EQUINIX

DIGITAL PAYMENTS AND BANKING

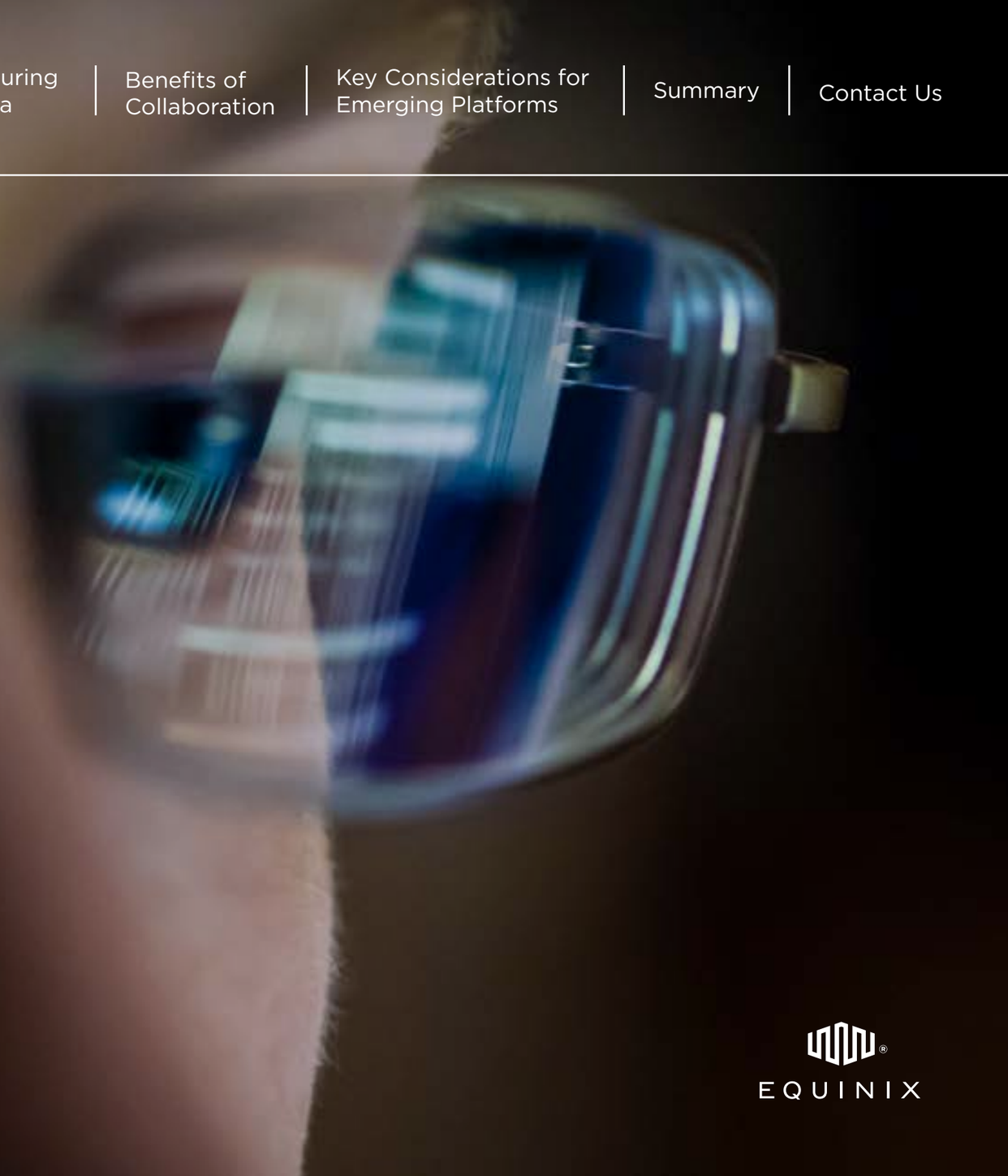
KEY TRENDS IN SECURITY RISK MANAGEMENT

Simplify and secure the digital payments ecosystem and its sensitive data

AN INCREASINGLY INTERDEPENDENT ECOSYSTEM EXPOSES NEW ATTACK SURFACES

Payment platforms remain a favorite target for attackers because of the potential monetary gains and profiting from personal information. As new players expand the payments ecosystem, the transaction chain's complexity and security risks increase.

Cyber criminals look for weaknesses across a business's entire digital platform. As workloads and capabilities shift to the cloud, the attack surface available to a hacker increases significantly.



