The Next Generation of Cloud Infrastructure Expands New Areas for Emerging Vendors, Strategic Buyers and Institutional Investors

CONTRIBUTORS

Chris Brooks, Managing Director, London
Chaim Lubin, Managing Director, Chicago
Matt Cautero, Vice President, Dallas
Roger Knight, Managing Director, New York
Sam Jackson, Director, New York
Alejandro Yu, Vice President, New York

The US Department of Defense recently awarded a $10B technology contract for the Joint Enterprise Defense Infrastructure to Microsoft. This contract allows for modernization of our government's technology as much of today's military systems operate on legacy infrastructure. Unifying information in the cloud will allow the Pentagon to leverage new, cutting edge defense solutions such as remote sensors, semiautonomous weapons and artificial intelligence. This access to advanced, general purpose cloud infrastructure will bring the US Defense department up to speed with bleeding edge technologies that is common throughout modern enterprises.

Now that cloud architecture has infiltrated business and government at every level, the next evolution of cloud infrastructure is underway. This evolution sees system administration being automated, giving a 360-degreee view from the user interaction to the network layer and the mainframe to the cloud, without human interaction. New technologies leverage machine learning (ML) and artificial intelligence (AI) for autonomous cloud operations and cutting-edge statistical tools to efficiently detect and fix anomalous cloud infrastructure conditions. This allows companies to materially reduce manual effort in an area where labor is often times time consuming, error-prone, subject to turnover and comprises the majority of expenses.

Cloud architecture also allows companies to consolidate their technology stacks and reduce the number of necessary vendors. Additionally, security awareness, paired with developments in compliance, such as GDPR and other privacy/data regulations, means that software testing and security need to be integrated into every operation. For example, there is hyper-focused innovation in critical business segments such as

(continued next page)

HCIT, IoT devices, supply chain visibility, and new technical solutions including large-scale public key infrastructure management (PKIM), zero trust models and quantum encryption. Additionally, next generation workloads will require the rethinking of current architectures and the creation of new opportunities from serverless cloud deployments and increased levels of edge computing power.

At Lincoln, we continue to see the ability to efficiently and correctly consume data, while finding and remediating anomalies as a key differentiator for automated solutions, attractive to strategic buyers and institutional investors and garnering higher valuations. Additionally, we see private equity firms continuing to fuel both platform expansions and innovation investments in enterprise software. A recent Lincoln survey of over 160 private equity investors during our annual Growth Conference found that four tech industries experiencing significant interest include application software, education technology, data analytics and management, and supply chain software.

We also see leading companies moving away from legacy, monolithic software solutions as a way to reduce internal friction and provide swifter software development to benefit their end customers. As a result, we see engineering teams moving to microservices architectures and application containers, as these allow them to update and scale services independently while providing better resilience.

