



GUIDEBOOK
PROGRAM: SECURITY AND INFRASTRUCTURE
DOCUMENT NUMBER: U73



**NUCLEUS
RESEARCH**

GUIDEBOOK

UNDERSTANDING THE VALUE OF MIGRATING FROM ON-PREMISES TO AWS FOR APPLICATION SECURITY AND PERFORMANCE

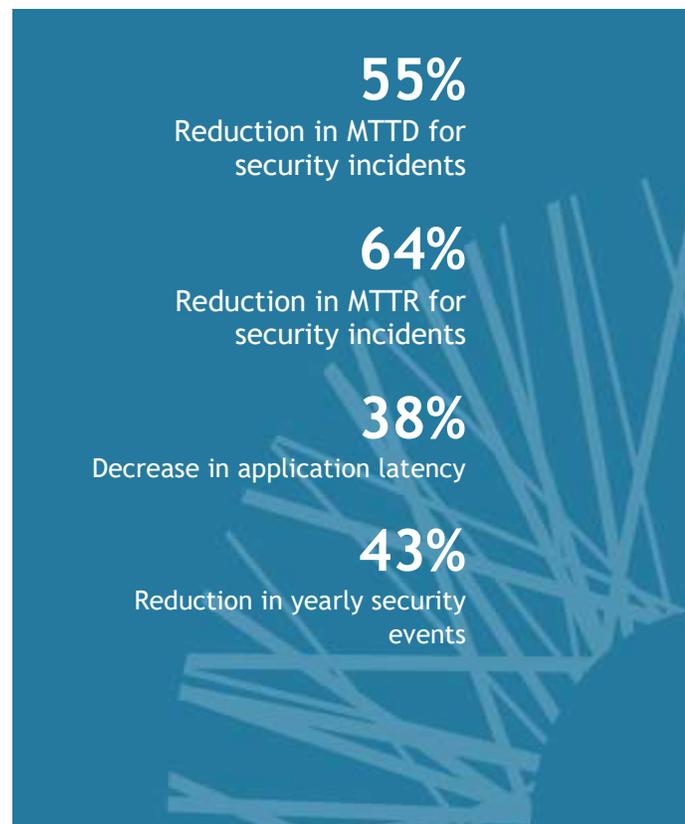
ANALYST

Daniel Elman

Nucleus Research, Inc.
100 State Street, Boston, MA, 02109
+1 (617) 720-2000
www.nucleusresearch.com
©2020 Nucleus Research, Inc.

THE BOTTOM LINE

Nucleus studied enterprise organizations' journey to the cloud with AWS to understand how moving applications from an on-premises to public cloud environment affects the security, performance, and availability of those applications. Nucleus interviewed executives and development team leaders from 33 global enterprises spanning a wide range of industries who migrated a collective 351 applications from on-premises environments to the AWS cloud. We found that migrating to AWS substantially improves application availability, reducing both planned and unplanned downtime by 29% and 69%, respectively, and decreasing application latency by 38%. Further benefits of migrating to AWS include a reduction of IT costs, typically falling within 20 to 40 percent annually, a 55% reduction in the mean time to detection (MTTD), a 64% decrease in the mean time to resolution (MTTR), and improvements in application security, including a 43% decrease in security events.