EQUINIX

KEY TRENDS IN PAYMENTS SECURITY RISK MANAGEMENT

Expanding Ecosystems

Success in the digital economy demands an ecosystem strategy, which opens a complex web of new connections for data exchange.

The Journey to Cloud

The industry continues to drive toward cloud, both for internal transformation and to meet ecosystem partners.

Data Security

Increasing volumes of data are moving in more directions, across more counterparties—in real time and all the time, creating a crucial need for greater security.

Emerging Central Utilities

As competitive pressures force a review of core values and strategic differentiators, industry utilities are emerging to support the evolving payments, banking and commerce economies.

INNOVATION HELPS BUSINESSES TRANSFORM

Innovation is fuelling the growing payments ecosystem to bring flexibility, scalability and new ideas to a legacy industry. This includes open banking and real-time payments; new technologies like cloud, AI and APIs; and competition from new entrants.

Open Banking, Real-Time Payments

New Technologies Cloud, AI and APIs

Competition from Transformative Entrants

EQUINIX

LEVERAGE INNOVATION WITHOUT COMPROMISING SECURITY

Businesses in the payments industry need to consider how initiatives might impact the security of their digital platforms, and stay informed of security best practices as they evolve. This means:

Securing an expanding perimeter

Safeguarding with more partners to protect an ever-increasing volume of data.

Controlling access in a more dynamic network environment

Includes real-time provisioning to partners.

Restricting access to cloud applications from the public internet

Removing internet ingress and egress points eliminates a stealth option for criminal activity. Forcing all activity onto your private network provides full visibility of traffic and full control to shut down/ringfence.

Rethinking old school network practices to meet the dynamic needs of an evolving partner ecosystem

Includes real-time provisioning to clouds and scalable access as ecosystems evolve. Consider the limitations of public internet for security (DDoS and access threats), alongside your SLA requirements for stability, resilience and latency.

Colocating infrastructure to enable secure and reliable private connectivity to cloud and partners

Physical proximity—colocating technology in the same building—provides ultimate physical security, while enabling cost-effective, large-volume and low-latency data exchange via the shortest of network links. It's also crucial to evaluate your proximity to cloud ecosystems, via cloud private networks (such as Azure ExpressRoute or AWS Direct Connect).

EQUINIX

HOW CAN EQUINIX HELP?

Offer partners and suppliers a range of secure interconnection—or private data exchange—options. You can invite them to "meet me at Equinix." They can also choose to deploy their services in the same room as your stack within Equinix, so that data exchanged never leaves the building—providing the ultimate in network security.

"Simplifying the complexities of integrating the global fintech ecosystem with banks is key to the future of finance. We set out to be a key enabling component of this simplification process, as well as being there to solve the tension between security, agility and interconnection."

Nigel Verdon, CEO, Railsbank

EQUINIX

THE DIGITAL SUPPLY CHAIN

The payments value chain is evolving, thanks to a few key trends. This demands a fresh look at security practices as the volume of interfaces grows and data assets get distributed across third-party platforms.

Shifting IT from CAPEX to OPEX

Shifting to a pay-as-you-go model helps businesses better compete in the digital economy, freeing up cash to adapt investments as market trends change. This creates a more complex system to secure as data and processes are distributed across multiple providers.

Increasing openness toward XaaS (Anything as a Service)

As the industry increasingly moves core banking and payment processing off-premises, both newcomers and existing vendors are obliging with managed and SaaS solutions.

Innovative new entrants are adding value to all aspects of the payments process

This creates an expanding portfolio of partners to securely integrate and monitor. For example, there are now many solutions that support functions that include customer onboarding, faster checkout and open banking. FinTech has expanded to PayTech, RegTech and InsurTech.

This reshaping of the digital supply chain requires a fresh look at cyber risks.

That’s why making your connections secure is essential. Secure your partner interfaces and take control of data exchange with private interconnection, delivered in real time.

EQUINIX

MAXIMIZING CLOUD'S POTENTIAL WHILE KEEPING PLATFORMS SECURE

As more banks and payments providers move to cloud, they are shifting more critical workloads, like banking, risk management and analytics, there as well. These workloads, as well as traditional networking and security models, are being tested—sometimes to destruction.

The good news is there are proven architectures for hybrid multicloud solutions. Clouds offer the private networking needed to overcome security and performance concerns associated with the internet.

