CXO FOCUS

SECURITY IN THE COVID-19 ERA: **DO YOU HAVE THE RIGHT PROTOCOLS IN PLACE?**

—

OCTOBER 2020

POWERED BY

NUTANIX™

Cloud computing has never been so essential to business continuity as it has over the past six months, as remote working has become a necessary practice — one that will likely persist even after the threat of COVID-19 subsides. In fact, Gartner reports that 82% of company leaders plan to allow employees to continue working remotely at least some of the time.

As businesses adjust to this workplace paradigm shift, digital activity is skyrocketing. Remote employees across industries rely on digital channels and cloud platforms to connect and collaborate every day, from their homes and other remote locations. Cybercriminals have taken notice, and they've turned up the heat. Here are some alarming statistics:

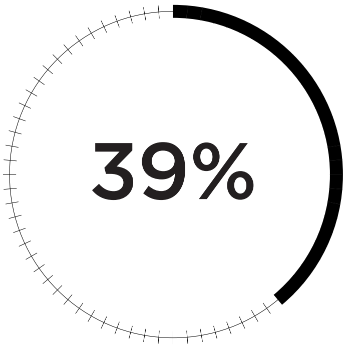
- Scams grew by 400% in March, making Covid-19 the largest security threat ever.

- According to an IDC report, 39% of companies surveyed experienced phishing attacks, 34% suffered malware attacks, and 27% experienced DDoS attacks.

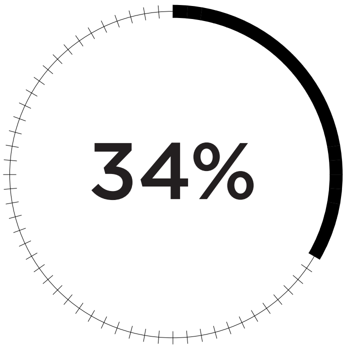
- Web application breaches account for 43% of all breaches this year and have doubled since 2019. Cloud-based applications are a likely target for bad actors, and the leading channels for breaches are file sharing apps (68%), web apps (47%), and video conferencing (45%).

- Not only has remote working contributed to an increase in the number of breaches, but the cost of each breach is higher — to the tune of $137,000 per breach.

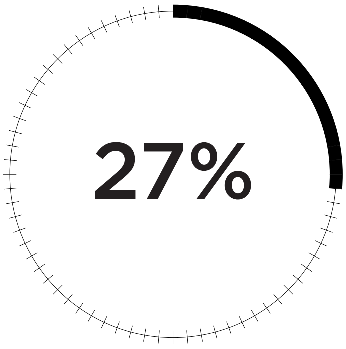
IDC suggests the rising adoption of cloud services to support remote workers during the pandemic could be one of the major reasons cybercrime has increased. As organizations hurried to shift business-critical applications to hybrid and multicloud environments, the attack surface grew rapidly, and IT departments may not have had the time to implement adequate security protocols.



of companies surveyed experienced phishing attacks



of companies surveyed suffered malware attacks



of companies surveyed experienced DDoS attacks

Traditional Security Tools Fall Short

Despite the many effective security features available from cloud providers, securing critical applications and data while staying in compliance with regulatory mandates continues to be a challenge. Add that to the fact that remote workers are connecting using unprotected endpoint devices and home networks, and you've got a security nightmare.

To address this issue, CISOs and cybersecurity-operations teams are strengthening perimeter security, leveraging next-generation identity and access controls, enabling secure remote access, and providing employees with training, according to McKinsey. But IT budgets are shrinking, and security executives may not have the funds available to adopt advanced threat intelligence solutions, behavioral analytics, or other tooling.

Even when security features are implemented, they fail to get to the root of the problem — platform misconfigurations.