THE SITUATION

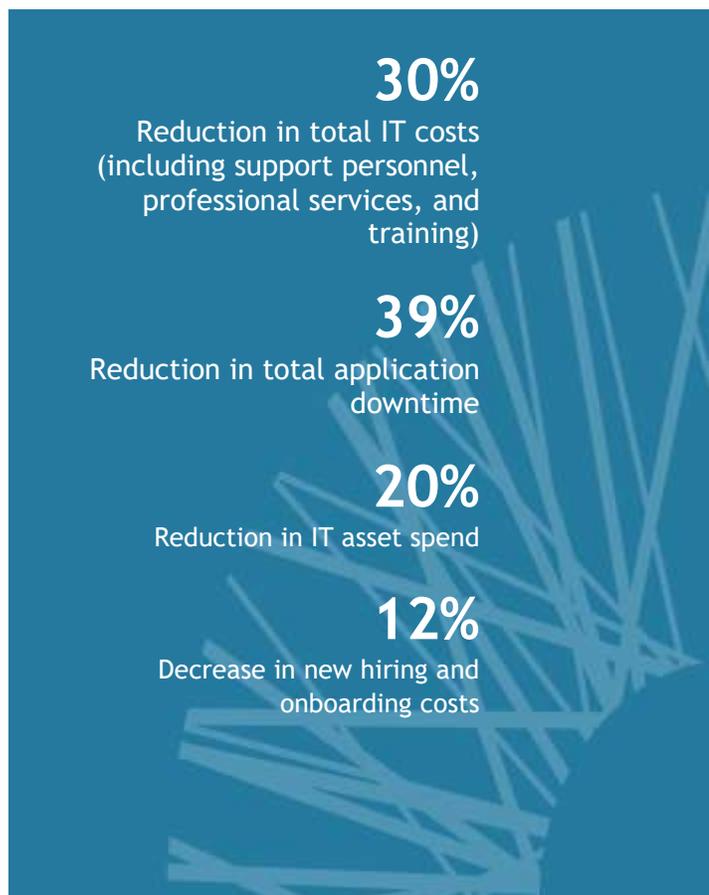
Before cloud computing technology was widespread, internal IT and development teams were primarily responsible for building, maintaining, and securing applications and the underlying infrastructure they ran on. In our research, customers highlighted how on-premises infrastructure lacked the ability to adjust to rapid changes in demand leading to latency issues, downtime, and lost business. While in-house IT and on-premise solutions gave companies' complete control of their own systems, it often created a bottleneck that limited agility for future innovation, and produced tech debt from legacy technology investments. Additionally, customers noted that development teams operated reactively, constantly looking to clear old tickets and fix reported bugs. There was little proactive maintenance or stress testing of applications because internal teams were stretched too thin and lacking expertise. For example, taking down an application to patch it would result in the application being unavailable. By doing so, a failure within the patch could lead to more downtime, or developers could risk being able to bring an application back online. For a load test, developers would need to create and configure a mirrored solution in a second environment with time, cost, and standardization issues.

METHODOLOGY AND USER PROFILES

For this project, Nucleus interviewed executives and development team leaders from 33 global enterprises spanning a wide range of industries, including manufacturing, e-commerce, aerospace and defense, technology, health sciences, media, and others. Interviews were conducted to understand how migrating workloads from on-premises environments to the AWS cloud was able to enable better development processes and application performance, security, and availability.

To understand how migration affected these core areas, we compared a number of common metrics from before and after the cloud transition, including the number and severity of security incidents annually, the average time needed to detect and resolve security and performance issues, the average amount of planned and unplanned downtime experienced, and the average application latency.

The following table shows the demographics of the interviewed companies. For each industry included, between two and eight companies with annual revenues greater than \$100 million were interviewed to understand motivation behind moving applications to the cloud, the number and type of applications, the migration strategy, and other factors relating to the company's use of AWS' cloud.



Industry	Annual Revenue (USD)	Number of Applications Migrated
Biotechnology and Healthcare	\$100M-\$250M	62
Technology	\$100M-\$20B	111
E-commerce and Retail	\$100M-\$750M	47
Communications and Media	\$250M-\$5B	21
Professional Services	\$100M-\$2B	27
Manufacturing	\$250M-\$1B	28
Energy and Utilities	\$150M-\$2B	36
Aerospace and Defense	\$1.5B-\$50B	19

#1 – APPLICATION LIFT AND SHIFT

A biotechnology research company that sequences DNA to identify genes and research potential treatments for genetic diseases has migrated 50 applications to AWS and retired resources from two self-managed datacenters. The applications migrated included tools for data pipelining and ETL; an analytics engine for data processing; a data warehouse; an automation engine for programming repeatable processes like batch upload to the data warehouse at regular intervals; and a visualization tool, among others. It began migrating applications in 2015; the company chose a lift-and-shift strategy for initially moving to the cloud. In recent years it has begun to optimize certain apps for the cloud, however the first priority was to rehost the applications on AWS and retire on-premises resources.

