opentext™ | Cybersecurity

Position Paper

Managing Policies in the Age of the Multicloud

In today's world, a hybrid, multicloud environment is nothing new—most companies have been moving workloads to SaaS applications and the cloud for years. But recently, as companies created remote working environments nearly overnight, the move to the cloud has shifted to warp speed. As Microsoft CEO Satya Nadella said in April 2020, "We've seen two years' worth of digital transformation in two months."

Whether it's accomplished in days, months, or years, moving to a multicloud, multi-vendor environment brings distinct advantages. Each cloud provider offers a unique service, and working with a variety of vendors allows companies to adopt solutions best suited for their particular needs.

But in their haste to adopt cloud-based solutions, many organizations have yet to realize the serious security and compliance problems that can arise in a scattered, hybrid environment. Among organizations that required remote work as a result of the COVID-19 pandemic, 76 percent said it would increase the time to identify and contain a potential data breach, according to the Ponemon Institute's 2020 Cost of a Data Breach report. Unless organizations have the right processes and management tools in place, security problems are bound to occur as they move additional applications and services to the cloud.

Many organizations erroneously believe cloud-based applications afford them the same protections they have in their on-premises environment. In reality, this assumption is simply not true.

Many organizations erroneously believe cloud-based applications afford them the same protections they have in their on-premises environment. In reality, this assumption is simply not true. Unless they take steps to ensure that their security and configuration policies are constantly enforced throughout the organization—at offices, across all devices and endpoints, and in all cloud-based apps and services, regardless of vendor—companies are setting themselves up for security gaps and compliance violations.

The Policy Configuration Conundrum

The move to a hybrid working environment has enormous implications for security and compliance. The tools most organizations use for setting and enforcing security policy—Microsoft Group Policy and Active Directory—were developed for an all-Windows system using on-premises Windows servers.

Group Policy and Active Directory weren't designed to work in the cloud, where the vast majority of SaaS applications use Linux servers. Big public cloud providers such as AWS and the Google Cloud Platform run on Linux machines and servers. Even 75 percent of the resources in Microsoft's Azure Cloud run on Linux systems. Common business apps like Salesforce, Box, Slack, and a host of others use Linux, and so do many companies' in-house-developed custom applications.

As technology has moved to the cloud, the workforce has followed. Even before the work-from-home movement went into overdrive recently, employees were conducting business not only on Windows PCs, but also on laptops, tablets, and smartphones using a variety of operating systems.

These changes have made managing security and compliance much more complex. Lacking the tools to manage security policy overall, some IT workers have created scripts to manage security settings for machines and applications outside the on-premises Microsoft environment.

Writing scripts is a laborious process filled with pitfalls. First, administrators must create security settings and access rights for operating systems. Then they have to create other sets of access rules for individual applications. Each server and each app must be configured separately, and they don't all use the same language to manage similar configuration items and security settings. These piecemeal procedures are tedious and introduce opportunities for errors and misinterpretation. In addition, script writing—even writing simple configuration scripts—is highly idiosyncratic. Code written by one administrator may be difficult or impossible for others to understand.

Outdated and noncompliant security settings are extremely dangerous. Hackers are continually trolling the internet looking for loopholes that can give them a foothold onto corporate networks.

Alternatively, organizations may use configuration managers such as SUSE Manager, AWS CloudPlatform, Red Hat Ansible Automation Platform, or others to configure security policies outside of Microsoft. But, as with scripts, rules may easily be overturned. Once a configuration item is set, other administrators with access rights to the system can immediately change and overwrite it.

It happens all the time. If someone changes settings to use a different port, add services, or grant access to new users, their actions may bring the organization out of compliance with state or federal regulations, or with the company's security policy. Individual application administrators may also fail to keep up with patches and updates. Without centralized policy management to provide an enforcement mechanism, the organization has no way of knowing these problems exists, much less solving them.

How Security Policy Errors Can Cause a Breach

Outdated and noncompliant security settings are extremely dangerous. Hackers are continually trolling the internet looking for loopholes that can give them a foothold onto corporate networks. Organizations that don't centrally manage security are handing them a golden opportunity. Here are just a few notorious examples of breaches that have occurred as a result:

- **The Equifax breach (2017).** The names, Social Security numbers, addresses, dates of birth, and driver's license numbers of 143 million people were stolen after hackers entered the network through a customer complaint web portal, which contained a known vulnerability that should have been patched earlier.

  In addition, the company had failed to renew a security certificate for an application that otherwise would have alerted it right away to the presence of the intruders on its network. Instead, the intruders were able to give themselves elevated permissions and remote access. They lingered for 76 days as they mined for and exfiltrated valuable data.

- **The Federal Depository Library Program breach (2020).** The Federal Depository Library website, which helps the public access government documents, was hacked to display messages calling for revenge for the death of an Iranian military commander. It showed images of the Iranian flag, Ayatollah Ali Khamenei, and a doctored photograph of President Trump being punched in the jaw. The hackers got into the website through a misconfigured content management system, the U.S. government later said.
- **The JPMorgan Chase breach (2014).** Cybercriminals gained high-level administrative access to more than 90 servers after the bank neglected to upgrade one of them with a multifactor authentication requirement. Names, email addresses, and phone numbers of 76 million households and 7 million small businesses were stolen.

