Next-generation Security for Modern Enterprise in the Digital Era: Distributed Integrity, Scalability, and Optimization

Steffi Han, Research Director
June 2019
Innovating in the Digital Economy
Chapters of the 3rd Platform

Platforms & Communities
“Innovation @ Scale”
- AI
- IoT
- Blockchain
- Natural Interfaces

Autonomous Systems
“HyperComplexity @ Scale”
- Exponential AI
- Quantum Computing
- BioDigital Integration

New Technologies & Delivery Model
“IT Access @ Scale”
- Cloud
- Mobile
- Social
- Big Data

We Are Here

2007  2015  2023  ...

EXPERIMENTATION

MULTIPLIED INNOVATION

AUTONOMY
Multiplied innovation is enabled via digital mashups, which are combinations of 3rd Platform techs and Innovation Accelerators.

5G is an enabler of digital mashups in that it is the connectivity platform for next-generation innovations such as AR/VR, robotics, wearables, mobile devices, and the IoT, and 5G vision goes well beyond just people, connecting devices in various sectors.

With the evolutionary path to 5G, the appeal of edge computing is rising, driving the shift from centralized to distributed architectures.
3rd Platform Adoption and Multiplied Innovation Will Drive Security Complexities

- Death of the Perimeter
- Distributed IT/Cloud
- Sophistication of Attacks
- Growth of Compliance
Distributed Cloud: Everywhere for Everything..

By 2021, we’ll see a cloud world that is...

$565B

20% at the edge

over 15% specialized

over 90% multicloud
Placing an **architecture closer to the edge** relieves the burden of increased congestion in core networks due to fast-paced growth of internet traffic from websites, apps, APIs, online video, and IoT devices, as well as the rapid uptake of emerging techs such as blockchain.

**Distributed integrity** (zero-trust) approach can offer adaptive access to corporate applications across the digital ecosystem, VPN-less secure access to corporate applications without corporate network access, application microsegmentation, and cloud-based threat protection.

**Security as a service** is an efficient and cost-effective way of adding new features and capabilities to core, on-premise technologies while minimizing complexity. Security as a service can enhance the security agility of large IT organizations.
Key Security Themes: Marginalized perimeters create new control points

- Buzzwords = Software Defined Perimeter, Microsegmentation
- Death of the perimeter
- Cybersecurity investments coalescing around four central control points as network- and perimeter-centric security measures become more permeable:
  - Identities
  - Applications
  - Data
  - Endpoints
- Distributed integrity is a function of moving up the stack, away from defined endpoints and networks towards security anywhere of data as it is used by identities and applications.
  - The endpoints (incl. servers) operate at a slightly lower, often more physical layer of the infrastructure.
Key Security Themes: Identity still a security cornerstone

- Buzzwords: Zero Trust, Digital Trust, Trust Crisis
- Integration of identity context into digital transformation initiatives to improve the inherent integrity of digital interactions, reducing the reliance on network security and enabling security measures at the data and application levels.
- Digital trust enables the decisions made between two or more entities that reflect their level of confidence in each other; these decisions are based on each entity's digital reputation as well as the assurance levels provided by each entity's cybersecurity programs.
  - Note: Digital trust operates at a higher layer than zero trust (distributed integrity) which is about allowing users access to resources in real-time. Conversely, digital trust is about making decisions about who should be your business partner.
Key Security Themes: Data collection beyond logs

- Buzzwords = Network traffic analytics
- Artificial intelligence and machine learning are tools that are be used to improve our security efficacy. Analytics, however, are constrained by data.
  - Security professionals are inject as much information as possible, grabbing previously unused data.
  - Logs plus metadata including netflows, packet header information, full packet capture, endpoint telemetry
- Everything in real time
  - No security teams have time to look at old logs
  - Forensic evidence delivered expeditiously to response units
Key Security Themes:
Data privacy regulation drives security and compliance workflows

- **Buzzwords** = GDPR, CCPA, PIPEDA, Right to be Forgotten, Data Portability, Pseudonymization, De-identification, crypto-agility

- **Distributed Data Fuels Complexity**
  - Organizations are updating fragmented, outdated and poorly maintained crypto implementations in favor of centralizing key management or key management as-a-service offerings.

- **Emerging Data Security Platform**
  - Endpoint and network security components are being integrated to support data discovery, classification, rights management, and file access monitoring capabilities. Telemetry from those solutions, combined with intelligence from backup and recovery, antimalware and other endpoint security solutions will enrich security analytics engines and improve threat detection and rapid response.

- **Addressing Data Privacy Compliance**
  - Increasing emphasis on information governance workflows and discovery. Technologies are emerging to optimize compliance-driven processes such as intake, management, and completion of data subject access requests.

- **Addressing Data Sovereignty/Residency Requirements**
  - Enterprises that need to move data across the globe within their organization can address this issue with investing in creating corporate binding rules that must go through a government approval process.
"Technology is changing work as we know it. This impacts organizations' culture, required skills, the way talent is sourced, the workspace, and the nature and makeup of the workforce itself."

Driving Fundamental Changes in the Workplace

1. Artificial intelligence (AI), robotics, and intelligent process automation software automating work
2. Human/machine collaboration
3. The role of the digital worker
4. New work categories created; reskilling

CULTURE

1. Talent sourcing, management and development
2. Employee FoW metrics, including key behavioral indicators (KBIs)
3. Employee experience
4. Organizational structure

SPACE

1. Space redesign and working facilities
2. Mobility and immersive experience
3. Productivity and collaboration
4. Security and trust

FORCE

>50% of the AP workforce by 2020 will be millennials

11
Reimagining the Future of Work: The Future IT view

Outcomes
- Productivity
- Commerce
- Superior Experiences
- Collaboration
- Innovation
- Personalization

Enablers
- Users
- Device
- Things

Unified Computing Management
- Apps
- APIs
- UCaaS
- Bots/Voice
- AR/VR
- 3D printing

- Analytics/AI
- Cloud/Hybrid
- Intelligent ERP
- Software-Defined
- Digital Trust and Security

Top Challenges Cited by IT Decision Makers
1. Security
2. Integration With Legacy Systems
3. Lack of Skills, Resources

Source: IDC AP Future of Work Practice, 2018
Key Takeaways

- DX Causing an Exponential Jump in Complexity
- As 5G progresses, the edge computing would be rising, driving the shift from centralized to distributed architectures
- New security features are embraced, including distributed integrity, closer to the edge, and as a Service, in the DX era.
- Technology is rapidly changing work as we know it, leading to the Future of Work, and this changing paradigm requires the Next Gen Security
Thank you!

Steffi Han
Research Director
shan@idc.com

www.idc.com