HCL

21ST CENTURY CYBER SECURITY FOR MEDIA AND BROADCASTING

THE AGE OF DISRUPTION:
THE AGE OF CYBER THREATS

While the digital era has brought with it significant advances in technology, capabilities and experiences, it has also opened the doorway to continuously evolving threats, stringent IT governances and compliances, and cloud service adoption. With sensitive data being collected, processed, and disseminated within the infra and cloud environment, it is imperative to implement robust network and infrastructure security—leveraging greater depth and breadth of knowledge, toolsets, and other resources. This onset of the new breed of cyber attacks over the time stands as a grim reminder that the organization's IT requires the expertise and resources to assess and enhance network and infrastructure security.

DEALING WITH RANSOM THREATS FROM HACKERS?

Facing violation of your media rights through piracy in media value chain or customer end?

Tackling with illicit rebroadcasting of your content across geos?

Is your social media site and webpage being hijacked?

Is your content protected against theft or alterations?

IS YOUR INFRASTRUCTURE SECURE ???

Protect your media Infrastructure Components.

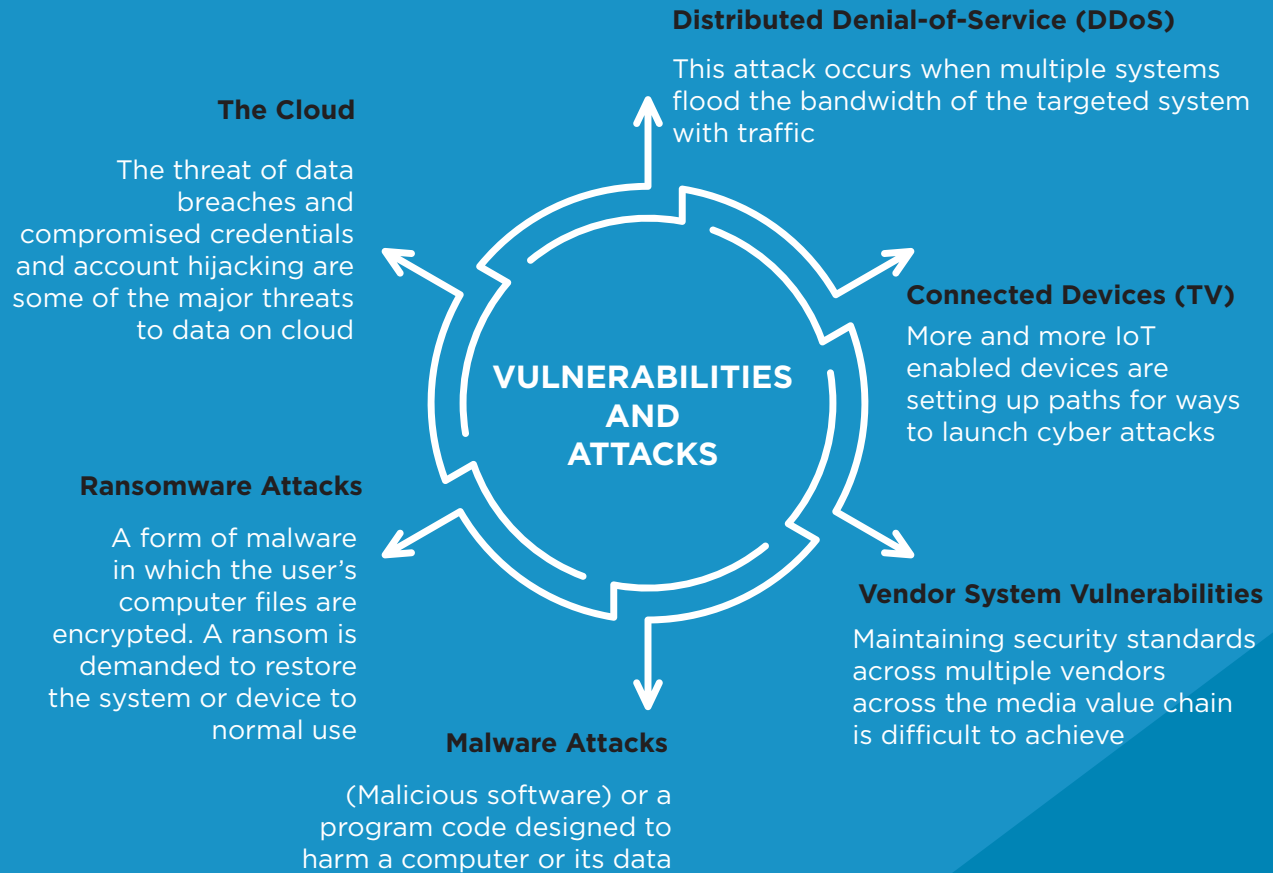| Production & Distribution Networks	Digital & IoT Devices
Multiple Media Platforms	Media Stonage Locations