The Solution: Universal Policy Administrator

If organizations consistently enforced their security policy across all operating systems, apps, and devices, they would prevent many breaches and minimize the impact of others. NetIQ Universal Policy Administrator (UPA) by OpenText™ automates the enforcement of security rules and configuration settings everywhere. It allows managers to view and control security settings from a single pane of glass using a very familiar tool: Microsoft Active Directory. We've extended it to apply far beyond Microsoft devices. Mobile devices, virtual machines, Linux servers, SaaS apps—you can place them all under centralized policy management with UPA. UPA even covers kiosks and other endpoints that are not connected to the corporate domain.

NetIQ Universal Policy Administrator (UPA) automates the enforcement of security rules and configuration settings everywhere. It allows managers to view and control security settings from a single pane of glass using a very familiar tool: Microsoft Active Directory.

Once UPA is in place, if a policy violation occurs—for example, if someone changes configuration settings—the system immediately notifies the appropriate administrator. Unless the administrator responds with a policy change, settings automatically revert to their previous state within one minute. Even privileged users cannot deviate from policies.

When hackers gain access to a company's computer, they often disconnect it from the corporate network so they can make changes undetected. But with UPA, all policy files are cached, so even a disconnected computer will reject the changes and revert to standard policies within a minute.

If Equifax had used UPA, it would have spotted hackers' access to its network in one minute or less. Perhaps a few dozen accounts would have been breached, instead of millions.

At the Federal Depository Library, the unauthorized changes to the website's index file would have been noticed instantly and replaced with the previous, authorized version.

At JPMorgan Chase, hackers gained root-level access to servers by listing themselves as "sudoers" with administrative privileges. UPA would have recognized the phony sudoers as imposters, kicked them off the site, and notified the real administrators.

Flexibility with Additive Policy Management

UPA is comprehensive, but it is also flexible. Additive policy management allows organizations to create unique custom policies for specific applications, machines, and servers. They can sometimes more easily enforce the principle of least privilege by creating groups of local administrators who can determine who needs access to applications or machines, at what times they need it, and for how long. An administrator who leaves the company or moves to a new position is simply removed from the group providing access, without anyone having to manage local user accounts and access.

Additive policy management gives control over resources to the people who understand them best—those who are closest to them. It also means that fewer human hands are needed for configuration, so there are fewer opportunities for mistakes or conflicts.

Easier Compliance Audits

PCI DSS, HIPAA, FINRA, GDPR, the California Consumer Privacy Act—the list of regulatory agencies and rules that organizations are required to follow is long and growing as public demands for data privacy increase. Enforcement of these rules becomes more difficult as organizations increase the number of network-connected devices and services they use. A large retailer, for example, might have tens of thousands or even hundreds of thousands of Linux endpoints, with perhaps a hundred administrators managing them.

To ensure that compliance rules are followed uniformly, organizations can have the CISO or chief compliance officer define common and custom settings that are pushed through UPA to all the Windows, Mac, and Linux servers and applications the organization uses or adopts in the future.

In addition to making compliance administration much easier, this system helps auditors. UPA's central portal allows them to obtain all the information they need in one place. Without it, the organization has to rely on spreadsheets containing raw security and configuration data from hundreds of business unit administrators. It must collect all this information and hand over to auditors.

Simply having a security policy in place is not enough to satisfy today's auditors. They need to see proof that it is being enforced. Without a central information portal, they may spend weeks or months sifting through data sheets with a fine-tooth comb. With so many different people putting them together, they are bound to find inconsistencies and errors, leading them to mistrust the organization and demand even more evidence. The longer auditors stay, the higher the cost to the organization. The end result could be an embarrassing failed audit and fine.

Simply having a security policy in place is not enough to satisfy today's auditors. They need to see proof that it is being enforced. Without a central information portal, they may spend weeks or months sifting through data sheets with a fine-tooth comb.

With UPA, auditors' work is vastly simplified and shortened. Because security is enforced and reported on universally and consistently, they have the proof that automated processes are in place and working. Everything they need is at their fingertips, and they are much less likely to find any violations.

Automation: The Key to Better Security

As organizations accelerate their presence in the cloud, they must replace outdated security management tools with solutions that work across boundaries. Without centralized, automated security policy management, they place themselves in danger of experiencing a breach.

Because their response is delayed if a breach does occur, they also suffer worse consequences from it. The Ponemon Institute has consistently found that the faster a data breach can be identified and contained, the lower the costs. In this year's report, businesses without security automation had an average breach cost of $6.03 million, more than double the average cost for those with a fully deployed security automation system in place.

With UPA, you can be certain that your security rules are enforced throughout the enterprise at all times across Windows, Mac, Linux, and non-domain-joined resources.

Instead of having IT administrators write complex scripts or use an array of policy managers for outside applications and servers without oversight, you simply use Active Directory and Group Policy to control your security and policy configuration—just as you have always done within Microsoft. Every server, app, or device you move to the cloud is scrutinized in advance to ensure security, compliance, and compatibility. With additive policy management, you can choose to delegate some decisions to local administrators you trust.

As your company moves more workloads to the cloud, you need a security policy solution that moves with you, not against you. UPA makes the transition easy and gives you the visibility and control you need in a multicloud workplace that is no longer constrained by geography.

The NetIQ Advantage

As your company moves more workloads to the cloud, you need a security policy solution that moves with you, not against you. UPA makes the transition easy and gives you the visibility and control you need in a multicloud workplace that is no longer constrained by geography.

About NetIQ by OpenText
OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/universal-policy-administrator

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.