Clouds connect with a new network model

Payments and banking rely heavily on a combination of internet and traditional network carriers; however, both routes are reaching their natural limits in a cloud-enabled world. The internet has no SLA, poor QoS and a large attack surface. Traditional telecommunications companies have the SLA, but are slow to deploy, killing agility and economics. Connecting cloud platforms securely requires a new networking model that marries the agility and economics of internet with the robustness of traditional telecommunications companies: private cloud networks such as MSFT Expressroute and AWS Direct Connect, available on demand via cloud exchanges across the globe.

Cloud exchanges are the new network

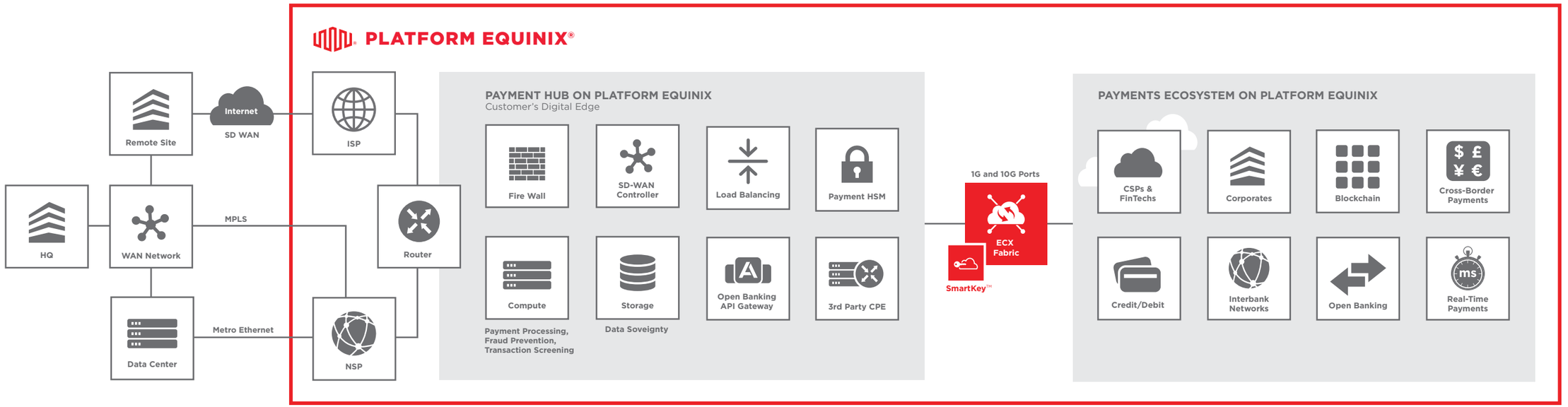
Cloud exchanges offer highly secure, low-latency, real-time connections to your applications and partners across any cloud. They also provide software-defined networking to match your software-defined future services, including routing between clouds, reaching partners or preparing for failover needs. Dedicated private connections ensure production-quality solutions, available on demand, on a pay-per-use basis, via a user-friendly GUI.

EQUINIX

Overcome the limits of virtualization at the edge of cloud

Not all platform elements are cloud-ready today, perhaps due to demanding industry standards or being too complex to shift. For example, a common infrastructure element in the payments card industry which cannot be virtualized is the payment HSM.

As payment applications transition to the cloud, components will force firms toward a hybrid cloud strategy, and a need for an on-premises private home operating alongside the public cloud. Securing data exchange and the need for a tight network SLA that avoids payment transaction time-outs, means the natural “on-prem” home is at the edge of the cloud private networks.



EQUINIX

SECURING DATA WITH A DISTRIBUTED PLATFORM ARCHITECTURE

Data continues to grow exponentially, while APIs and financial services regulations are supporting the movement of data in more directions, across more counterparts in real time, all the time. Increased exposure of sensitive data must be carefully managed to minimize regulatory and reputational risk.

The payments industry employs multiple methods to protect sensitive data.

Examples include point-to-point encryption encryption of data stored at rest and tokenization by turning a key piece of data (e.g., an account number) into a random string of characters that has no meaningful value if breached.

Optimize your platform's performance and security with distributed control points.

As expanding ecosystems and the growth of outsourcing create increasingly distributed platforms, decentralized architectures can reduce attack surfaces. By creating distributed control points (close to people, partners and customers), you can optimize your platform's performance and security.

EQUINIX

DISTRIBUTED CONTROL POINTS ENABLE:

Regional Data Hubs

To meet sovereignty and compliance demands for localization.

