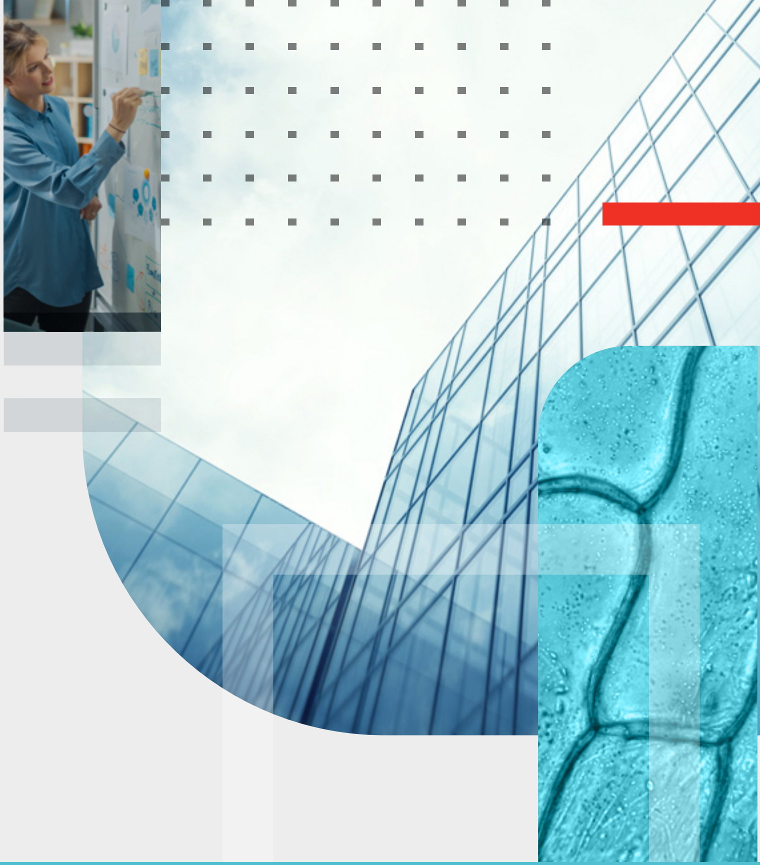
POINT OF VIEW

Fortinet Answers Burning Questions from EMEA Banking Executives on Cybersecurity Excellence



Key Highlights

- Learn how to elevate cybersecurity beyond defense, steering organizations toward strategic goals with resilience and risk management.
- Unleash a dynamic defense strategy, harmonizing efficiency with customizable layers for robust cybersecurity.
- SASE and Zero Trust enable simplicity, strength, and strict access.
- Navigate strategic cybersecurity investments, prioritizing resilience for lasting impact and organizational success.

Fortinet's experts, **Melih Kirkgoz**, Director of Systems Engineering (International Emerging Region), and **Jason Ward**, Major Account Manager (UK&I), address questions posed during the recent roundtable event titled, "Streamlining Cybersecurity: Overcoming Challenges in ZTNA Adoption and Remote Access Security."

Discover how Fortinet's solutions tackle the complexities of cybersecurity infrastructure, align with strategic goals, navigate standardization, prioritize investments, adopt SASE technologies, support Zero Trust architecture, and address the evolving regulatory landscape. Melih and Jason share their expertise on these critical topics, offering valuable perspectives on simplifying and enhancing cybersecurity for today's challenges.

Could you elaborate on how your cybersecurity solutions align with an organization's strategic goals, ensuring that our cybersecurity efforts contribute to our success?

Melih | Our solutions are designed not only to defend but to propel your organization toward its strategic objectives. By focusing on risk management, compliance, business continuity, and resilience, we align cybersecurity efforts with operational integrity, critical for client retention and market reputation. Leveraging data-driven insights, scalability, and flexibility for growth, our solutions ensure a consistent and robust security posture aligned with your organization's strategic goals.

Jason | Our approach when collaborating with clients is to focus on how our solutions can be operationalized to measurably improve their ability to Detect, Disrupt, then Investigate and Remediate against attacks. Our value is to help significantly reduce their MTTR and MTTD, ensuring they can deliver against their impact tolerance KRI and KPI's. We are asked more regularly about how we can contribute to an organization's ESG goals. An example we give is our commitment to the Environment, outlined in our 2022 Sustainability report, showcasing a 66% average reduction in product energy consumption* and 100% biodegradable packaging for the FortiGate-40/60/70F series. Further details can be found here: Fortinet Sustainability Report.

How does your approach account for standardization of products and controls while maintaining effective security measures? What's the balance between standardization and defense in depth?

