GUIDE

PROPER AWS CYBER HYGIENE DURING THE REMOTE WORKFORCE ERA

As the COVID-19 crisis continues its hold on the nation, cybercriminals have been using the uncertainty and unease as a window through which to exploit the situation for personal gain. InterVision's cybersecurity specialists have already seen, and helped clients overcome, a significant rise in malware, phishing and ransomware incidents as critical information continues to shift from offices to work-from-home environments. The expanded attack surface of each employee's home office rather than a singular office location means that businesses, overall, are less secured. As a result, IT departments now have hundreds or thousands of "offices" to secure, which can be much more difficult to do, given these attack vectors are remote and therefore, less visible.

InterVision has gathered some important cyber hygiene tips from our team of cybersecurity experts. These tips will help keep your business secure as your employees continue to operate business from their homes. Many organizations are embracing the cloud for accessibility and flexibility during uncertainty, using virtual desktop infrastructure (VDI) and cloud-based application hosting platforms to deliver connectivity and critical application access for employees. The AWS cloud is the most popular, with 32% of the market, according to a recent report from Canalys. From this perspective and for the purposes of brevity, these tips dive into specifically how to secure AWS technologies for a remote workforce. However, the rationale and intent behind these tips apply to all cloud service providers.

**The content of this guide appeared originally as an article in IT Toolbox.*

TIP 1

PROVISION SECURED ACCESS & AUTHENTICATION

When you have employees working from anywhere, corporate office space or from home, you need to secure their access to perform duties while excluding outsiders from accessing those same assets. This means **integrating with existing directory and authentication services** to reduce administrative overhead and increase control. Using multi-factor authentication significantly strengthens your security and is highly recommend. Digital certificates for additional device identification and policy-based limitation can further strengthen your security posture.

When it comes to AWS's VDI solution, WorkSpaces, you should be sure to protect and monitor administrative functions such as key rotations, group membership changes, image imports, tag deletions, etc. **Use metadata and tagging of WorkSpaces resources** to keep effective track of, organize, and manage against intended privacy and security restrictions; however, avoid storing confidential information in the tags themselves. Leverage and fine-tune extended AWS tooling such as AWS Security Hub to have regular compliance validation measures in place for WorkSpaces. When you are in the provisioning process of WorkSpaces, streamline the applications needed for users; separate applications into containerized instances via WorkSpaces Application Manager to simplify deployment and management of the base images/bundles apart from your users' needed software.

TIP 2

VERIFY COMMON ENDPOINT PROTECTIONS

Even though VDI with AWS WorkSpaces brings some additional inherent protections, continue to **use (and improve) all the standard endpoint controls** needed to secure at-risk desktops from common threats such as ransomware; this is especially true for Windows-based systems. Consider a well-pruned custom image; similar to the principle of least privilege, reduce the surface area of attacks and exploitations by removing software that isn't needed even down to a particular group or role. Ensure you're comfortable with the included Trend Micro endpoint solution in certain bundles, otherwise package your preferred solution alternatively.

AWS AppStream 2.0, which is cloud-based application hosting, elevates endpoint protection of critical assets away from employee devices to the server level. Employees need only have a secure internet connection to perform their role, which means your team can worry less about the security posture of each device.

More broadly in AWS, **encrypt all storage systems**; the slightly additional cost and performance impact are almost always warranted. AWS KMS is easy-to-use and supports customer-provided and managed keys if needed. Once you have this provisioned, test backup recovery of files, of images, etc. Really test it end-to-end, not just a sample file restore. No really...don't set yourself up to figure this out in the middle of a crisis.

Patch, patch, patch for every application, library, etc. that may be unique and outside supported images; it's much easier to use a patch and release pipeline in WorkSpaces than rolling upgrades out in conventional desktop deployments, so use this to your advantage.

TIP 3 LEVERAGE COMMON NETWORK CONTROLS & AWS TOOLS

Beyond the foundations of restricted access and endpoint protection lies the important governance aspects of preventing malicious actors from identifying alternate vectors. Having a solid governance policy that requires gated network connectivity to perform tasks is just one way of allowing your business to evolve to challenges as they arise.

Consider bringing your company's connectivity through a supported VPN connection, leveraging the system to catch known and suspicious issues. **Set up policy-based cloud controls for network isolation and segmentation** such as VPC security groups, public/private networking, whitelisting of IPs, VPC endpoint policies, etc. By turning on flow logging, the system will feed into GuardDuty, which in turn should feed into Security Hub.

Once you have a foundation for this new normal of networking in place, then your staff can begin searching for new, innovative solutions to further iterate the protection of your network and connectivity.

TIP 4 RAMP UP LOGGING

Part of maintaining strong cybersecurity during an era of remote workforces demands keeping an eye on who has accessed what and why. For this reason, your IT department should ramp up how intricately you track change management activities. With IT staff spread out, it's imperative to know if a task has already been performed or not, so that you can retrace any steps if something goes awry. Not being in an office together means you no longer have the luxury of turning to a team member and asking about performed duties. **Logging is a quick way to keep track of everything.**

CloudWatch Events and Metrics can be useful for security, additional to cost and performance metrics, allowing administrators to review activities from a holistic perspective with drill-down capabilities. When using your logging tools, **check for unusual connection/disconnect metrics and events from unusual IPs or platforms not expected.** Aggregate and collect all access, authentication, authorization, system events, local application events, encryption events, administrative utilization, network flow, security detections, etc.

Be sure to set alerts for the above aggregated items. Ensuring these are being recorded, received, acknowledged, and responded will be key to the review process later. Don't let red flags pile up and get ignored.

aws partner network

Premier
Consulting
Partner

Migration Competency
DevOps Competency
Storage Competency
Education Competency
Government Competency

REMOTE WORKFORCES REQUIRE A BUSINESS TO REMAIN NIMBLE

In the end, the COVID-19 crisis has taught us a lot about what it means for a company to be prepared and flexible to new challenges as they arrive. Cybersecurity professionals, in order to truly keep their business guarded against threats, must embrace new models of connectivity and office work. We know this can be challenging as remote work can go against many norms of due diligence, but the traditional nature of office work will never be the same again. It's up to the IT department in each company to not only outfit the business for the moment at hand, but also prepare for the next wave of uncertainty, **keeping the technology ecosystem flexible and secure to evolve as needed.**

ACCELERATE YOUR STRATEGIC JOURNEY WITH AWS

The AWS cloud offers unprecedented advantages in terms of scale, flexibility, cost savings and security. However, operations in AWS require different expertise and processes than on-premises environments.

As a certified AWS Premier Consulting Partner, InterVision takes a consultative approach to help organizations migrate to the cloud, secure and optimize their cloud operations, and leverage the development cycle of application environments. With a team of AWS certified architects and engineers backed by our matured process and technology partnerships, we empower clients to get the most out of their AWS operations.

InterVision

InterVision, an AWS Premier Consulting Partner, unlocks value through the evolutionary power of technology through a consultative approach.

Let's connect to find ways to protect and defend your remote workforce.

Click to dial
844.622.5710

Click to visit
www.intervision.com