IS YOUR INFORMATION SECURE ???

Information protection across media value chain

Digital Media Content	Media Software Application
Social Media Sites	Email and Webpages

CYBERSECURITY THREAT IS REACHING A TIPPING POINT IN MEDIA AND BROADCAST INDUSTRY

During The Digital Broadcasting Symposium 2017, various vulnerabilities and threats were identified that need to be addressed to combat cyber attacks:
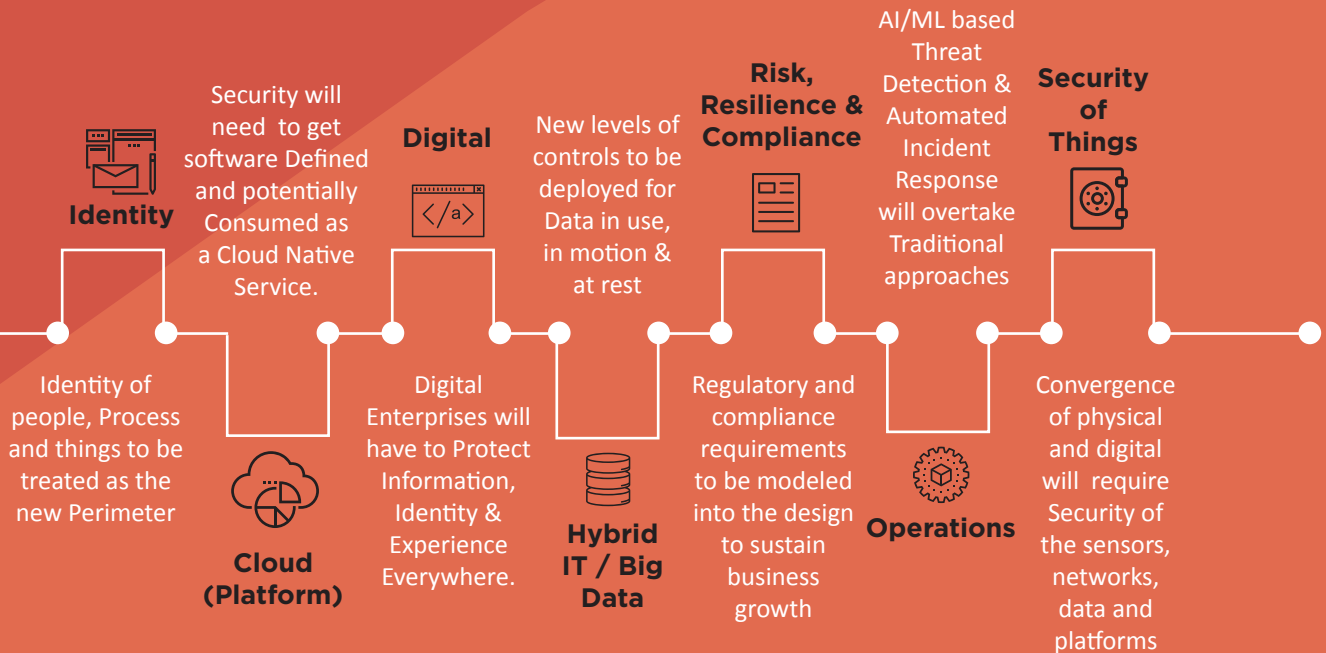
Distributed Denial-of-Service (DDoS)