Melih | Our approach is based on a multi-layered defense-in-depth strategy, balancing standardization for efficiency and consistency with customizable layers of defense. Standardization simplifies management and ensures a consistent security posture, while our solutions offer flexibility for varied and robust defense mechanisms tailored to specific network segments. Intelligent integration with existing third-party systems, training programs, and awareness initiatives complement our technological solutions.

> Our approach views standardization and defense in depth as complementary, **ensuring both operational efficiency and secure** alignment with business goals.
>
> **Melih Kirkgoz**
> *Director of Systems Engineering (International Emerging Region)*

Can you explain how your solutions prioritize cybersecurity investments that align with our strategic direction and long-term goals to ensure lasting impact?

Melih | Our approach prioritizes investments based on risk assessment, scalability, maximizing ROI, compliance, regulatory alignment, and enhancing customer confidence. By aligning closely with long-term goals and strategic direction, our solutions ensure a lasting impact, driving organizations towards a secure future. Fortinet aligns capabilities to help organizations achieve Operational and Cyber Resilience goals, contributing to cost control and supporting increased organizational Cyber awareness.

Jason | A key tenet of Fortinet's long-term value comes from our Secure Product Development Lifecycle (SDLC) approach, founded on secure-by-design and secure-by-default principles. This means our solutions are inherently robust, minimizing vulnerabilities from the outset and reducing the need for patches and updates, leading to measurable reductions in the risks of breaches, vulnerabilities, and costly security incidents.

How does your adoption of SASE and cloud-based components help in simplifying and strengthening cybersecurity, especially in ensuring strict access control and continuous monitoring, regardless of user location?

Melih | Our adoption of Secure Access Service Edge (SASE) natively integrates on-premises advanced secure SD-WAN/branch with cloud-based SSE (Secure Service Edge) components to simplify operations, providing a consistent security posture with zero trust principles. Through a unified console, streamlined networking and security operations, direct secure on-demand access, micro-segmentation, and an adaptive universal SASE framework, we ensure a cohesive and future-ready network.

> In essence, Fortinet's Universal approach creates a protective fabric around every part of your organization, ensuring **smooth operations and enhanced security**.
>
> **Melih Kirkgoz**
> *Director of Systems Engineering (International Emerging Region)*

Are your existing security solutions designed to support Zero Trust architecture? What are the key challenges and concerns in transitioning to a Zero Trust architecture, especially in a complex legacy and hybrid cloud environment?

Melih | Our solutions support the journey towards Zero Trust architecture, addressing challenges in legacy and hybrid cloud environments. They ensure compatibility with legacy systems, hybrid cloud integration, robust identity and access management, micro-segmentation, continuous monitoring, end-to-end encryption, and automated security operations. We propose a phased implementation strategy to minimize disruptions during the transition. Fortinet provides the tools, strategies, and support necessary to navigate the transition to Zero Trust architecture smoothly.

Could you provide more information on how financial institutions view Zero Trust architecture as a long-term journey and what they consider the realistic outcomes in terms of achieving zero risk?

Melih | For financial institutions, the journey to Zero Trust is incremental and strategic, aiming for enhanced security posture rather than zero risk. It involves a phased implementation, continuous adaptation, balancing security with user experience, cultural and organizational shift, strong focus on identity and access management, enhanced regulatory compliance, reduced impact of breaches, and long-term cost-effectiveness.

> Transitioning to **Zero Trust is a strategic**, long-term journey for financial institutions, significantly enhancing their security posture.
>
> **Melih Kirkgoz**
> *Director of Systems Engineering (International Emerging Region)*

How do your solutions address the regulatory landscape, especially considering regulatory authorities shifting towards embracing risk and improving resilience in the face of cyber threats?

Jason | In the UK&I, we achieve this by working with client organization's Chief Operations Function (SMF24), their teams, and extended IT ecosystem partners, helping them to assure and improve Operational and Cyber resilience capabilities, mapped to their identified Important Business Services and impact tolerance KRI, KPI's.

Our collaborative approach, value, is achieved by helping our clients securely deliver against their PRA, FCA, PSR regulatory responsibilities, while leveraging industry and sector standards best practice i.e., MITRE, NIST2, DORA, and in the UK&I including guidance from UK Finance and CMORG, the Cross Market Operational Resilience Group.

For more information, visit
Fortinet Financial Services Solutions
or take our **Cyber Threat Assessment**.

FORTINET

www.fortinet.com

December 4, 2023 4:38 PM
fortinet:Shared:CREATIVE SERVICES:EMEA Creative Server:03_DOCUMENTS:21_PointOfView-POV:2023:FSI-Q&A:2023-Q4-PoV-Q&A-FSI
2279526-1-0-EN