Growing Role of Platforms in Cybersecurity

Eric G. Troup

ABSTRACT

Platforms are becoming a dominant force in business and software architecture. Regardless of where you look across commercial, government, health or military/defense sectors, platforms are increasingly becoming core features of the digital world. They are at the center of digital ecosystems.

When we think platforms today, it is important to realize that there is a business view, a technology view, and an ecosystem view. Evolving from highly specialized and expensive Service Delivery Platforms, today these multi-tenant and multi-role platforms provide reusable sets of building block capabilities designed to accelerate the growth and to sustain multiple digital ecosystems.

Increasingly today, the technology platform implementation is cloud based and software defined. Furthermore, the cloud infrastructure itself is becoming a commodity. Highly virtualized cloud platforms are dominating because of their huge advantages in automated hyper-scale resource utilization efficiency. The economies of scale are overwhelming.

Platforms enable many important software tasks that would formerly have had to be custom built into each system or application to be accomplished much more effectively by the reusable capabilities provided by the platform. For example, an identity management system provided by a cloud platform can meet the individual needs of hundreds of different services and systems hosted on or accessible via that platform. Thus, by their very nature, platforms are subsuming many of the cybersecurity roles that were formerly performed by individual systems or applications.

The increasing role of platforms requires adjustments to system architecture but, properly approached, offers significant enhancements to cybersecurity. The marketplace recognizes this: *CIO Insight* reported, "52% of (survey) respondents believe cloud apps are as secure, or more secure, than on premise applications, up from 40% last year." [1]

Eric Troup is Chief Technology Officer for Worldwide Communications and Media Industries, Microsoft Corporation. As the lead industry technology strategist for the Telecom, Cable and Media sectors, Mr. Troup is responsible for influencing the evolution of a growing ecosystem of enterprise solutions for customer and resource management, data analytics, and service orchestration across cloud platforms, software defined networks and devices. He held a variety of leadership positions in the U.S. Army before joining NYNEX in 1985. He held management positions at Unisys and Cap Gemini before coming to Microsoft Consulting Services in 2004.

Mr. Troup earned a Bachelor of Science (BS) degree from West Point, received a Master of Business Administration (MBA) from the University of Utah and is a graduate of the U.S. Army Command and General Staff College. He was the first individual recipient of the NYNEX Chairman's Award and is a TM Forum Distinguished Fellow.

Platforms and the Digital World

In *Platform Revolution,* the authors define a platform as "a business based on enabling value-creating interactions between external producers and consumers." [2] In the continually evolving digital era, platforms are causing some important shifts in focus. We are evolving from monetizing by selling a right-to-use license of a hard-to-make competitive service or capability towards extracting smaller pieces of the recurring value from each of the massive numbers of interactions between producers and consumers in digital ecosystems.

As explained in *Platform Revolution*, the model for valuation of platforms becomes a function of the number of producers and consumers across a network provided the platform itself retains an ability to curate content and moderate network interactions. The focus thus shifts outwardly towards these interactions in a network effect between producers and consumers rather than inwardly on something being produced or licensed by the platform owner. In some cases, items being produced are provided free of charge to not impede growth of the new monetization process. These shifts fundamentally alter the cybersecurity threat surface.

Digital Platform Reference Architecture

Industry groups have been working on standards and best practices for implementing and operating digital platforms and for joining digital ecosystems. The TM Forum [3], in liaison with NIST, ETSI, ITU and Industrial Internet Consortium (IIC) has been evolving its Frameworx [4] to address the needs of digital platforms and digital ecosystems. As part of this effort, the TM Forum is evolving a Digital Platform Reference Architecture (DPRA).

As shown in Figure 1, a Digital Platform has to be understood from both a business and a technology viewpoint. This separation of concerns makes it much easier to understand how to deal with fundamental requirements such as cybersecurity.