By retiring its on-premises datacenter resources and turning to cloud hosting, the company reduced 30 percent of its total IT costs, which included technology costs as well as internal support personnel and third-party consulting. It has also increased application performance across the board, reducing total downtime by 39 percent compared to its self-managed infrastructure. Most important to the long-term health of the organization, the company has adapted its development procedure such that all new applications have been built to be cloud native. This improves performance and security in the long-run and has accelerated the overall rate of development for the company; it has brought 21 new applications to production on AWS, 3 times more than could have been built and deployed on-premises.

#2 – APPLICATION REFACTOR

A global financial services provider has employed cloud migration approach depending on the priority level of the applications (this priority level was based on the importance to the business, for example apps with the most daily users). It had originally acquired the on-premises resources to support its applications internally, but realized the long-term costs were unfeasible. It anticipated the organization's digital footprint growing significantly, rendering existing infrastructure in constant need of upgrade – outsourcing the bulk of IT infrastructure would allow the company to reduce IT costs and accelerate the deployment of new application code, improve performance and enable integration with other cloud services in the future, and enable internal development teams to focus on value-added activities instead of data-center management and support.

For the most critical workloads, such as a wealth management tool and a real-time data aggregator, the company decided to completely refactor the code to be cloud native. It wanted to leverage microservices based architecture to improve the application flexibility and pace of subsequent updates. Simpler applications with lower priority were simply lifted and shifted to the cloud as a way to control costs and complete the migration in time; it wanted all mission critical workloads to be running in the cloud within 12 months of the start date.

For the wealth management tool and other apps to be refactored, the company opted for a full microservices based architecture. It was able to successfully refactor the applications and integrate them with a Microsoft SQL Server (that has since been retired and moved to AWS). After completion, the application was able to leverage auto-scaling which notably improved performance. It also shortened the time needed to deploy new update code to production from over two weeks to between 30 seconds and one minute. Retroactive cost analysis showed the company was able to reduce its spend on cloud resources by approximately 20 percent. Developers are also more productive, building value-add apps and functionalities instead of maintaining infrastructure. This migration allowed the organization to change the hiring criteria for developers, reducing onboarding

costs and attracting top-tier development talent. Annually, the spend on hiring and onboarding new developers was cut by 12 percent after migrating to AWS.

#3 – DISASTER RECOVERY

The company is a regional energy company that distributes electricity to customers; it serves as an alternative to global power providers, particularly serving small towns, and small to medium sized businesses. It was assessing its disaster readiness and realized it needed a backup plan in the event of a failure or loss of one of its own data centers. It partnered with AWS to create a business continuity plan to ensure it would not lose any customer or operational data in the event of a calamity. Additionally, the company's growth trajectory was such that buying and maintaining the physical infrastructure for more data centers (and upgraded technology within these data centers) would become a disproportionately large cost area. It considered partnering with a disaster recovery specialist, but realized that migrating its data and application portfolio to the cloud with AWS was a better long-term strategy not only for controlling costs, but to support future application development projects and increase overall IT flexibility.

It created a digital copy of its infrastructure and deployed it to the AWS cloud. It created images in the Amazon Virtual Private Cloud (Amazon VPC) of several enterprise tools including several Oracle and Microsoft SQL Server databases of customer information and operational data, accounting, billing, and financial reporting tools, workforce management tools and internal employee files, and other tools. It copied the databases to Amazon Glacier for the most cost-effective long-term storage and also leveraged S3 for more frequently accessed data. The company was able to retire a quarter of its physical data centers and is continuing to scale back on-premises resource usage as it moves operations to the cloud; in 2018 it stopped purchasing new physical hardware and will only support existing systems until all data and workloads are fully cloud-based.

After migrating its finance toolset to AWS, the application performance was notably improved – application response time decreased from 250 milliseconds to 100 milliseconds. While difficult to quantify, the company could suffer a complete failure to its own physical infrastructure and experience negligible business disruption since critical files and workloads are regularly backed up in the cloud. By moving away from the purchase of its own physical infrastructure for data centers, the company was able to reduce its IT infrastructure-related spend by approximately 33 percent.

CUSTOMERS SEE IMPROVED SECURITY AND AVAILABILITY WITH AWS

SECURITY

Cloud-based solutions continue to make security improvements to data encryption, application-specific firewalls, and event logging to monitor user activities. While these measures aim to mitigate security risks, cloud-based and on-premises solutions still face threats from internal and external sources. Internal risks associated with employees prove to be the most difficult to prevent. Barriers to entry can be placed, but stolen user or administrative credentials can fool any system. Additionally, APIs are routinely exposed to the public for business partners, opening company communications to unauthorized individuals. Externally, either through the exposure of these APIs or from other sources, software always faces risks associated with malware.

