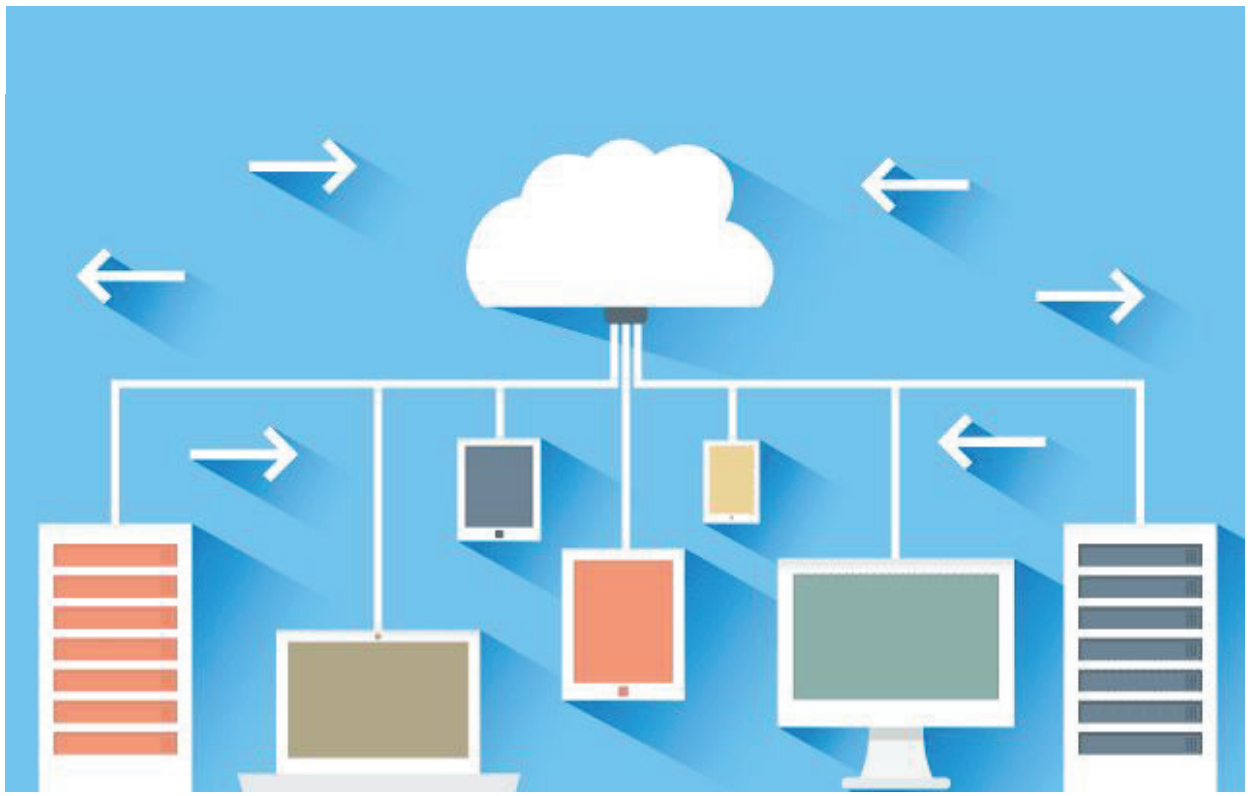
STARTEK

Secured CX: Strike a Balance Between Security and Experience

Reaching for the Cloud



The coronavirus pandemic has revealed how important the cloud is for bolstering societal resilience. More than half of our workload could be migrated to the cloud by 2022 compared to 33% now; this target could be met earlier than anticipated given a pandemic-related boost.

Specifically, the business advantages of cloud computing include:

- Resources purchased and consumed on a 'pay-as-you-go' basis, and increased or decreased as needed for optimal utilization
- Rapid innovation without the expense and complexities of hardware procurement and infrastructure management
- End-user productivity because no software is installed, configured, or upgraded on personal devices, and services can be accessed from anywhere
- Customers benefitting from 'vertically integrated' stacks that are customized at every level, which would normally be out of reach for on-premises deployments built from off-the-shelf components
- Data archiving on a public cloud that can provide data storage at a massive scale and cost-effectively
- Specialized compute-intensive workloads: When access to massive computing power is needed but only on a transient/ad-hoc basis, the cloud is an efficient option

