cyber-attackers strike gold** **Mariana Pereira,** Director of Email Security Products, Darktrace • We discuss, how advanced cyber-defence technology protects the entire digital estate in high-risk environments • Learn how cyber-AI thwarted a spoofed chase fraud alert aimed at gathering information for fraudulent transactions • Discover how attackers are set to supercharge social engineering techniques with offensive AI
15:00	**Education Seminars | Session 3** **Menlo Security** **Why SASE is primed to secure the evolution of finserv** **Tom McVey,** Solution Architect, Menlo Security **OneTrust GRC** **5 steps to overcome data overload** **Nick Pavlichek,** Product Manager, OneTrust **Virtru** **Ensure true privacy in the cloud with data-centric protection** **Rob McDonald,** SVP of Platform, Virtru, and **Mark Williams,** Customer Success, EMEA, Virtru
15:30	Break and networking
16:00	**Customer digital identity in the financial services** **Martin Ingram,** Product Owner, Identity and Access Management, NatWest Group • What is a customer digital identity? • What are the benefits for both customers and the business? • How does customer digital identity change identity and access management in FS firms?
16:20	**Securing FinTech organisations** The tendency for global banks to move their infrastructure to the cloud has much of its origin in the pressure exerted by the FinTech upstarts who have revolutionised the financial services across the past decade. Finance is changing, and at the forefront of this change are digital native, cloud-first, data driven organisations. How, then, is the FinTech vanguard protecting its crown jewels? **Philip Edwards,** Director, Global Head of Security, Revolut **Tiago Rosado,** Head of Cybersecurity, Curve
16:40	**Are you cyber-insurance friendly?** **Laure Zicry,** Head of Cyber Insurance Western Europe, Willis Towers Watson • State of the cyber-insurance market • Trends in claims • Be prepared for an underwriting meeting
17:00	Closing remarks
17:05	Break and networking
17:30	Conference close

Education Seminars	
BeyondTrust **Solving the cloud identity challenge** **Karl Lankford,** Director, Solutions Engineering, BeyondTrust	Today, many financial services organisations rely on multiple cloud services with their end users regularly consuming dozens, or even hundreds, of different SaaS applications. This great cloud migration has successfully enabled the increase in remote working and is accelerating digital transformation initiatives. But, more clouds also means more challenges. In addition to the fundamental cloud security issues, there's the additional complexity and interoperability issues arising from siloed identity stores, native toolsets, and conflicting shared responsibility models between cloud providers, creating an expanded attack surface that organisations need to address. The identity challenge is the most important security problem for organisations to solve and is best accomplished by standardising the management and security controls across the entire IT ecosystem. Join this session to learn: • The most pressing cloud security risks • Where native toolsets leave gaps in security that you must address • How to implement 7 cloud security best practices with privileged access management (PAM) to vastly decrease your likelihood and scope of a cloud-related breach
Centrify **Privileged access management challenges when moving to the cloud** **Nick Colin,** Regional Sales Director – EMEA, UK&I, Centrify	Only a few years ago financial services were wedded to the perceived security and ownership of on premise infrastructure. Times have changed. Now many organisations are cloud first. However, much of the on premises infrastructure will remain for many years to come. Moreover, with multiple cloud providers often being the normal, this adds further complexity to the management and security of the entire estate. To fully benefit from rapid technological transformation, it is imperative that enterprises embrace strategies for safeguarding their infrastructure and services both during and after cloud migration. In this session, we will discuss common challenges and the tools and strategies IT and security leaders are finding most effective for managing a secure transformation to the cloud. • Managing security in a hybrid environment presents challenges that on premise vaults are not able to manage effectively • Identity remains one of the few aspects that an organisation retains control over in the cloud • Leveraging identity for effective privilege access management in the multi cloud hybrid world delivers the best blend of secure access methods
LogRhythm **Detection and response strategies for cloud security incidents** **Daniel Crossley,** Sales Engineering Manager, LogRhythm	Join Daniel Crossley, LogRhythm, Sales Engineering Manager, UK, to discover common security incidents that happen in AWS environments and gain helpful tips for detecting and responding to them. In this session you will learn: • Common security incident types in AWS • The various log types in AWS • Helpful response strategies

Education Seminars

Menlo Security

Why SASE is primed to secure the evolution of finserv

Tom McVey, Solution Architect, Menlo Security

Few industries have changed as dramatically as financial services (finserv) in the last decade. Banking and financial transactions were once an exclusively in-person process, but today the vast majority of customers conduct their financial affairs digitally. Additionally, finserv employees are highly dependent on websites and cloud or SaaS apps to perform their jobs, putting increased pressure on the security and reliability of these systems. To address the challenges presented by both a distributed workforce and accelerated digital transformation initiatives, there's a movement spurring on the adoption of secure access service edge (SASE) architecture, which assures cloud security with any new deployments.

Join this session to understand more about why this forward-thinking framework is considered key to converging the network and security functions within finserv organisations today.