While there are risk factors associated with the cloud, measures to prevent future exposure are implemented faster and easier with cloud-based solutions than on-premises ones. The AWS cloud infrastructure is maintained solely by AWS at designated data centers instead of customer facilities. AWS employees manage data centers instead of customer employees, leaving less room for error and reducing the risk of stolen credentials. It is difficult for any one company to have the proper training or protocols in place to accurately monitor security risks while AWS continuously improves security measures. For example, a customer's AWS instance can be configured to establish role-based permissions, so each user can only access relevant code, data, and content for their specific role within the company.

Furthermore, AWS is backed by a deep set of cloud security tools, with more than 200 security, compliance and governance services and key features. AWS's scale allows for significant investment in security policing and countermeasures where even the largest organizations may lack the resources and funding to maintain such a structure. AWS investments in security and the policies, architecture, and operational processes of AWS are then able to be leveraged by all AWS customers. Out of the box, AWS provides security certifications such as ISO 27001, ISO 27017 (cloud security), ISO 27018 (privacy), ISO 9001, AWS PCI and SOC 1, 2 and 3, HIPAA, FERPA, CJIS, SEC Rule 17a-4(f), IRS 1075, and SRG Impact Level 2 and 4 for DoD systems. Public sector certifications such as FedRAMP at the Moderate and High level for Federal government systems are also provided to validate AWS' FISMA and ITAR compliance.

51%

Reduction in P0 incidents

24%

Reduction in P1 incidents

69%

Reduction in unplanned application downtime

29%

Reduction in planned application downtime

For on-premises solutions, the same infrastructure could be neglected with poor maintenance and delayed updates that could expose the system. Often, on-premises infrastructures become too costly and labor-intensive to continually upgrade while also maintaining the backlog of developer requests. A common theme among on-premises customers is that the burden of maintaining the infrastructure becomes so great that the performance and quality of applications eventually suffers. By migrating to AWS, developers can modernize operational processes by adopting secure DevOps principles such as least privilege, adding governance and controls for new code commitments, and regular reviews of event logs.

Reduce yearly
security events by
43%

After speaking with customers who migrated applications from on-premises to AWS cloud, multiple security benefits were realized. Customers noted a significant reduction in overall security breaches, amounting to a 51% reduction in critical P0 incidents and a 24% reduction in less-severe P1 incidents. This breaks down further to a 43% reduction in yearly security events on average.

Users also realized a 55% reduction in the MTTD, the average time needed to detect an intrusion or security failure, and a 64% decrease in the MTTR, or the average time needed to resolve issues such as a security breach or outage. Altogether, switching to AWS saved developers and administrators time and energy to devote to other tasks and reduced the total amount of downtime for applications.

Reduce MTTD by
55% and MTTR by
64%

For customer-facing applications, performance and security is one key area of differentiation. This was repeatedly brought up as one of the primary motivations for partnering with AWS to migrate these applications to the cloud. With business in all industries becoming more digitized, the quality of the digital experiences companies deliver to their partners and customers has become a key differentiator. The ultimate goal for companies interviewed was, using tightly integrated applications to share and retrieve data with other apps in the ecosystem, while keeping user data secure, and remaining outage-free. Customers cited AWS's growing list of third-party security certifications (FedRAMP, GDPR, PCI-DSS, etc.) and portfolio of high-profile enterprise customers as key factors contributing to their perception of AWS as a market leader in cloud security.