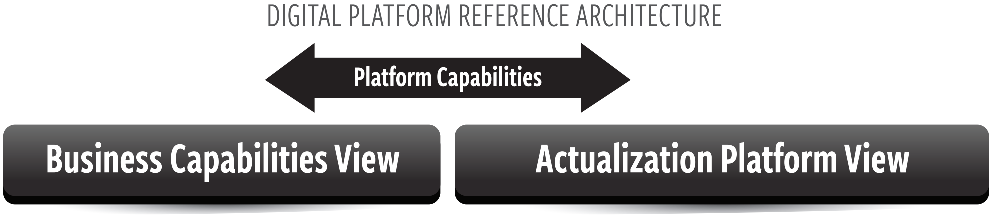
DIGITAL PLATFORM REFERENCE ARCHITECTURE
Platform Capabilities
Business Capabilities View
Actualization Platform View

Figure 1. TM Forum Digital Platform Reference Architecture contains a Business Capabilities.

Figure 2 contains an expanded and modified view of the current work-in-progress TM Forum DPRA based upon a recent Microsoft contribution. Microsoft Azure is a commercial example of a platform supporting multiple ecosystems across commercial, public/government, health and defense sectors. The platform provides sets of reusable building block capabilities or services that can be used to create higher-level services. Some of these building blocks can come from the platform maker (First Party services) while others could have been developed by others and exposed via the platform to a community (Third Party services). The Technical Capabilities depicted are an illustrative list and constantly evolving.

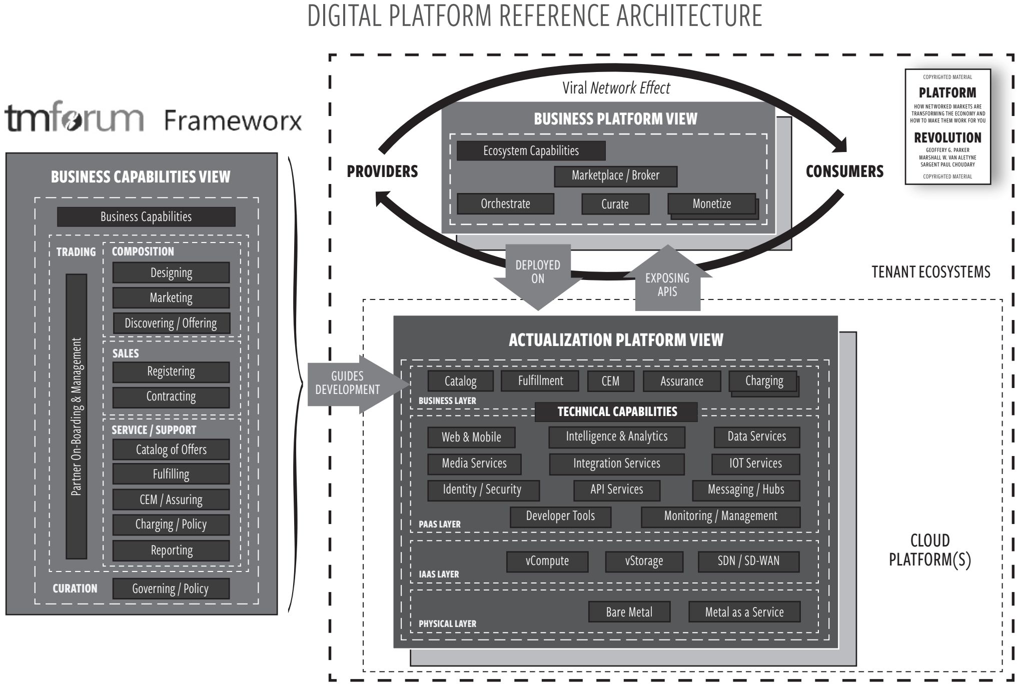

Figure 2. Modified TM Forum Digital Platform with Microsoft Azure adapted Actualization Platform View.

In this context, Uber is a Business Platform with car owners/drivers as providers and travelers being the consumers. It is deployed onto an Actualization Platform.

Microsoft Azure is primarily an Actualization Platform that hosts many Business Platforms; it is multi-tenant yet secure. It is always important to understand which point of view of the platform is being discussed.

The Actualization Platform View makes it easier to visualize the cybersecurity issues across the physical datacenter/network layer, virtualized infrastructure layer, the platform services layer, and business application layer. Each have specific functions to perform as a part of a layered cybersecurity defense.