Localized Security Services

Where you need them—close to your distributed applications for visibility and performance.

Cloud integration

For your applications, and connection capabilities to deliver hybrid and multicloud payments services to users.

"Security services need to be in close proximity to today's increasingly distributed platforms and applications so that they may best safeguard data integrity and sovereignty, ensure compliance with an evolving set of local, national, and international regulations, and maintain consistent policies across dispersed applications and infrastructure."

John Morgan, Vice President and General Manager, Security, F5 Networks

---

EQUINIX

HOW CAN EQUINIX HELP?

Leverage a global platform with access to a growing ecosystem of security partners to support your decentralized security hubs. Equinix is a global leader for cloud and network access for ultimate visibility.

Equinix SmartKey® is a unique HSM as a Service that provides secure key management to protect data in public, private, hybrid or multicloud environments, simplifying provisioning and control of encryption keys. This enables a service-based approach to key management to support use cases such as point-of-sale point-to-point encryption, signature and verification of digital wallets and much more.

SmartKey®

EQUINIX

CENTRAL UTILITIES—MAKING SECURITY STRONGER, TOGETHER

Financial services and commerce face increasingly sophisticated threats that require fresh responses. Where common industry needs exist, collaboration will enable mutual benefits and efficiency gains.

While data represents a core asset to any firm, and security remains a highly individual endeavor, where could shared utility services emerge, and what would be key to their success?

For example, criminals are quick to move money across sophisticated channels. A whole-market view, leveraging shared data, enhances the ability and speed of identifying patterns and malicious activity.

"Collaboration is key to detecting fraudulent activity because fraudsters are not brand loyal. We see an overlap of more than 35% between the fraud cases of our community members. Therefore it is highly likely that emerging fraud services within the digital payments ecosystem will have a foundation in shared data for the benefit of the entire community—to improve fraud detection, faster."

Maarten Alleman, CEO, Perseuss

EQUINIX

USER IDENTIFICATION AND AUTHENTICATION IS STRENGTHENING SECURITY FOR PAYMENTS AND BANKING

This encompasses digital identities for humans as well as device identity to enable viability of large-scale IoT ventures.

Various technologies and specialist players will play a role, and it's clear that future cybersecurity and cyber resilience will rely on layers of technology and an ecosystem of experts.

Scale will be a prerequisite to success, so we can expect consortia to emerge from industry associations (such as Perseuss, emerged from the travel industry and IATA), and clusters of significant banks (such as BankID in Sweden). Will we also see governments play a role?

Watching this collaborative space for new services and being ready to engage and leverage shared knowledge will be central to managing risk.

CRITICAL CONSIDERATIONS FOR EMERGING UTILITY PLATFORMS

Neutrality

A private, secure environment where industry data can be aggregated.

Accessibility

Ease of access for all ecosystem participants.

Real-time capability

Speed of data access and analysis is critical to detecting malicious activity as close to the source as possible.

Tools

Access to cloud technologies and analytics tools, enabling partners and expertise.

Next-generation data marketplace solutions

Enablement for third parties to access and interrogate your data, in your own environment.

EQUINIX

HOW CAN EQUINIX HELP?

3,020+
Enterprises

2,900+
Cloud & IT providers

340,000+
Interconnections

1,800+
Network service providers

As the global market leader in colocation and interconnection services for the financial industry, collaboration is flourishing on Platform Equinix. Interconnect with the largest ecosystems on our global platform.

EQUINIX

COMPLEX ECOSYSTEMS NEED NEW SOLUTIONS TO STAY SECURE

In an age of digital disruption, implementing fresh solutions is necessary for growth and scalability. However, security should also be at the top of any payments company's agenda.

The payments and banking industry is subject to:

High Regulatory Scrutiny

Targeted Cyberattacks

Increased Data and Management of IoT

Private interconnection, hybrid cloud solutions and distributed control centers can protect your growing volumes of data in a highly distributed world.

EQUINIX

PROTECT AND CONTROL YOUR DATA

In an increasingly interdependent payments ecosystem, it's critical to manage the complexity and security of transaction chain risks. Secure your connections and partner interfaces with private interconnection, hybrid cloud solutions and digital control points.

To find out more about how interconnection can help

Contact us

Payments Security eBook_EN | 8534 | vMarch 24, 2020 9:16 AM | 0320 | Q418

EQUINIX