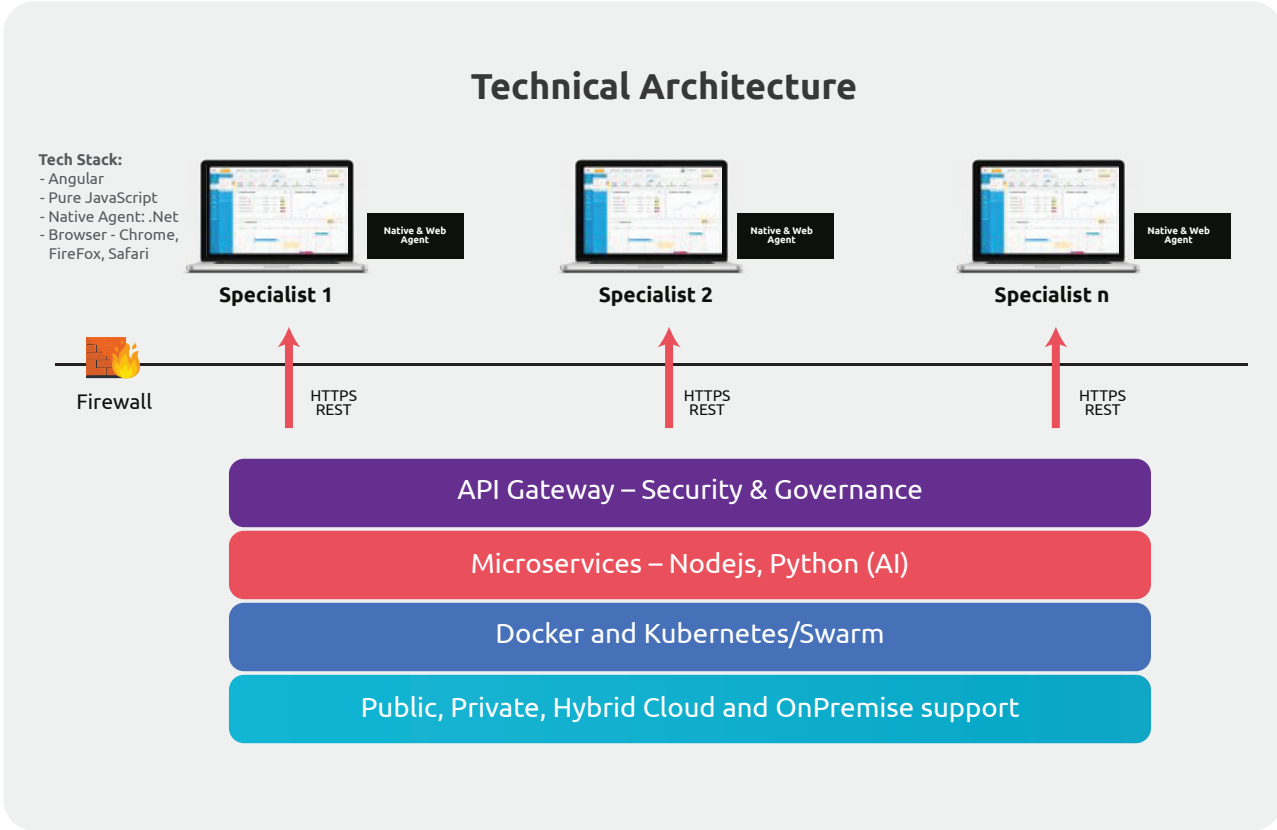
Cloud, and Working From Home

Cloud computing has been used by companies for over 14 years, starting with Amazon's Elastic Compute Cloud. This meant that many organizations were able to make a relatively quick transition to a largely work-from-home environment as the COVID-19 pandemic swept the world. For the most part, cyber security teams were largely successful in supporting business continuity and protecting the enterprise and its customers.

BPM's had to make a quick transition on two levels—leapfrogging their own long-term business plans for cloud computing while providing secure work environments at home for their customers. Along the way, the pandemic has created new security vulnerabilities—attackers seeking to exploit the gaps opened when telecommuting employees use insecure devices and networks. Threat actors also use known attack techniques to exploit people's COVID-19-related fears.

For example, Google tallied more than 18 million malware and phishing emails related to the novel coronavirus on its service each day in April. It also reported identifying more than a dozen government-backed groups using COVID-19 themes for these attempts.

BPM companies handle billions of customer transactions each year; there is an intense focus on digital security around Personally Identifiable Information (PII), and compliance with HIPAA, PCI, and SOX standards. That focus doubled this year with companies switching to a largely work-from-home environment, and their clients requiring greater assurances as a result. An unintentional consequence of this shift is that years after it was first developed and implemented, the debate about cloud security often remains vague.



Enabling Increased Digital Security

It has often been said that the weakest link in digital security is, in fact, the human one—and they are called insider threats. Some of the best practices around creating employee monitoring solutions to mitigate these threats include:

- Determining what behaviors are high risk i.e. copying files to external drives, using cloud storage to share corporate files, downloading/opening files and attachments from unknown sources. Then defining activity and content-based rules to block or restrict such actions
- On a more extreme case, creating a white list of apps/sites and blocking the rest, say, on a bank teller's workstation
- Preventing data loss by using predefined classified data for financial information, health, personally identifiable data, etc. or defining groups of sensitive data and monitoring their access, transfer or changes with technology like OCR, fingerprinting, tagging
- Implementing more scrutiny for privileged users and vendors for things like backdoor accounts creation, attempts to gain additional system privileges, unauthorized remote access, changing configuring files or accessing registry editor
- Using session recording features for evidence and forensic investigation in case of a security incident
- Connecting through a VPN—keeping in mind that a VPN alone does not stop a threat actor from accessing and compromising the internal network
- Adopting and enforce best practices for cyber hygiene
- Setting protocols for penetration testing

