Secureworks®

GUIDE

Migrating to the Cloud

Experts Share Transition Strategies for every data type and organization

Organizations migrating application workloads to the public cloud face multiple alternatives, ranging from simple application like-for-like migration to refactoring to complete replacement with a native cloud solution. Although optimal migration strategies vary according to organizational objective and application criteria, effective cloud security is a constant requirement. Migration to cloud computing is an ideal opportunity to reassess your IT architecture and recalibrate your security framework.

Cloud Migration and Security Recommendations

Organizations are increasingly taking advantage of the speed, agility and cost savings realized by moving application workloads to the public cloud. Since cloud migration is not a "one-size-fits-all" prospect, transition strategies range from like-for-like application migration, refactoring, modernization, and replacement. Strategy selection considerations include migration goals, application and data attributes, functional requirements, and resource constraints.

One constant in every migration strategy is the need for robust information security. Legacy on-premise security approaches are not always effective in the cloud. This means cloud migration is the perfect time to reevaluate and recalibrate your security tools and resources. Transitioning to public cloud computing can seem daunting, yet organizations that utilize smart planning, information and data management, and proactive response can exceed on-premise security levels.

> ***"With cloud, there's a kind of double-edged sword. The same automation that facilitates greater efficiency and agility may be the catalyst that opens a vulnerability without the right configuration hygiene, monitoring and controls."***
>
> — Rob Scudiere - Senior Vice President of Engineering and Chief Information Officer

A Migration Tailored to your business is a Successful One

The ideal cloud migration strategy can vary significantly across organizations, even among different applications within the same company.

"An organization typically has hundreds if not thousands of applications in use across the company. Cloud migration requires evaluating each application against your migration goals and criteria as a starting point,"

- Robert Scudiere, Senior Vice President of Engineering and Chief Information Officer at Secureworks.

Some firms may find that migration options are limited and application migration away from on-premise, such as the case with some legacy mainframe applications, is not possible. In each case, the optimal strategies reflect trade-offs between solution quality, speed-to-benefit and cost goals.

- At one end of the spectrum, a like-for-like or "lift-and-shift" migration process creates virtual replicas of on-premise resources in the new cloud environment. For its speed and affordability, this can be an attractive path to the cloud. Commercial off-the-shelf software from other vendors is not a candidate for lift-and-shift because only the original software vendor can perform architecture changes. Scudiere cautions that, "lift-and-shift can be a highly automated, low-cost option, but you don't necessarily take advantage of all the benefits of the cloud like scalability."
- A second option is to refactor or modify an application to optimize cloud performance and compatibility. Refactoring may improve quality versus lift-and-shift, but it's often slower, more expensive and may not match the benefits of a native cloud approach. Candidates include resource intensive applications such as those that are data and image intensive.
- Finally, cloud migration may entail a completely new, native cloud solution. This generally incurs more upfront investment in planning, time and resources than lift-and-shift or refactoring, but the resulting cloud-optimized solution may offer better long-term quality and cost performance. Alternately, adoption of a commercial Software as a Service (SaaS) solution can deliver native cloud solution benefits without the cost and risk of custom development. The trade-off here is the risk of vendor lock-in and rising subscription fees.

Cloud Security Considerations

In any cloud migration strategy, security is a key consideration. Migration still requires complying with current and even new and emerging industry regulations while preparing for industry audits, in some cases. "Definitely the biggest concern about moving to the cloud is security," says Sanjeev Kumar, Secureworks Global Cloud Security Lead. "Cost, availability, data residency requirements, operations — customers are interested in being secure."

Fortunately, the public cloud can be even more secure than a legacy on-premise configuration, especially for organizations with limited in-house security resources. This improved security is enabled by the facility, technology and staff expertise of major cloud service providers, which may be impractical for an end-user to provide. Unfortunately, these impressive capabilities have a downside because they often create a false perception that the cloud provider's environment is a safe "walled garden." Although the cloud provider plays a critical role, overreliance on them to address every security requirement is a common mistake.

"The important thing to understand for the cloud is that it's a shared responsibility model. The actual roles and responsibilities may vary, but, ultimately, you're storing or posting some of your data on a third-party infrastructure."

- Chris Yule, Senior Security Researcher at Secureworks Counter Threat Unit™ (CTU™)

Cloud security is based on a shared responsibility model, where the cloud provider and the cloud user each bear part of the security role. Here, the security roles are much like those of an apartment landlord and tenant. Like an apartment landlord, the cloud provider is responsible for securing the grounds, building and hallways, but the apartment tenant is responsible for locking up their own doors, windows and property.

When applied to cloud security, the shared responsibility model means a public cloud provider typically provides environmental and physical security, such as hardened facilities and guards for the provider's data center. They also secure core elements of the IT stack, which may entail failover configurations and network perimeter controls.

However, the security responsibilities of the cloud provider generally end at the virtualization hypervisor. Much like an apartment tenant is responsible for securing their apartment front door and valuables, the cloud user is responsible for managing security inside their virtualized environment.

Beyond the cloud's shared responsibility model, cloud-specific technologies and interfaces can create new vulnerabilities and risks. The cloud facilitates easy application and workload deployment, but it's also easy to make errors when learning and implementing a new technology. Digital transformation requires always-on availability of data and applications, for employees, suppliers and customers alike. Identity and Access Management (IAM) is one application that has evolved and a move to the cloud offers increased capabilities and options. Cloud-based IAM application and software features reduce or eliminate error-prone manual processes such as deactivating employees who leave your organization or no longer need access to corporate resources. While cloud applications and tools can be automated and streamlined, people and processes are still critical to oversee security policy and execution.

