Cybersecurity for Hybrid Cloud Environments

How to set up optimal threat protection

ESET ENJOY SAFER TECHNOLOGY™

TechTarget Custom Media

To protect data and other digital assets in hybrid cloud environments, businesses need to adopt a modernized, flexible and scalable cybersecurity solution. While small and mid-sized companies may not have the same IT challenges—and benefits—of larger organizations, their security needs, especially in an increasingly hybrid cloud world, are equally essential and just as daunting.

The move to hybrid cloud computing is now a nearly universal trend. Organizations have taken to hybrid cloud in a big way for many well-documented reasons: flexibility, cost efficiency, the ability to balance internal control with workload migration, widespread scalability and faster time to value for new applications and services.

In fact, organizations are substantially shifting their IT environments' structure to take advantage of the cloud. Many are adopting a cloud-first architecture or, increasingly, a hybrid cloud model.

Organizations have been particularly adept at leveraging hybrid cloud computing to maximize their existing on-premises IT investment, while optimizing the many benefits of cloud.

However, hybrid cloud is not immune to something that is often organizations' top fear and operational snag: security risks. Organizations certainly understand the need to secure their data, devices and applications in the cloud; even though overall IT spending growth in 2020 was dampened by the pandemic, **research** indicates that spending on cloud security jumped by 33%.

Organizations of all sizes need to stay abreast of the rapidly evolving cyber risk landscape, and seek out new, modernized and highly flexible solutions to help mitigate those risks in a hybrid cloud environment. Specifically, they need security frameworks that embrace homogenous cybersecurity solutions to simplify their cyber defenses. This is done by combining and integrating multiple security services and features into a centralized platform, often as a cloud service.

Security and protection challenges in hybrid cloud architectures

Organizations are experiencing an increasing number, diversity and sophistication of cyber threats. Advanced threat protection and overall cybersecurity management are often at the front and center of an organization's approach to modernized cybersecurity, especially in hybrid cloud environments. Using a centralized approach to cybersecurity through advanced software solutions, often as a cloud service, to stay secure from these multiple threats is an ideal method for protecting end users and valuable business data. Cloud management provides a stark contrast to legacy security approaches that typically started as a series of disparate point products—for instance, one solution for endpoint security and antivirus, another for encryption, another for mail security, and so on.

Implementing a comprehensive security solution is far more efficient to deploy, simpler to manage and, in many cases, far more cost-effective than purchasing individual products for different threats. It also makes it easier to automate security monitoring, management and remediation actions that traditionally had to be performed by dedicated security engineers, often in a monolithic Security Operations Center (SOC). That approach no longer works well for modern organizations for several reasons, but especially because of (a) the huge cyber skills gap that makes it extremely difficult for companies to hire enough (and the right kind) of security professionals, and (b) the increasingly distributed nature of SOCs, with security tasks often carried out virtually in remote locations.

Compared to legacy approaches, cloud-based cybersecurity management is:

- *A more appropriate fit for the increasingly challenging threat landscape, driven by overlapping attacks of different natures, often with no advanced warning.*
- *A better strategy to gain increased visibility into network, application, data and user behavior over physical and virtual networks.*
- *A far simpler and more automated approach to coordinate a unified response to security threats.*

In anticipation of the growing threat landscape, companies of all sizes are rapidly ramping up their investments in cybersecurity to better defend their organizations from this increasingly broad set of threat vectors: ransomware, malware, identity theft, advanced persistent threats, zero-day threats, phishing, spoofing and more. **Global cybersecurity expenditures have been projected to exceed $1 trillion between 2017-2021.**

Long gone are the days when organizations could focus on mainstream, relatively simple security threats like viruses and keystroke logging. Now, the growing diversity of threats, combined with their overlapping attacks and long "dwell times" (the length of time an attack remains undetected inside an organization's cyber defenses) has raised the stakes.

Of course, it's not as though organizations are unaware of the evolution of new, more insidious and potentially more dangerous threats brought about by an increasingly sophisticated set of attackers—both physical and virtual. Smart security and IT executives have invested in more and more security tools over the years, above and beyond the native security offered by their hardware and application software vendors. However, the plethora of providers, tools, architectures, subscription services and infrastructures has become more difficult to manage, as well as more expensive and less efficient.