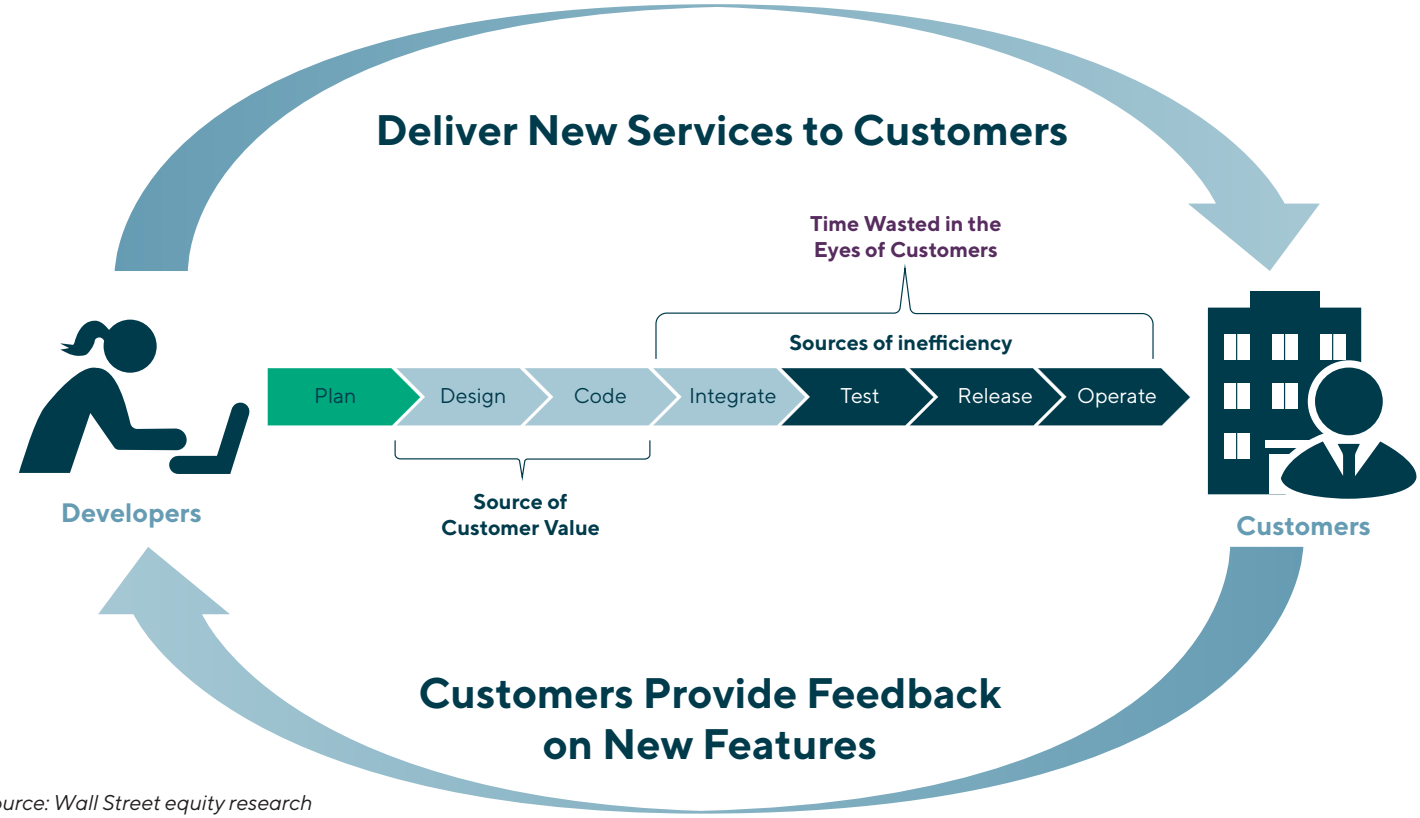
Throughout multiple conversations with industry vendors and key investors, we see an emerging trend in infrastructure and security software, as companies move from monolithic apps to microservices, and as faster software development and delivery becomes a competitive advantage. This not only allows developer teams to use any technology they chose, but also provides better application resiliency and scalability. In line with this trend, we also see an exponential increase in application containers in turn fueling the relevance of container management, security and orchestration solutions.

A recent Lincoln survey of over 160 private equity investors during our annual Growth Conference found that four tech industries experiencing significant interest include application software, education technology, data analytics and management, and supply chain software.

(continued next page)

DEV-OPS

DevOps is already mainstream as faster software delivery becomes a key strategic differentiator for companies in all industries. As a result, removing any frictions in the creation, testing and delivery of software continues to be a common discussion topic among company Boards and management teams.