Distributed Computing /Mobile Edge Computing

Another characteristic of digital platforms is that the services and supporting cloud/ network infrastructures are increasingly geographically dispersed. As shown in Figure 3, digital platforms invariable involve chaining together resources hosted across multiple datacenters and devices. Instead of mostly static linear value chains, we have an overlapping value mesh designed to be agile in construction and provide low-latency at the edge. In this context, devices become a part of the platform and thus an integral part of nearly any cybersecurity strategy. Workload placement across the fabric becomes part of the optimization process of highly-automated, close-looped management systems.

DIGITAL PLATFORM REFERENCE ARCHITECTURE

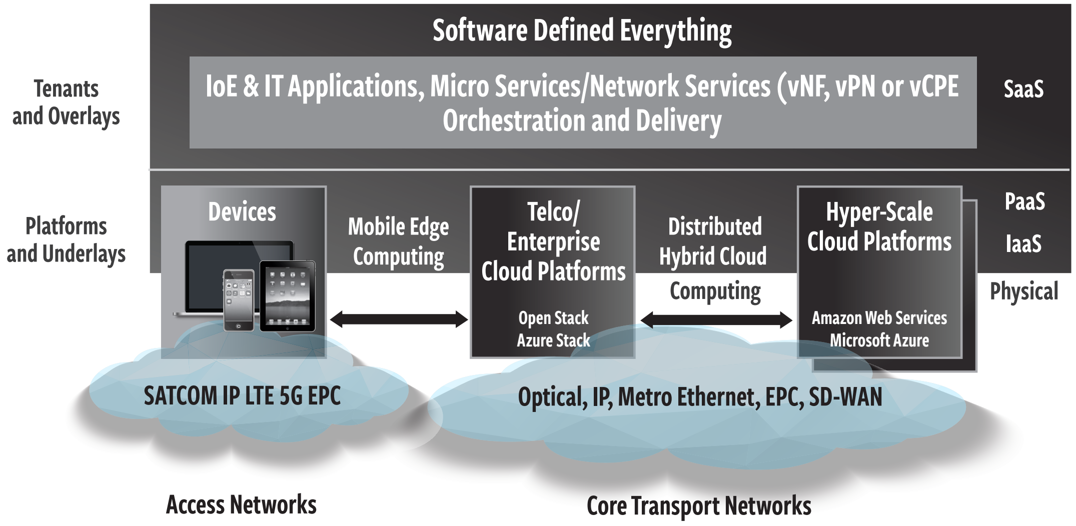
Software Defined Everything
Tenants and Overlays
IoE & IT Applications, Micro Services/Network Services (vNF, vPN or vCPE Orchestration and Delivery
SaaS
Platforms and Underlays
Devices
Mobile Edge Computing
Telco/ Enterprise Cloud Platforms
Open Stack
Azure Stack
Distributed Hybrid Cloud Computing
Hyper-Scale Cloud Platforms
Amazon Web Services
Microsoft Azure
PaaS
IaaS
Physical
SATCOM IP LTE 5G EPC
Optical, IP, Metro Ethernet, EPC, SD-WAN
Access Networks
Core Transport Networks

Figure 3. Cloud Platforms are geographically distributed for performance and regulatory reasons. This means that platforms must have built-in 'native capabilities' for distributed cloud platform and ecosystem management including cyber-security. They also must be able to gracefully accommodate different security and privacy requirements that may vary by context, country, industry, and tenant.

Platform Workload Types

Digital platforms can also be represented as falling under three fundamental business scenarios for cloud platforms:

1. Internal IT Workloads such as line of business applications, business support systems, operations support systems supporting an organization's internal requirements.
2. External IT Workloads such as hosting the workloads of external organizations and to implement B2B and/or B2B2C use cases.
3. Internal Network Workloads such as those associated with Network Function Virtualization (NFV), Software Defined Networking (SDN) and Software Defined Wide Area Networking (SD-WAN).

The third category is the newest use case. The telecom and data communications industry is in the midst of a massive $150+ billion worldwide transformation to build a network of cloud based platforms to dynamically host the virtualized network functions that implement and manage the connectivity of people, devices, applications and data leveraging 5G Wireless and IP Evolved Packet Core (EPC) technologies. Eventually all datacenters and networks will not simply employ virtualization but become cloud platforms differentiated only by the nature of the workloads primarily hosted.