What you will learn:

- Key insights and considerations on protecting employee productivity, preventing attacks, and optimising security operations for a distributed workforce
- Why the fundamentals of SASE matter to the future of networking and security
- How modern cloud-first solutions are critical to delivering on the promise of SASE security

OneTrust

5 steps to overcome data overload

Nick Pavlichek, Product Manager, OneTrust

Every organisation is working to reduce the delay between issuing a risk assessment, receiving a response, gaining risk insight, and making a risk-based decision. Risk insights quickly lose value as time elapses from the initial assessment request. Businesses should leverage the digital workstreams to collect information as updates occur using data discovery tools to find, document, and classify in real-time.

Exploring your data universe can be an overwhelming exercise, giving you more information than you know what to do within certain circumstances. Using careful data classification methods and flexible risk formulas, organisations can map information to harness real-time updates through a data discovery engine to fuel and standardise risk at scale with the latest information.

In this webinar, we'll review how you can quickly connect enterprise data through automated data discovery and translate the data into meaningful risk insights.

Attend to learn:

- Identify data across business applications for the latest risk insights
- Automatically categorise information to deliver meaningful insights across risk, compliance, and your executive teams
- Explore a new way to aggregate and standardise risk using real-time data points

RangeForce

Revolutionising cybersecurity training for your enterprise defence teams

Rupert Collier, VP Sales – EMEA and APAC, RangeForce

Continuous professional development is crucial to keeping technically focussed teams ahead of the game. CISOs, VPs and Team Leads must also be able to monitor and assess skill levels within those teams, in order to identify any possible coverage gaps that could represent a threat to the organisation. They also need to ensure incident response best practices remain fit for purpose and that everyone can execute their role in the event of an emergency.

In this seminar you will learn:

- How cyber-defenders can continue to acquire and hone their skills entirely through a browser but still in a hands-on fashion
- How they can learn essential real-world skills in real networks and real VMs. From security operations to forensics to secure DevOps, modules cover a breadth of mission-critical topics
- How users learn to defend against advanced attacks, quickly recognise and fix vulnerabilities and develop muscle memory in how best to react when it happens in the real world
- How actionable insights and metrics about performance and skill levels of team members can help identify the cybersecurity superstars, both already in your organisation and amongst those that may want to join
- How a combination of self-paced learning together with pressurised group exercises is the best way to prepare your teams for every eventuality – at a fraction of the cost of traditional learning

Education Seminars	
Red Sift **DORA: Why future proofing email security is essential.** **Dr. Rois Ni Thuama,** Head of Cyber Governance, Red Sift	The EU has recently proposed the Digital Operational Resilience Act (DORA), aimed at improving security standards within the financial sector. Scheduled to become law as early as September 2021, it means that financial entities must 'address any reasonably identifiable circumstance in relation to the use of network and information systems'. But what does this mean in practice, and will these measures really help to protect firms? In this session, Dr. Rois Ni Thuama makes the case that DORA is a force for good and will help businesses to make better decisions, faster. Dr. Rois Ni Thuama will cover: • Current cyber-threats within the financial industry • Due diligence and its positive correlation with business efficiency • Why DMARC is necessary for protecting business email
Virtru **Ensure true privacy in the cloud with data-centric protection** **Rob McDonald,** SVP of Platform, Virtru, and **Mark Williams,** Customer Success, EMEA, Virtru	There's no argument as to the benefits of the Cloud – ability to scale easily, improved productivity, heightened collaboration fuelling innovation, growth and seamless customer experience. But whatever stage of the Cloud journey you are on, one constant remains – how do you ensure that sensitive data that demands privacy – investor and banking PII, corporate IP – remains private and secure, and protected from unauthorised access (including your cloud provider) wherever it is shared and stored? Join this session to understand how by adopting a data-centric security strategy, you can protect and control access to the data itself – everywhere it travels. • Differences between traditional, perimeter-focused data security policies and data-centric protection • How to implement a data-centric strategy that supports compliance and data sovereignty needs • How to empower employees to collaborate in the cloud with seamless and secure sharing
Zivver **How the financial services sector benefits from secure digital communication** **Rick Goud,** CIO, Zivver	Organisations of all sizes have been accelerating their digital communication efforts, especially since the onset of COVID-19 and the shift to remote working. A common misconception is that digital security is complex, intricate and will require many changes in the way people work. But organisations struggle to combine security with usability, and they need both to reap the benefits of digital communication in terms of efficiency, higher customer engagement and satisfaction. • A sharing of experiences of how COVID-19 accelerated the need for digital communication, and the challenges that brings • Examples of how the right secure digital communication tools can lower your costs, increase efficiency, and improve stakeholder satisfaction • Gain insight and perspective into international financial services organisations who have successfully embraced digital communications and achieved better risk mitigation, cost control and adoption • Key takeaways: Resources to better equip yourself, your team, as well as your citizens, residents and patients in how to reap the benefits of secure digital communication both now, and in the future