Breach Detection Toolset – Startek Work From Anywhere

WF Anywhere solution is designed to ensure compliance for the agents working from home by triggering near real-time alerts for breach detection

- Face, Object & Gesture Detection/Recognition
- PII Screen Masking
- Screen Watermarking
- Task Management
- Mouse, Keyboard Activities & Screen Captures
- Drowsiness Detection

Enabling Security at Startek

The components of the device-independent Startek Cloud ecosystem that enables Work Anywhere

Startek's innovative Startek Cloud uses a selection of platforms depending on client requirements. These range from Microsoft Azure; Microsoft Virtual Desktop; Citrix; VMWare; AWS; and an internally-built Business Process Management (BPM) platform—all supporting and integrating a variety of omnichannel options including voice, email, video, social media, digital, and messaging.

Each Virtual Desktop Infrastructure (VDI) is individually built and deployed to fit the vertical and application configuration of every client. All cloud VDI platforms are certified Payment Card Industry (PCI) and Healthcare Information Portability and Accountability Act (HIPAA) compliant and mirror the contact center User Interface (UI) and policies for a seamless transition.

At Startek, over 55% of our workforce now WFH with state-of-the-art information security protocols in place to protect customer information, layered with webcams that have an AI-based application deployed for real-time tracking of performance.

Startek's wAnywhere eSecuritySolution

Startek facilitates proper safeguards through its best-in-class wAnywhere eSecuritySolution. Developed to ensure the security of customer data, this comprehensive solution applies to every one of the company's agents; its elements include:

- **Task Reporting and Visualization**
  - Using a tracking productivity matrix that is time, task, and application-based
  - Providing collaboration tools including MS Teams, Slack, Skype, WebEx and the use of a notice board for consistent communication across the company
  - Using integration tools including CRMs, Issue Management, Task Management
  - Facilitating secure document storage and sharing
  - Ensuring activity tracking including:
    - Last Activity – KeyPress or Mouse Movement
    - Breaks taken – Lunch, Tea, Bio, Miscellaneous
    - Unauthorized application and websites
    - Total login and session hours
  - Providing intuitive and customizable dashboards for managers and employees that help facilitate Visualization and Reporting
- **Metrics**
  - Ensuring an Audit and Logging trail
  - Ensuring the security of PII including the masking of data on Web Apps e.g. Credit Card Info, SSN, PHI data, etc.
- **Face Detection and Recognition**
  - Using Facial Authentication and Unknown Person detection
  - Detecting more than one person in the room (unauthorized)
  - Monitoring Not at Desk – Time away from the system
  - Monitoring Gesture Detection – Sleep, Mood
  - Using cognitive services to help serve customers better by monitoring their reactions
- **Intrusion testing**
  - Monitoring intrusion levels on four fronts:
    - Low: Capture analytics
    - Medium: Images and app usage
    - High: Videos, break time limits, etc.
    - Break thresholds

The Role of Artificial Intelligence and Facial Biometrics

Arguably two of the more powerful tools in use today are artificial intelligence that can identify abnormalities or irregularities in the network, and facial biometrics. The latter uses facial recognition to track attendance and avoid any malicious activity in premises; the former analyzes user behaviors and deduces patterns. With such data, it is much easier to identify cyber vulnerabilities quickly.

Complicated hacking techniques, such as obfuscation, polymorphism, and others make it a real challenge to identify malicious programs. With AI stepping into cybersecurity, experts and researchers are trying to use its potential to identify and counteract sophisticated cyber-attacks with minimal human intervention.

AI networks and machine learning, a subset of AI, has enabled security professionals to learn about new attack vectors.

Machine learning in cybersecurity can be used to analyze cyber threats better and respond to security incidents. There are a few other significant benefits of machine learning, which include –

- Detects malicious activities and stops cyber attacks
- Analyzes mobile endpoints for cyber threats – Google is already using machine learning for the same purpose
- Improves human analyses – from malicious attack detection to endpoint protection
- Uses in automating mundane security tasks

Future Vision

Among the IEEE Computer Society's Top 12 Technology Trends for 2020 are projected trends of direct relevance to the BPM industry. The first is the increasing use of AI and ML for cybersecurity through a partnership among members of industry, academia, and government on a global scale. Designed well, AI/ML can drive down response times from hundreds of hours to seconds and scale analyst effectiveness from one or two incidents, to thousands daily. It can preserve corporate knowledge and use it to automate tasks and train new analysts.

Technology is making it harder to distinguish between legitimate and fraudulent technology content and this is a development worth keeping an eye on, even as we rely on our omnichannel approaches to gather accurate data from a variety of sources, including social media.

It is about refreshing our thinking toward cybersecurity. McKinsey's approach to the new normal—our post-pandemic world—includes remote cybersecurity operating models and talent strategy. While realizing that the new approach will have implications across the enterprise, they recommend rethinking the cybersecurity operating model and continuity plans for physical-location-constrained operations, including automation opportunities. The approach is Derisk by design and further embedding application-development processes, principles and capabilities of DevSecOps— the linkage among development, security, and operations.