Solution Flyer
Security

Security and Compliance in the Cloud: Build a Cloud-Ready Security Program

Cloud computing offers flexibility and savings, but as data, systems and services move to the cloud, organizations expose themselves to serious security and compliance challenges.

"… you have to think less about (the) perimeter and you have to think more about the data and the identities that are going to be managed, and managed anywhere, and you have to make an assumption that they're not secure channels."

JAMES STATEN
Vice President, Principal Analyst
Forrester Research

Cloud computing is highly disruptive. Not only does it change the way an organization gets its services, it also changes the way in which users (individuals and business units) interact with central IT and security teams. Data, systems and services are moving rapidly outside of the control of centralized IT organizations, presenting significant risks to the security of sensitive data and the ability of the organization to maintain compliance with industry regulations and corporate security policies. You need a way to effectively mitigate these risks while ensuring that you achieve your business, security and compliance objectives.

Understanding Your Business Challenge

Cloud computing greatly increases an organization's ability to achieve its business goals. It also introduces complexity to IT environments that significantly expands the scope of work required to securely deliver services to end users. Because of the cloud's interconnected nature, it is possible for an attacker who identifies a single vulnerability to compromise a vast number of systems.

With so much potential for damage, it is important to have a good security program in place prior to implementing cloud technology. A "cloud-ready" security program will help you manage the complexity and risk introduced by the cloud. Additionally, the program will effectively scale throughout mixed environments made of both traditional and cloud (public and private) components. Cloud-ready security programs are data centric, focused on risk mitigation, and help teams to maintain continuous security and compliance.

Data-Centric Threat Defense

You can no longer effectively mitigate data security and compliance risks simply using traditional approaches. Instead of continuing to focus protection on a perimeter that now extends well beyond traditional borders, security professionals now target proven security controls at the data itself—wherever it may reside—as the most effective way to protect sensitive data and meet compliance objectives.

Proactive Risk Management

You must achieve and maintain alignment with key business objectives to successfully balance the demands of users who want 24-hour access to cloud services with those of business stakeholders. To do this, you must work proactively with the business to mitigate security and compliance risks for sensitive systems, whether they are on premise or reside in a third-party cloud infrastructure.

Continuous Security and Compliance

Being compliant with industry regulations and policies cannot shield you from security breaches. To reduce risks, you should build continuous processes that put in place—and keep in place—good security controls. With security as the goal, compliance becomes a measure of the organization's security "health" and you achieve it as a result, or by-product, of good security.

Resolving Your Business Challenge

Micro Focus believes that security teams need heightened visibility and control of their mixed environments to more quickly detect and disrupt threats to sensitive data and systems. Our

integrated and automated solutions work together to help teams build continuous security and compliance processes that focus protection at the data level and deliver effective risk mitigation and management.

Our advanced approach delivers the capabilities security teams need to more easily and reliably deliver a cloud-ready security program.

Secure the Data, Not the Cloud

We focus on the most sensitive systems and users, and surround them with defensive layers. We help ensure the security of your most critical traditional, private cloud or infrastructure as a service (IaaS) environments by delivering solutions that proactively monitor and report on the activities of privileged users and on the integrity of critical systems and files. Additionally, we ensure that users have only the rights they need to business systems and services when they need them, throughout the employee (or contractor) lifecycle. Our data-centric approach provides:

- User activity monitoring for greater visibility into unusual behavior or unauthorized access to sensitive files.
- System configuration assessment to help teams correctly configure systems to meet security best practices.
- Security event and change monitoring capabilities that deliver real-time detection of accidental or malicious changes to sensitive files and systems.

Manage Risk Proactively, Including at Initial Assessment

We provide timely and effective decision support to security teams that must respond rapidly to threats in both their traditional and cloud environments. For example:

- We provide risk reporting that helps prioritize the remediation of potential vulnerabilities based on the threatened asset's value.
- Our solutions enrich security event data with context about user identity, data, applications, assets, threats and vulnerabilities to help you discern true threats from noise.
- We provide risk management and mitigation before, during and after project implementation.

Implement Foundational Security, with Compliance as a By-Product

We believe that being compliant does not mean you are secure. Therefore, we help teams build processes that ensure organizations put good security controls in place in a continuous manner. In this way, you achieve compliance as a by-product of your organization's security, and do not treat it as a standalone task. Our solutions:

- Provide automation and integration to ensure you can deliver processes reliably and scale them efficiently to help reduce complexity brought about by emerging technologies, services and changing IT operations.
- Ensure systems and policies remain in compliance with industry standards and best practices by delivering rich security intelligence and content.
- Promote greater risk visibility for executive stakeholders to help them make better business-risk decisions.

Micro Focus's Identity, Access and Security Management solutions integrate seamlessly to help you control access to cloud services and data, reduce your risk of data breaches in mixed environments, and achieve compliance with industry regulations and security policies in the cloud.

The Power of You and Micro Focus

With the emergence of such consumer-driven technologies as mobile computing devices and user-initiated cloud applications in the workplace, organizations of all sizes find themselves struggling to understand how these business-enabling technologies impact the security and compliance of their critical data and systems.

Micro Focus understands that the traditional approaches to mitigating data security and compliance risks are no longer effective by themselves and that you require a comprehensive solution. Our suite of Identity, Access and Security Management solutions integrate seamlessly to help you control access to cloud services and data, reduce your risk of data breaches in mixed environments, and achieve compliance with industry regulations and security policies in the cloud.

Products

- **NetIQ® Secure Configuration Manager™**—Helps ensure you consistently enforce security policies across traditional, private cloud and IaaS environments.
- **NetIQ Change Guardian**—Details privileged user access and changes to sensitive data and systems in traditional, private cloud, and IaaS environments, providing teams the control and visibility

A cloud-ready security program will help you to proactively detect and disrupt threats to sensitive data and systems in mixed IT environments, securely deliver business services that reside in—or originate from—the cloud, and achieve compliance with industry regulations.

Contact us at:
www.microfocus.com

Like what you read? Share it.

they need to rapidly detect and disrupt threats.

- **NetIQ Sentinel™ Enterprise**—Provides integrated security information and event management (SIEM) to identify cloud services accessed from the network, affording greater control and faster response to an attack.
- **NetIQ Directory and Resource Administrator™**—Provides protection in and out of the cloud by limiting the number of people with Active Directory domain rights, improving the security and efficiency of back-end Active Directory administration.
- **NetIQ Access Manager™**—Provides a single sign-on experience to internal and cloud-hosted applications, making access secure and convenient by allowing only authorized users while eliminating the need for users to save passwords in an unprotected format.
- **Micro Focus® CloudAccess**—Extends identity and access management beyond the organization's walls out to cloud-hosted software as a service (SaaS) applications.
- **NetIQ Identity Manager**—Lets you standardize user management and allows you to create a single, rich identity store for your organization.

MICRO FOCUS