> The correct level of cybersecurity will always be a judgment call—but one needs to understand the risks and impacts involved.

As a result, there will be virtually no business scenarios where mission critical data is not flowing across software defined datacenters (clouds) and software defined networks (clouds) invoking allocated resources many of which may not be entirely under the control of any one party.

Having set the stage, let us now look at some cybersecurity principles for digital cloud platforms.

Cybersecurity as a Core Platform Feature

Within the TM Forum, the discussion has begun to shift to Ecosystem Risk Management—addressing the collaborative risks resulting from virtualization and cloudification across an Open Digital Ecosystem. The word "*Open*" here means "*easy to find and consume*"—not vulnerable or free.

While organizations like to believe they have a handle on their own risks—those they own and physically control—increasingly the delivery of a service/product is reliant on a web/ fabric of partners over whom they have less control but have to trust if they are to operate and deliver in this agile new world.

A risk approach was adopted at the TM Forum primarily because members believe there is never a 100% solution to security and any investment in security needs to be appropriate for the value of that being protected. The correct level of cybersecurity will always be a judgement call—but one needs to understand the risks/impacts involved.[5]

On the other hand, for hyper-scale Azure, Microsoft is finding that the costs of providing extensively differentiated levels of cybersecurity is not cost effective and in fact introduces other risks. It is safer to simply provide many of the essential cybersecurity features consistently across the entire Azure ecosystem.

To play in a specific industry environment may require adherence to certain specific security criteria/ standards. When a platform achieves certifications such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS, specific cybersecurity capabilities must be met by that platform.

Security and Privacy Must be Embedded into All Aspects of the Platform

For a cloud platform provider like Microsoft, security and privacy is a priority at every step. For this reason, Microsoft designs its platform and tenant software for security from the ground up. A specific approach known as the Security Development Lifecycle (SDL)[6] is followed. This company-wide, mandatory development process embeds security requirements into the entire software lifecycle, from planning through deployment. To help ensure that operational activities follow the same security priorities, Microsoft has developed rigorous security guidelines laid out in an Operational Security Assurance (OSA)[7] process. When issues arise, a feedback loop helps ensure that future revisions of OSA address them.

Platforms are increasingly able to provide very robust security protection perimeters but they can never be totally impenetrable.

Security must be able to first protect from and then detect threats. Platforms are increasingly able to provide very robust security protection perimeters but they can never be totally impenetrable. Platforms need to supplement protection with efficient and fast reacting detection mechanisms. Passive and active countermeasures can then mitigate and defeat threats. In some cases, intruders can be sent to honey pots (false data) while then activating cybercrime law enforcement or cyber-warfare counter measures.[8]

Consumer Privacy is another aspect to the cybersecurity regulatory challenge. Over the past year, the TM Forum has focused on privacy as driven primarily by EU legislation (general data protection legislation GDPR) which focuses on giving citizens control over their data and places requirements on organizations collecting data to handle it appropriately (protection, access, etc.). Some of the privacy requirements can be very onerous and their implementation can conflict with certain other certification requirements. Nonetheless, data protection across its lifecycle is critical.

Keeping Customer Data Safe

Hyper-scale cloud-based platforms utilize a robust set of security technologies and best practices including multi-tenant cloud virtualization. These are essential to ensure the cloud platform infrastructure is resilient to attack, safeguards user access to the environment, and helps keep customer data secure. Some specific cyber-security capabilities present on mature, cybersecurity enabled platforms like Microsoft Azure include:

Managing and controlling identity and user access to environments, data, and applications by federating user identities and enabling multi-factor authentication for more secure sign-in. Biometric capabilities on devices such as fingerprints or artificial intelligence enhanced facial recognition enable stronger identity and role-based security.

Encrypting communications and operation processes. For data in transit, use of industry-standard transport protocols between user devices and datacenters and within datacenters themselves. For data at rest, a wide range of encryption capabilities up to AES-256, giving the flexibility to choose the solution that best meets each need.

Securing networks. Infrastructure necessary to isolate tenants and to securely connect virtual machines to one another both with within one datacenter (such as with Clos VL2) [9] and between multiple networked datacenters as in hybrid cloud use cases. Capability to block unauthorized traffic to and within datacenters, using a variety of technologies. Software Defined Virtual Networking to extend on-premises networks to the cloud through site-to-site VPN.