Source: Wall Street equity research

LINCOLN PERSPECTIVE

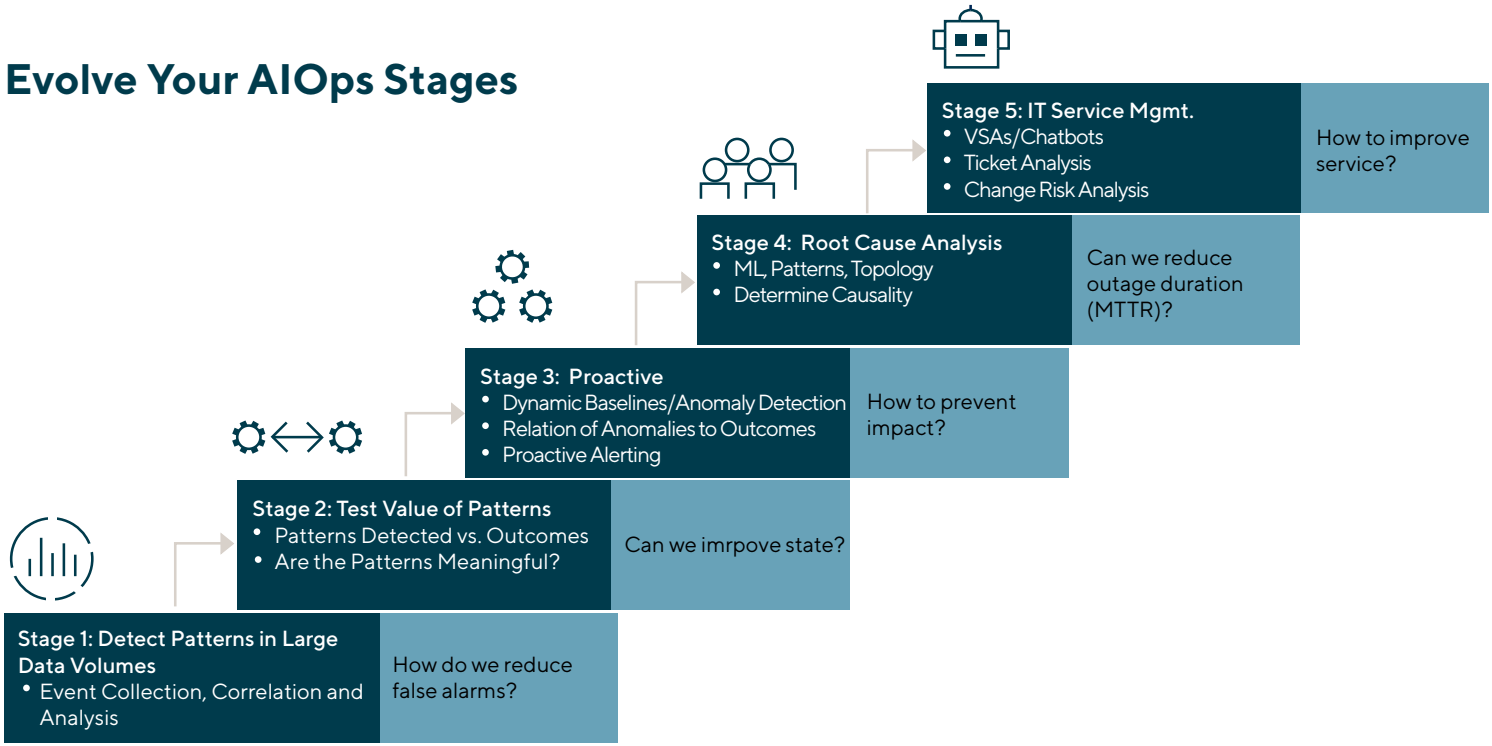
We see CI/CD, paired with Continuous Testing and Monitoring as key competitive differentiators

- Lack of developer supply is a meaningful constraint as demand for these professionals continues to increase. According to CompTIA, there were 275K IT job openings in 2Q18, for example, with only 71K being produced by the US education system
- We see continuous testing and monitoring of software development and microservices/containers becoming a key focus, as these solutions compose the backbone of high-end DevOps structures

AI-OPS

As cloud platforms reach global scale, the actual operation and maintenance of the infrastructure supporting enterprise applications can no longer be done manually as teams are tasked with analyzing exponentially increasing data in the administration of globally distributed platforms. However, this is exactly where machine learning models shine. Leading companies in AIOps leverage machine learning models and automated solutions/response to globally manage distributed infrastructure operations.