This attack occurs when multiple systems flood the bandwidth of the targeted system with traffic

The Cloud

The threat of data breaches and compromised credentials and account hijacking are some of the major threats to data on cloud

VULNERABILITIES AND ATTACKS

Connected Devices (TV)

More and more IoT enabled devices are setting up paths for ways to launch cyber attacks

Ransomware Attacks

A form of malware in which the user's computer files are encrypted. A ransom is demanded to restore the system or device to normal use

Vendor System Vulnerabilities

Maintaining security standards across multiple vendors across the media value chain is difficult to achieve

Malware Attacks

(Malicious software) or a program code designed to harm a computer or its data

Over 30% of Media and Broadcasting companies admit to having experienced a cyber attack of some type or other.

SOME RECENT AND PROMINENT CYBER ATTACKS

BUILD ENTERPRISE CONFIDENCE THROUGH A FUTURE-PROOF CYBER SECURITY ARCHITECTURE

To be a 21st century media and broadcasting enterprise, companies need to address and enable major industry shifts in the following areas:

Identity

Identity of people, Process and things to be treated as the new Perimeter

Cloud (Platform)

Security will need to get software Defined and potentially Consumed as a Cloud Native Service.

Digital

Digital Enterprises will have to Protect Information, Identity & Experience Everywhere.

Hybrid IT / Big Data

New levels of controls to be deployed for Data in use, in motion & at rest

Risk, Resilience & Compliance

Regulatory and compliance requirements to be modeled into the design to sustain business growth

Operations

AI/ML based Threat Detection & Automated Incident Response will overtake Traditional approaches

Security of Things

Convergence of physical and digital will require Security of the sensors, networks, data and platforms

By adapting to and evolving with constant changes in the technology and threat landscape, media companies can overcome the growing security challenges and inspire business confidence.

GET THE 360-DEGREE CYBER SECURITY ADVANTAGE WITH HCL

HCL partners with you from the time of media content creation to consumption across the security journey

STRATEGY, ARCHITECTURE & CONSULTING SERVICES

TRANSFORMATION AND INTEGRATION SERVICES

MANAGED SECURITY SERVICES

Through comprehensive expertise in various domains, we are well-poised to offer 360° security across the enterprise.