- *"We are processing genomic data of patients to discover new drugs and treatments for genetic diseases. AWS enables our clinical research in a secure, HIPAA-compliant environment. Since moving onto AWS, we have experienced zero security incidents and grown our catalogue of genomic data by nearly 40 percent year-over-year compared to the pre-AWS setup."*
- *"It would have taken us years to achieve the security certification levels internally that AWS has, so it was an obvious choice. With the Amazon VPC, we can fully customize and provision our virtual environment to meet industry-specific requirements, and the initial instance was live in production in just under 4 months of the project start date."*

AVAILABILITY

Nucleus found that downtime for servers and applications costs enterprise organizations \$5,519 per minute on average (Nucleus Research *u25 – Cutting through the noise in cloud IaaS* – February 2020); this makes minimizing MTTD and MTTR crucial, not only for saving developer time but also for reducing business disruption and missed revenue generation opportunities. With on-premises solutions, downtime for maintenance could cause all users to stop using the application, leading to a disruption in organizational processes and decreased customer satisfaction for customer-facing applications. A cloud-based infrastructure such as AWS enables developers to target specific risks and allow users to continue using the modules of the application not associated with the risk factor. These assumptions remained true when reviewing customer data after moving applications to AWS, where users saw a reduction in downtime across the board after migrating. Nucleus found on average 29% and 69% reductions in planned and unplanned downtime respectively. Improvements continued externally with the number of missed service-level agreements (SLA) reduced by 34%. Lastly, users saw improvements to application performance with latency improving by an average of 38% since moving to AWS.

Reduced missed
SLAs by 34%

With data centers in all geographic regions (and continued investment to expand coverage), AWS users can localize workloads to their region. AWS designs its data centers with significant excess bandwidth connections so that if a major disruption occurs there is sufficient capacity to enable traffic to be load-balanced to the remaining sites, minimizing the impact on customers. Along with reducing latency and outages, existing (and still to be conceived) customer privacy and data usage regulations like GDPR and CCPA stipulate that certain types of data cannot leave the locale where it is collected. The ability to easily comply with these regulations without requiring weeks of disruption or having to rebuild any applications can save customers millions of dollars in avoided penalties.

- *"After transitioning critical workloads onto AWS, we realized immediate cost savings from retired internal systems, but most significantly, we modernized our development process and the way we architect applications to take advantage of cloud-native functionality. This has enabled us to deliver more reliable applications that perform better under heavy traffic."*
- *"We refactored a document processing application with EC2 and it notably improved application performance from day one of deployment. Users described the update as being '1.5 to 2 times faster,' and the application failure rate has gone down, achieving 99.99 percent uptime over the past year, compared to the 99.95 benchmark achieved with our on-premises deployment."*

WHY AWS?

For this project, Nucleus sought to understand why customers chose AWS over other competing cloud vendors. Separate from availability and security, the three primary factors for migrating to AWS were the technological scale and expertise to handle critical and highly complex workloads, the anticipated cost savings and reduced internal IT burden, and the availability of support and online documentation.

ENTERPRISE SCALE AND CAPABILITY

AWS has the capacity and technology to support workloads at any scale. Since the infrastructure is all maintained and networked by AWS, customers can select the proper hardware for their workload types and the amount of storage needed. If the demand for storage or compute suddenly increases or decreases, the customer can scale accordingly and only pay for what they use, eliminating the ongoing cost of maintaining idle hardware internally. Further, AWS offers a market-leading number of additional cloud-based services and tools for developers to improve developer experience and expand application functionality. A couple of examples are, AWS Lambda for serverless computing, multiple container deployment, and orchestration tools, and Amazon SageMaker and Forecast for managing, deploying, and training machine learning models, and for leveraging machine learning for time series analysis and forecasting, respectively. This set of additional capabilities is a critical for customers when choosing AWS; it can save hundreds of developer hours and jumpstart technology initiatives that would be years away if internally built.

- *"Our infrastructure needs are complicated; our instance currently consists of nearly 3,000 virtual machines (VMs), 200 Kubernetes clusters on EKS, and additional containerized workloads on AWS Fargate. The scale and complexity of our environment is growing steadily as we've adopted a continuous delivery development model since migrating to AWS, with new improvements made to our most-used applications almost weekly. Along with the enterprise scale, we needed a cloud vendor that offered mature app networking capabilities that provided real-time visibility to performance, resource consumption, and load balancing across the infrastructure types. Further, we have machine learning initiatives in the pipeline, and needed a cloud solution for minimizing the cost and complexity of that undertaking. AWS offered the most functionally complete solution portfolio, and it has the track record of bringing value-add cloud functions and services to market months before its closest competitors."*
- *"We migrated a SQL server-based application to AWS cloud. The SaaS application helps customers manage scheduling and routing for field service technicians. Obviously, we needed to ensure greater than 99 percent availability, but what stood out most was the breadth of services AWS offered that could help us build new technology on top of our existing investments. The main platform was built on Aurora, but the ease with which AWS services integrate allowed us to create a new analytics module built on RedShift to enrich the scheduling app. When we map out future plans for optimizing the computation, building more automation across the platform, and embedding increasingly sophisticated analytics and visualizations, AWS has the cloud services and expertise to help us do it successfully."*