Evolve Your AIOps Stages



Source: Gartner

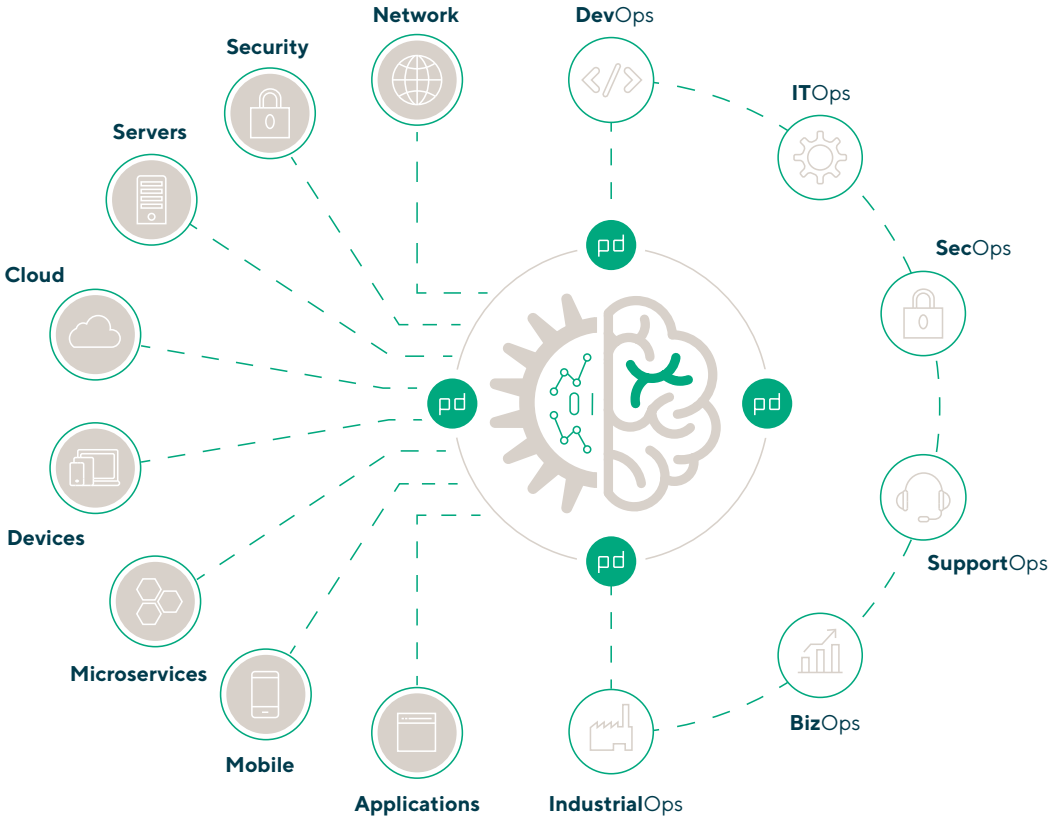
LINCOLN PERSPECTIVE

- AIOps tailwinds include customer demand for public and hybrid cloud applications and services and infrastructure complexity that continues to grow
- As machine learning solutions require specified knowledge, strategic buyers, especially cloud infrastructure vendors, are considering quick, tuck-in acquisitions of high-value ML and analytics solutions to complement existing product roadmaps and internal R&D efforts

DIGITAL-OPS

By leveraging automation and machine learning, companies can focus on real-time operations that improve their business processes and decision models, helping them bring clarity to complex use cases, quickly provide actionable insights—and real-time responses—and proactively prevent potential incidents.