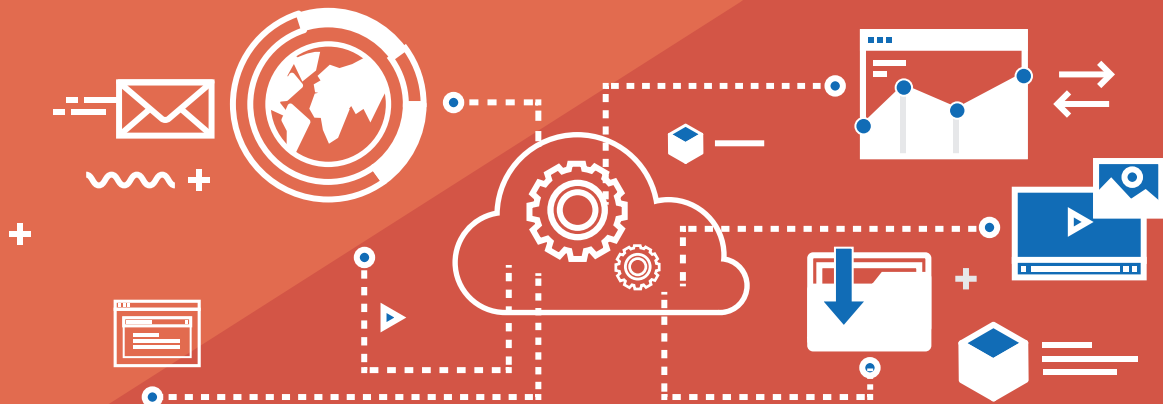**GOVERNANCE RISK AND COMPLIANCE**

INFRASTRUCTURE AND CLOUD SECURITY

APPLICATION SECURITY

IDENTITY AND ACCESS MANAGEMENT

ECP/DR

DYNAMIC CYBER SECURITY FRAMEWORK

Our Dynamic Cybersecurity Framework helps our customers move from a Static to a Dynamic posture to deal with an ever-escalating threat landscape, offering full spectrum of services.
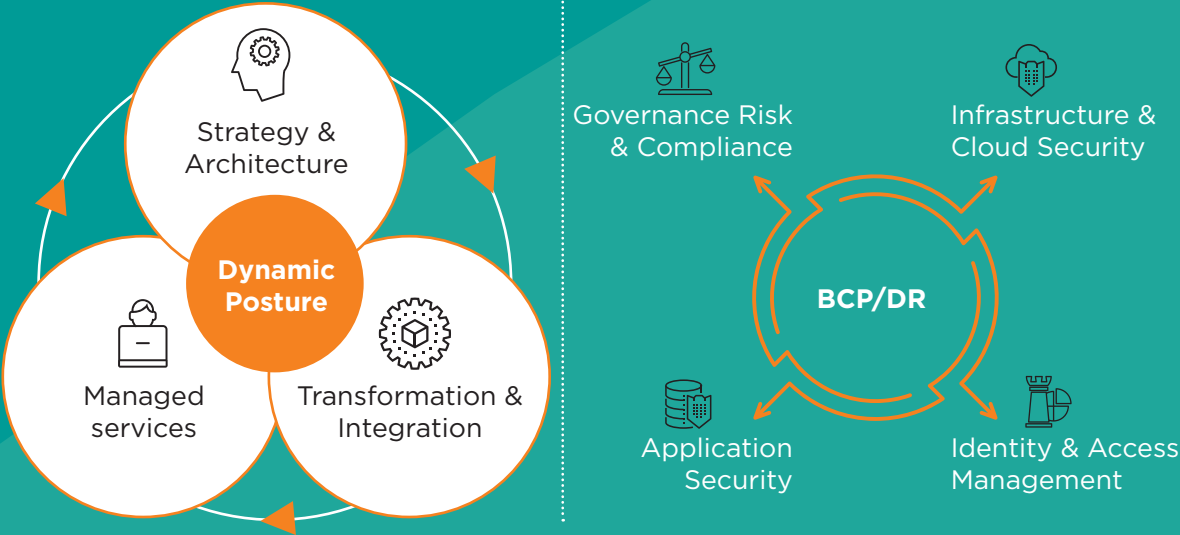
DYNAMIC FRAMEWORKS AND ACCELERATORS

SAFE	SecIntAI	BRiCS Business Risk Intelligence & Compliance Solution	DIGI-I-FORT	IDaaS	iBCM-iDRM

OUR PARTNER ECOSYSTEM

IBM	ca	RSA	Symantec	McAfee Together is power.	Check Point SOFTWARE TECHNOLOGIES LTD.
paloalto NETWORKS	SailPoint	Hewlett Packard Enterprise	r@nk	CISCO	Microsoft
MICRO FOCUS	FireEye	okta	TREND MICRO	MetricStream	CYBERARK

COVERAGE

Workplace · Mobile · Apps · Data Center · Network · Cloud · IoT

PROVEN SUCCESSES IN CYBER SECURITY

HCL has fostered over 200+ client relationships in cybersecurity and risk management domain.

CLIENT: ONE OF THE LEADING TELEVISION PROGRAMMING NETWORK

SOLUTION:

- Simplifying the security architecture and design and enabling systems integration
- Define content packaging and meta data standards for distribution
- Provide encryption for secured distribution of metadata across CDNs

BENEFITS:

- Security embedded into Enterprise fabric engineered for future
- Saved cost of distribution by 7-10% reducing manual intervention
- Improved compliance to regulations contributed to content monetization with increase the window of title ahead by 2-weeks,

---

CLIENT: ONE OF THE LARGEST ENTERTAINMENT AND MEDIA CONGLOMERATE

SOLUTION:

- Assessing and monitoring compliance to risks with host country government for each outsourcing vendor including people and processes compliance
- Implementing SAFE - Security Assessment framework for 24*7 monitoring for real-time threat detection

BENEFITS:

- Savings in millions avoiding penalty charges due to non-adherence of government rules and compliances

---