COST SAVINGS AND IMPROVED STAFF PRODUCTIVITY

By eliminating the internal hardware required to build and deploy applications at enterprise scale and reducing significant capital expenditure on software, on-going maintenance, and data center operations, organizations can save millions of dollars in infrastructure costs. For developers working on applications, moving workloads to the cloud can dramatically reduce the time and disruption around implementing and releasing updates, allowing for more time spent ensuring high quality applications are being built. This accelerates the pace of development and innovation for the customers, as it frees IT from the burden of environment maintenance and allows them to refocus on leveraging the tools and services provided by AWS to improve existing applications or build new ones. Since pricing is usage-based, there is no wasted spend on idle computing power or storage. Further, moving to AWS allows customers to eliminate large-scale budgeting and planning for IT infrastructure projects. On average, AWS customers saved between 20 to 40 percent of IT budget (including technology costs, support personnel for maintenance and upgrades, professional services, and training) after migrating, allowing funds to be redirected to new projects within the department. Cost savings came primarily from reduced or avoided labor costs by redeploying developers responsible for maintaining on-premises networks, and retired physical hardware (and the ongoing costs to maintain and upgrade the systems), especially redundant hardware that was in place to support rarely occurring super-high application demand.

Saved 20% to 40% of IT budget spending, including technology costs, support personnel, professional services, and training.

- *"It was critical to find a cloud partner that understands our business objectives. With AWS, we have dedicated personnel assigned to our optimizing our account. The technical account manager (TAM) and support team are extremely familiar with our business and AWS instance. With the support team's help, we've optimized our AWS spend to maintain performance levels while decreasing the annual bill by 15 percent. This has allowed us to accelerate the cloud development timeline by a full quarter."*
- *"We migrated nearly 40 applications onto AWS in the first year, primarily using the lift-and-shift model so we could eliminate our on-site datacenter and server network as quickly as possible. This allowed us to reduce our annual spend on networking hardware by approximately 70 percent (we still maintain some on-site servers for backup purposes) and redeploy a team of 12 developers who were responsible for supporting the on-premises systems. In total, we're saving hundreds of thousands of dollars per year because of this migration, while setting ourselves up for the future where business will be almost entirely cloud-based."*

CUSTOMER SUPPORT AND ONLINE DOCUMENTATION

In many cases, the developers involved with cloud migrations were relatively new users to cloud technology and complete newcomers to the AWS ecosystem. By having a responsive and educated support group, customers could reach out for help configuring and optimizing their AWS instance. Additionally, all of the tools have documentation readily available online with code libraries, explanations, and examples to help users get answers independently. Given that AWS is an established leader in the public cloud arena with millions of active users, there is regular sharing of best practices and tips to help answer questions in the community. Companies cited the availability of support and documentation as key drivers in selecting AWS; organizations want to create skilled, self-sufficient development teams and felt AWS provided the easiest avenue to achieving this.

- *"The support from AWS frees our internal development teams up to perform value-add improvements and expansions to existing products. When we maintained the infrastructure ourselves, we had an entire team that was responsible. These responsibilities have mostly been passed to our TAM and AWS support team. We've since reduced the internal infrastructure management team headcount by over half and redeployed those developers throughout the organization to value-add development tasks."*
- *"The quality of AWS support exceeds that of any other technology provider we've worked with. The dedicated account team understands the fundamentals of our business and helps us shape and optimize our processes to best leverage AWS capabilities and complement our business model."*



NUCLEUS
RESEARCH

Nucleus Research, Inc. | Boston, MA

Nucleus Research provides the ROI, insight, benchmarks, and facts that allow clients to understand the value of technology and make informed decisions. All research is built on an in-depth, case-study research approach that analyzes the results of actual deployments to provide technology advice built on real-world outcomes, not analyst opinions. Learn more at

NucleusResearch.com