Managing threats. To protect against online threats, offers such as anti-malware for cloud services and virtual machines. Robust intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the platform. [10]

Protecting the privacy of Customers. Time-tested approaches to privacy and data protection including maintaining organizations' ownership of and control over the collection, use, and distribution of their information.

Owning your own data. Customers own customer data—that is, all data, including text, sound, video, or image files and software. Owners should be able to access their customer data at any time and for any reason without assistance. Customer data or derive information from it should not be used for advertising or external data mining without consent.

Trust in the Rule of Law for responses to government and law enforcement requests to access data. When a government wants customer data—including for national security purposes—it must follow the applicable legal processes, in the applicable jurisdiction when serving a court order for content or a subpoena for account information.

Platforms are Strengthening Cybersecurity and Privacy

There are fundamental economic and technical reasons platforms represent such an important force in information technology evolution today. Most people think of the massive network scale required by digital systems today in order to achieve meaningful impact or economic success. To avoid high up-front capital costs, cloud computing platforms are a key enabler to failing fast, adjusting and then achieving successful business growth.

> Platforms, particularly those of hyper-scale, are increasingly in the best position to be able to innovate in cybersecurity.

It takes enormous investment to achieve rigorous adherence to standards for certification or best practices in such mundane areas like cybersecurity. However, cyber breaches represent a very serious and growing threat. As many businesses and government agencies have discovered over the past few years in a series of embarrassing and costly breaches, the threat is very high and growing. The cost of preventing and mitigating has become so significant that most organizations are simply not able to deal effectively with the challenges of a constantly evolving worldwide theat. Having a data center on premise has little to do with securing against cybersecurity threats.

Platforms, particularly those of hyper-scale, are increasingly in the best position to be able to innovate in cybersecurity and maintain on a continuous basis, the necessary large investments. With their huge scale, the larger platforms are much better able to maintain state of art capabilities and invest in costly cybersecurity operations centers equipped with high end, real-time data analytics capabilities and automated artificial intelligence enhanced mitigation capabilities. These costs can be distributed across an increasingly larger customer base.

For essentially the same reasons platforms dominate economically, platforms also enhance cybersecurity. All platform tenants benefit from a much higher level of protection than they could likely secure on their own allowing tenant owners to safely focus more on core businesses. Platforms and the networking of platforms will likely continue to be important to the cybersecurity conversation.

NOTES

[1] CIO Insight, http://www.cioinsight.com/it-strategy/cloud-virtualization/slideshows/cloud-apps-rise-despite-cloud-security-concerns.html.

[2] Geoffrey Parker, Marshall Alstyne, Sangeet Choudary, *Platform Revolution,* New York: WW Norton, 2016.

[3] TM Forum, www.tmforum.org.

[4] TM Forum Frameworx https://www.tmforum.org/tm-forum-frameworx – a suite of best practices and standards that provides the blueprint for effective, efficient business operations leveraging proven service-oriented approaches for flexible and agile end-to-end management of services across complex, multi-partner environments.

[5] Content in these two paragraphs contributed by Chris Stock, Director Security & Privacy Programs, TM Forum.

[6] Microsoft Security Development Lifecycle (SDL); https://www.microsoft.com/en-us/sdl/default.aspx.

[7] Microsoft Operational Security Assurance (OSA); https://www.microsoft.com/en-us/SDL/OperationalSecurityAssurance/.

[8] Content in this paragraph contributed by Michael Lawrey, Director TM Forum, previously Executive Director at Telstra.

[9] Clos network is a kind of multistage circuit switching network, first formalized by Charles Clos in 1952.

[10] For additional insights into the level of sustained cyber security investment required see; “Microsoft Announces new Cyber Defense Operations Center, Enterprise Cybersecurity Group; https://blogs.microsoft.com/firehose/2015/11/17/microsoft-announces-new-cyber-defense-operations-center-enterprise-cybersecurity-group/#sm.0001o8vmmz1cold49y-m514udg8bnw and http://blogs.microsoft.com/blog/2015/11/17/enterprise-security-for-our-mobile-first-cloud-first-world/#sm.000001annxgeojffrx8nvbknohw9x.