As organizations adopt hybrid cloud frameworks such as cloud-native application development/deployment, container-based architectures, microservices and serverless computing, they need a security approach designed for a cloud-first or even cloud-only environment.

What to look for in a cloud-based security platform

Selecting the right tool set for security in hybrid cloud environments carries far-reaching implications. Solutions that do not fully and properly address threats can result in compliance violations, data governance problems, legal exposure and the loss of customer confidence. At the same time, solutions that are difficult and expensive to deploy cost money, degrade employee productivity and take security professionals away from other tasks.

As buyers make their checklist—or oversee third-party organizations that augment their internal security teams—it is important to keep in mind some core functionality for a unified threat management (UTM) solution for hybrid cloud security. For instance:

- *Protecting traditionally unprotected or poorly protected endpoints, networks and applications now being used more frequently in remote work, such as home networks or personally subscribed cloud services.*
- *Enabling cloud sandboxing as isolated test environments to study, analyze and plan action against suspicious programs and/or files.*
- *Delivering multilayered protection of the expanding number of applications, data and devices at the endpoint, server, network and cloud levels.*
- *Supporting an integrated platform design, rather than disparate security point products, to ease management and support automated prevention, detection, response and remediation.*
- *Improving time to value by speeding deployment, facilitating scalability and reducing costs.*
- *Embracing a multi-purpose console to do more than just threat monitoring.*
- *Avoiding "one-size-fits-all" solutions through customized solutions, configurations and policies.*
- *Securing both data at rest and data in motion, due to the need to support both cloud and on-premises protection, as well as securing data as part of workload migrations.*

Cloud-based security solutions from ESET

With cybersecurity stakes higher than ever, organizations need to align with a security solutions partner that (a) understands the unique needs of its customers and (b) offers a portfolio of solutions that support cybersecurity in a hybrid cloud environment. Organizations looking for this kind of partner should

consider ESET, an experienced cybersecurity solutions and services vendor with an established track record for research and development, technology innovation and business results.

ESET's flagship product is ESET PROTECT, a cloud-optimized solution designed to protect against a variety of threat vectors for multiple devices and management consoles, as well as cloud-based applications and services. ESET PROTECT provides a central management console to direct efficient operation of all available security services from a single location. It enhances visibility and mitigates threats like ransomware, malware, botnets, advanced persistent threats, zero-day exploits, identity theft and more, while enabling smooth integration, reporting and recording of security information for real-time analysis.

With a variety of solutions, ESET provides benefits for different security use cases. For instance, ESET PROTECT Complete allows organizations to combat threats to the ubiquitous Microsoft Office 365 cloud application suite with ESET Cloud Office Security to provide a value-added layer of security for spam, malware and phishing. The solution is easy and fast to set up, comes with a clean dashboard design for evaluating security health status of cloud office applications and supports multi-tenancy with secure access management.

ESET also offers cloud-based sandboxing technology that enhances existing endpoint security by analyzing files from web browsers, mail clients, compressed files and removable media. It is designed to protect against zero-day threats, ransomware and advanced persistent threats, which have become increasingly prevalent and represent a growing threat to security health. It leverages the native intelligence of ESET Endpoint Security by combining it with a cloud-based sandbox to detect, prevent against and remediate threats without disrupting daily business operations.

Conclusion

Since hybrid cloud brings with it a unique set of security risks, organizations must identify, embrace and adopt cybersecurity solutions that simplify security for their applications, devices and data.

Security and IT decision makers should commit to solutions designed and optimized for hybrid cloud environments to reduce complexity, costs and inefficient capabilities overlap.

Solutions from ESET—especially ESET PROTECT for hybrid cloud environments—help organizations become more secure when facing important trends such as remote work, hybrid and multi-cloud architectures, virtualized infrastructure and sophisticated, relentless attackers. ESET's broad solutions portfolio, combined with its extensive security expertise and proven track record, makes it a viable partner for organizations looking to secure their increasingly important hybrid cloud architecture.

Please visit **ESET's website** for more information and to learn more about its solutions.