Multicloud Environments Are Plagued by Misconfigurations

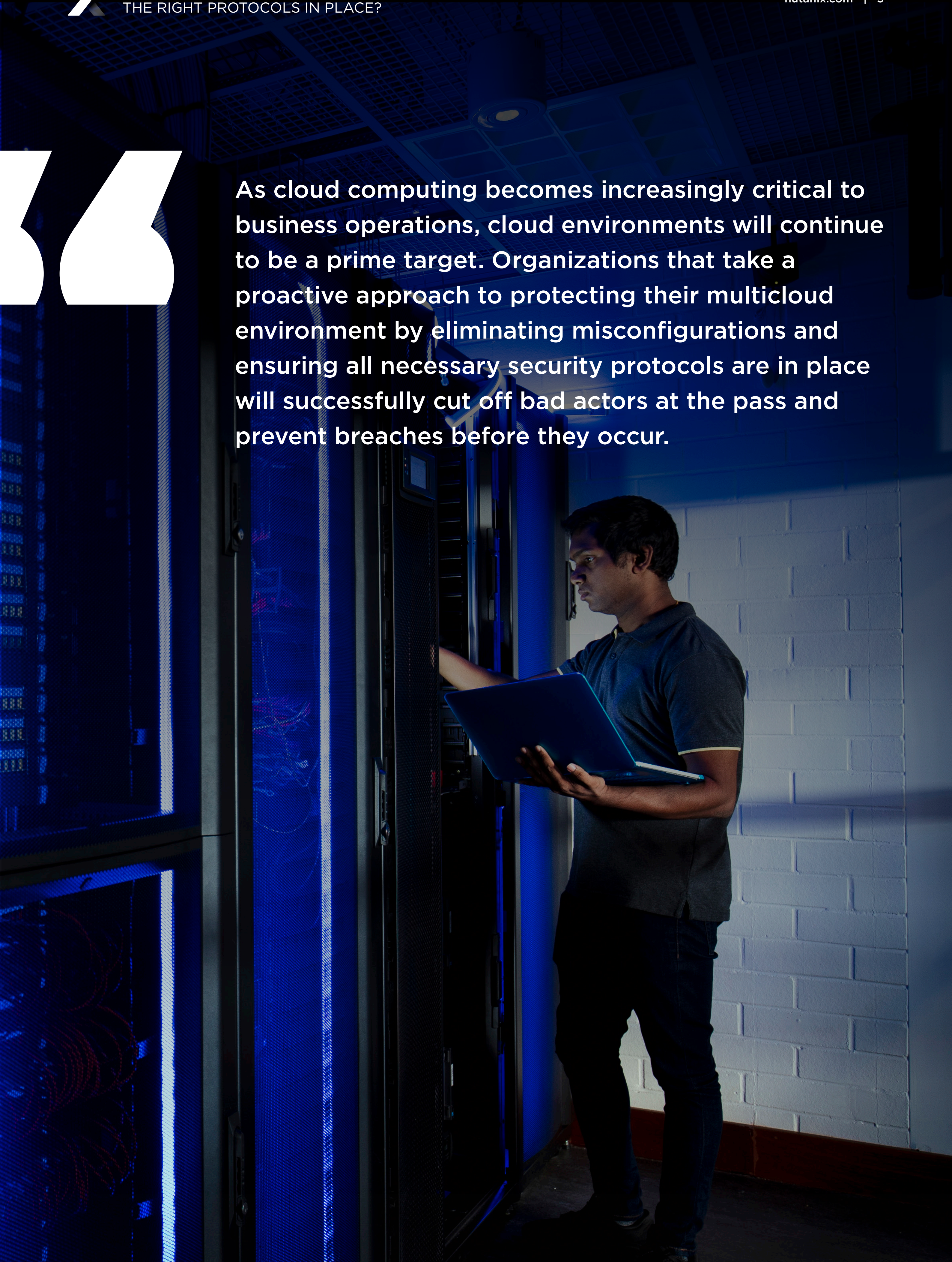
Many organizations are adopting a multicloud approach to benefit from optimal pricing and the best services for various needs, while avoiding vendor lock-in. However, in a multicloud environment, security risks increase. When workloads and applications are spread across multiple platforms, misconfigurations are common.

Misconfigurations create vulnerabilities, leaving the door wide open for cybercriminals to wreak havoc. For example, configuring a storage repository with global read/write permissions or leaving virtual machines exposed to public or external IPs over TCP or UDP ports can open the door for bad actors to initiate an attack. In complex multicloud environments, IT administrators are often overwhelmed by having to manage a high number of separate technologies, resulting in these types of misconfigurations.

In its State of DevSecOps Report, Accurics revealed that misconfigured cloud storage services and poor security practices have caused more than 200 breaches in the past two years and were prevalent in 93% of the cloud deployments researchers analyzed. Overly permissive IAM policies and misconfigured routing rules were also pervasive. The problem is so prevalent that Gartner projects misconfigured cloud resources will cause 95% of cloud security breaches by 2022. Not only can misconfigured cloud resources lead to data breaches, they make regulatory compliance impossible.

Simply adding on security features to protect against cybercrime is like putting a bandaid on the problem. Instead, organizations should work to ensure cloud platforms are configured correctly in the first place.

> As cloud computing becomes increasingly critical to business operations, cloud environments will continue to be a prime target. Organizations that take a proactive approach to protecting their multicloud environment by eliminating misconfigurations and ensuring all necessary security protocols are in place will successfully cut off bad actors at the pass and prevent breaches before they occur.



Proactive Security Measures and Self-Healing Features Close the Gap

Here are a few best practices to combat the problem of misconfigurations in complex multicloud and hybrid cloud environments, and ensure you have the right protocols in place:

- Implement a Zero-Trust approach: It's important to assign data and network access rights based on the bare minimum required for individuals and applications to operate. This involves segmenting applications, virtual networks, enterprise servers, VMs, and services into separate accounts. Isolating resources in separate accounts creates a security boundary to guard against potential network threats and reduce risk.

- Leverage automated self-healing configurations. A cloud platform that employs event-driven detection automatically runs security audits whenever an event happens anywhere within the cloud environment. For example, configuration changes to cloud services, user onboarding, or software and hardware changes all trigger security checks. Alerts are automatically sent to cloud security teams if any vulnerabilities or issues are discovered. In this way, teams can take immediate action to correct a misconfiguration, remediate an issue, or implement missing security protocols.

- Audit and report on regulatory compliance. Automated compliance audits simplify the process of detecting and remediating vulnerabilities — and they also serve to validate compliance with regulations and policies. Audits can be initiated to check the security policies of virtual machines that could be exposed to external IPs, or for instance, to ensure data encryption is enabled. Ongoing monitoring and logging is also critical to provide continuous visibility into your cloud infrastructure.

A Proactive Defense is the Best Defense

Data breaches and cybersecurity incidents are a fact of life for organizations in every industry, and bad actors will always try to take advantage of vulnerabilities. As cloud computing becomes increasingly critical to business operations, cloud environments will continue to be a prime target. Organizations that take a proactive approach to protecting their multicloud environment by eliminating misconfigurations and ensuring all necessary security protocols are in place will successfully cut off bad actors at the pass and prevent breaches before they occur.