Digital
Operations
Management



Source: Pager Duty

LINCOLN PERSPECTIVE

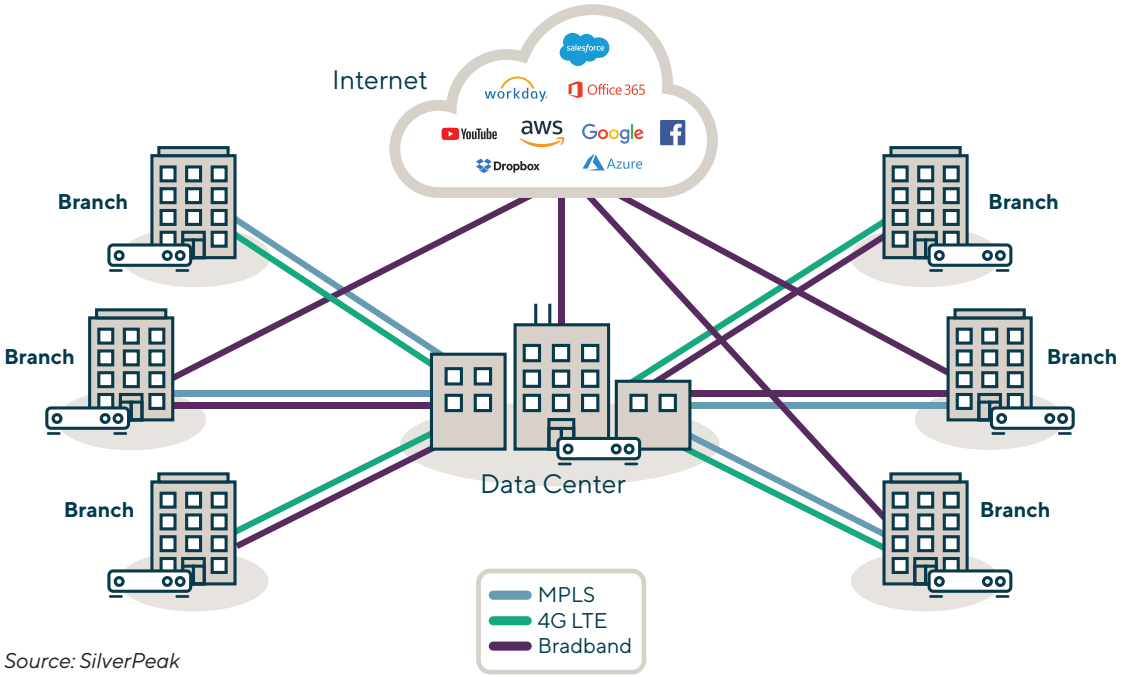
According to Gartner, CIO's are increasing investment in cloud services by 33%. As processes become digital and companies continue gathering large amounts of data, it becomes even more difficult for a single individual to understand the impact of particular events and maintain real-time communication with multiple teams. DigitalOps solutions bring modern incident response and orchestration to complex teams and organizations, providing seamless integration into other operational toolchains. Leading vendors can notify appropriate team members in a reliable and timely manner, materially increasing awareness and providing automated guidance/response

Successful vendors provide increased process visibility into operations management, effectively improving overall process time, communication and employee satisfaction

IT-OPS

ITOps allow IT staff to properly manage companies' business technology needs while servicing both internal and external clients. Paired with system standardization, automation of ITOps processes materially decreases human errors, increases uptime, and allows internal and external clients to increase collaboration. Leading vendors allow customers to use automation to synchronize tasks across complex systems and automatically control complex deployments while managing other solutions. With the increasing modularization of applications as a way to speed up development processes, microservices and application containers have enabled development teams to efficiently and independently build very small services. As a result of the strong growth in application workloads and container instances, we see Platform as a Service solutions and Container Management systems become a necessity, as it is still the end-customer's responsibility to manage the health, traffic, monitoring and uptime of these solutions.

