FROST & SULLIVAN

Lessons Learned from 2020 for **SUCCESSFUL HYBRID CLOUD SECURITY**

WHAT IS DRIVING THE NEED FOR ADVANCED HYBRID CLOUD SECURITY?

- **Hybrid cloud grew** in 2020 as **businesses needed it to manage a dramatic growth in data generation and usage. 60% of businesses say the cloud enables them to be competitive**
- **Cloud flexibility** means **businesses can quickly scale up and down applications and processes**. 80% of companies want to use the cloud to automate routine tasks
- A recent Frost & Sullivan survey of **IT professionals** shows **multi-cloud adoption grew 54% and hybrid cloud usage increased 14% in 2020**
- **Security challenges also rose in 2020:** more **malware** and **phishing attacks**; **higher ransomware sums being demanded**, and **more vulnerable end points created by the expansion of IoT devices** and **the move from office-based data access to a remote work**

HOW TO SUCCEED IN TODAY'S DATA-DRIVEN WORLD

Look at the bigger (corporate) picture:

Well-intended security strategies fall flat when not aligned with business objectives, or if lacking broad executive stakeholder support. (Bonus points if you can create silo-busting strategies that also make workflows more secure and efficient)

Secure the data, everywhere:

How secure is your hardware? Are your suppliers or customers potential threat vectors? Data needs to be secure within—and beyond—your four walls

Hybrid is essential, but not fully unique:

Cloud security should not be considered in isolation—many aspects of a robust security strategy applies across on-prem and cloud

Recognize Security is a Process, not a Product:

Don't just throw tools at security but build a strategy that addresses people, processes, and culture

NEXT STEPS:
THE CHECK LIST FOR ACHIEVING HYBRID CLOUD SECURITY GOALS

How many of these factors can you confidently say your company executes well? What can you prioritize and incorporate into your process?

People and Processes

- ✓ Align people, process and technology throughout
- ✓ Commit to ongoing employee (and IT staff) education around technology
- ✓ Establish best practices and guidelines for remote workers
- ✓ Create and automate a "need to know" permission tier
- ✓ Create an internal cloud team and internal IT checkpoints
- ✓ Balance external oversight with internal expertise and ownership of process

Strategy

- ✓ Drive communication and collaboration across the organization
- ✓ Secure funding, resources and leadership buy-in
- ✓ Build for flexibility and scaling
- ✓ Maintain internal visibility and control
- ✓ Design to meet all compliance requirements; automate when possible to speed processes and avoid human error
- ✓ Utilize cloud resources to efficiently manage data

Security across the Ecosystem

- ✓ Manage all areas of exposure: remote work access, insufficient network security, connected devices, customer portals, supplier security, bots and apps, edge data
- ✓ Drive toward secure central platforms for better decision-making
- ✓ Secure—and incorporate—legacy and unstructured data
- ✓ Utilize a tiered security strategy, i.e. level of security based on sensitivity of info
- ✓ Align cloud security strategy internally and externally

Optimizing partnerships

- ✓ Seek cloud providers who have deep, current industry expertise, including the latest security best practices
- ✓ Discuss hybrid cloud security protocols and practices at outset with your partner to avoid "bolt-on" security later in process
- ✓ Ensure partners evolve with technology and stay ahead of ever changing threats

FIND A STRONG PARTNER:

A partner on your side asks the right questions and ensures visibility, control, and security are built into any cloud environment

View our complementary OnDemand Webinar, **Securing Your Hybrid Cloud: Four Lessons for 2021**, featuring Frost & Sullivan, along with Red Hat and HPE

FROST & SULLIVAN | Red Hat | Hewlett Packard Enterprise