"Customers look to us because we understand all the different cloud environments. We understand how they can meet the necessary standards across the different platforms and how they can move their security operations and team to the next level."

— Sanjeev Kumar, Secureworks Global Cloud Security Lead

Cloud Security Alternatives

Organizations have two primary options for planning and managing a secure cloud deployment: "do-it-yourself" (DIY) or "find a good partner."

A big challenge for the DIY approach is the critical scarcity of qualified cloud security talent. It's a "perfect storm" — the only thing in shorter supply than people with cloud technology skills or people with security skills is people with both cloud and security mastery. Also, although on-premise security is traditionally a responsibility of IT, the shared responsibility model of the cloud creates new challenges and responsibilities. "A key requirement with cloud security is the need for cross-functional collaboration," said Chris Yule, Senior Security Researcher for Secureworks Counter Threat Unit™ (CTU™). "It's not just an IT security problem. Much of cloud security is a contract, auditing and vendor management piece, which is often done by a completely different part of the organization." If the DIY effort lacks the necessary skills and organizational alignment, it may fail in its cloud transformation role or to even protect assets and data.

Alternately, organizations may augment in-house capabilities with an external cloud security partner. Here again, it's tough to find qualified talent and looks can be deceiving. A house painter and a portrait artist both use similar-looking tools and techniques, but they aren't equally qualified for the same jobs. Effective cloud security collaboration requires the right provider with the right expertise.

Secureworks Cloud Security Solutions

To meet these challenges, Secureworks offers the industry's broadest portfolio of security solutions designed to help organizations securely take full advantage of the cloud and hybrid IT. Secureworks provides end-to-end coverage of all stages of your cloud deployments — from initial evaluation and architecture to ongoing assessments and monitoring. Services include:

Cloud Security Assessment

We help you understand strategies such as cloud adoption implications, insights on how to integrate cloud into your existing environment and even how to assess and select a cloud services provider. Our services help organizations make the right choices in their cloud investments, including governance and security strategies.

The first step often involves planning and vendor selection. Picking the right cloud provider at the beginning helps create the right foundation for your secure operations and response. Our cloud provider security assessments include reviews of key staff, documentation and processes relative to applicable security frameworks and best practices.

> ***"With cloud, there are a number of key things you should always do and we can help at every stage. We not only have the impartiality, we have the expertise and take a holistic view. We know what good looks like and how to find the blind spots the customer maybe hasn't thought about at all."***
>
> — Chris Yule Senior Security Researcher at Secureworks Counter Threat Unit™ (CTU™)

Cloud Security Design & Architecture

We assess your current architecture and its impact on your security posture in the cloud. We work with you to create a cloud architecture that scales as your organization changes and grows over time. With a comprehensive cloud design in place, we help you implement security processes and services that address your unique risk, compliance and operational requirements.

Cloud Penetration Testing

We leverage proprietary tactics and intelligence from Secureworks Counter Threat Unit™ (CTU™) Research Team to simulate potential threats and test your cloud infrastructure to minimize risks from cyber threats.

Independent validation of cloud provider security and penetration testing of your own cloud environment is essential. Secureworks delivers a rigorous penetration testing model that not only seeks out vulnerabilities, but also evaluates diverse attack vectors such as social engineering risks, compromised credentials or a bad actor in your organization or the cloud provider.

Managed Cloud Services

We monitor, analyze and distill the thousands of cloud events logged each day into prioritized, actionable security intelligence. This facilitates fast, effective risk mitigation, improved productivity and cost savings for your team. Our managed solutions continuously strengthen defenses and ensure that clients are able to protect and maintain control over their sensitive information and assets.

Cloud Incident Response

Helps organizations respond rapidly to, and minimize the impact of, a security breach. Services include proactive incident management and response, forensic investigation, and incident coordination.

When compared to a conventional on-premise environment, a properly configured public cloud can facilitate a drastic reduction in the time and effort required to identify, isolate and respond to threats. The accelerated response and agility enabled by the public cloud helps reduce the potential damages and costs of a security breach.

Next Steps to Secure Your Cloud Migration

Successfully and securely migrating on-premise workloads and leveraging new technologies offers the opportunity to transform your organization and enhance agility and competitiveness. Your decision to migrate applications allows you to recalibrate your approach and evaluate cloud benefits like scalability going forward. Secureworks has the cloud expertise and proven track record to build security into every step on this journey. Our cloud security consultants can balance diverse workload migration and security goals into a safe, actionable roadmap for your cloud success.

Featured Secureworks Experts

Sanjeev Kumar

Secureworks Global Cloud Security Lead Sanjeev has 14 years of experience in information security consulting, cloud security, cloud service provider strategy and business continuity. Sanjeev has led large, complex information security engagements around the globe. He holds an advanced degree in Computer Science with multiple technology certifications.

Rob Scudiere

Senior Vice President of Engineering and Chief Information Officer Rob Scudiere is responsible for Secureworks software engineering and the intelligence-driven Counter Threat Platform™ (CTP). The Platform is the core of Secureworks information security solutions which analyzes billions of events to prevent, detect, respond and predict threats across our client's data centers, cloud infrastructure, mobile devices and endpoints.

Rob has more than 25 years of experience managing and operating world class products and solutions across a variety of industries, primarily focused on managed security and cloud services. He is a graduate of Bentley University and the Harvard Business School Executive Education Program.

Chris Yule

Senior Security Researcher at Secureworks Counter Threat Unit Chris is a senior security consultant with more than 10 years of experience across firms of all sizes and vertical industries. He leads cloud, mobile and threat intelligence security strategy and advisory projects for European organizations within Secureworks.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.