SD-WAN Architecture



Source: SilverPeak

LINCOLN PERSPECTIVE

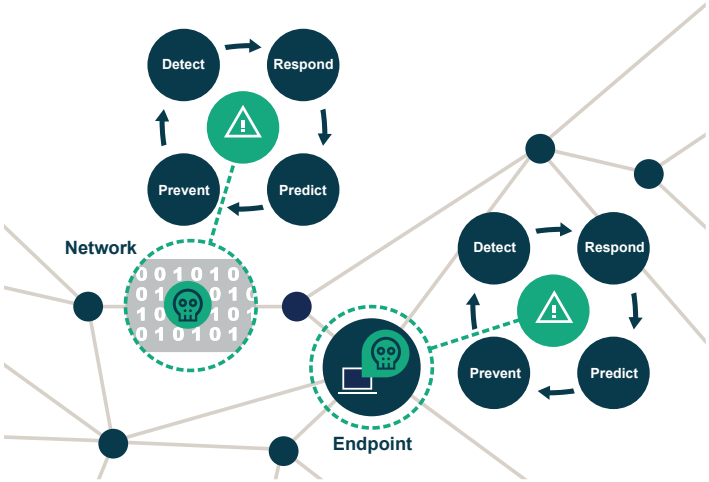
We see this segment increasing even further as a result of the proliferation of bring your own device (BYOD) models, IoT solutions, the expansion of the overall network surface and at-the-edge computing solutions

Infrastructure as code initiatives, such as SD-WAN, are transforming previously hardware-centric infrastructure within enterprises. This shift is creating substantial opportunities and growth among disruptive ITOps vendors offering management and security tools

SEC-OPS

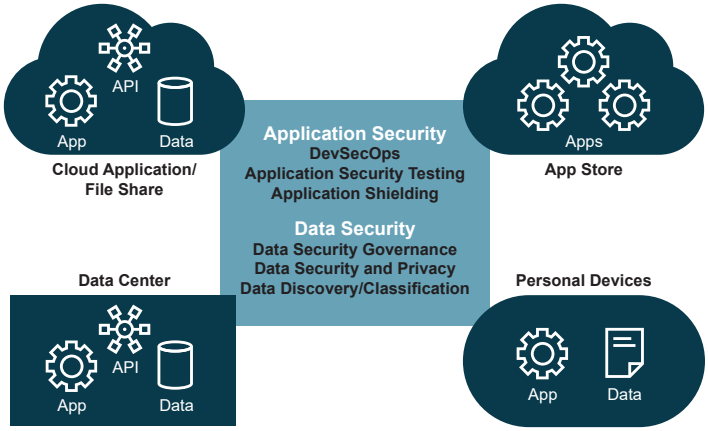
Security Operations teams oversee enterprise security and focus on decreasing risk while maintaining efficiency. These teams cover a wide range of security concerns, from application development and website security to endpoint protection and response. As a result of expanded attack surfaces, and as companies move into CI/CD processes, organizations now require real time analysis and response to security incidents. We see increasing interest in this space, with leading vendors providing increased operational visibility, actionable compliance and remediation solutions. As a result of the complexity of these solutions, leading vendors are leveraging automation to analyze vast data lakes and actively address and remediate unexpected behavior and turning fiercely to M&A as a solution to differentiate competitively.

Security of Networks and Endpoints



Source: Gartner

Security of Applications and Data



Source: Gartner

LINCOLN PERSPECTIVE

As a whole, ITOps has faced a dramatic change as the "castle and moat" security model—a parallelism to a castle in which you only trust activity inside the walls of your network and distrust anything coming from the outside—stopped being relevant. At the same time, the "perimeter"—the limit previously provided by the castle's external wall—has become more porous. We see a wide range of emerging solutions in SecOps that provide high levels of security to end-customers, from micro-segmentation and containment solutions, to new IAM and MFA developments as well as automated endpoint/network protection and response

As the perimeter continues to disappear, we see increasing interest in zero-trust security models and PKIM solutions, with successful companies in the space consistently using M&A to create large platforms that can link these solutions together and provide a more holistic security answer