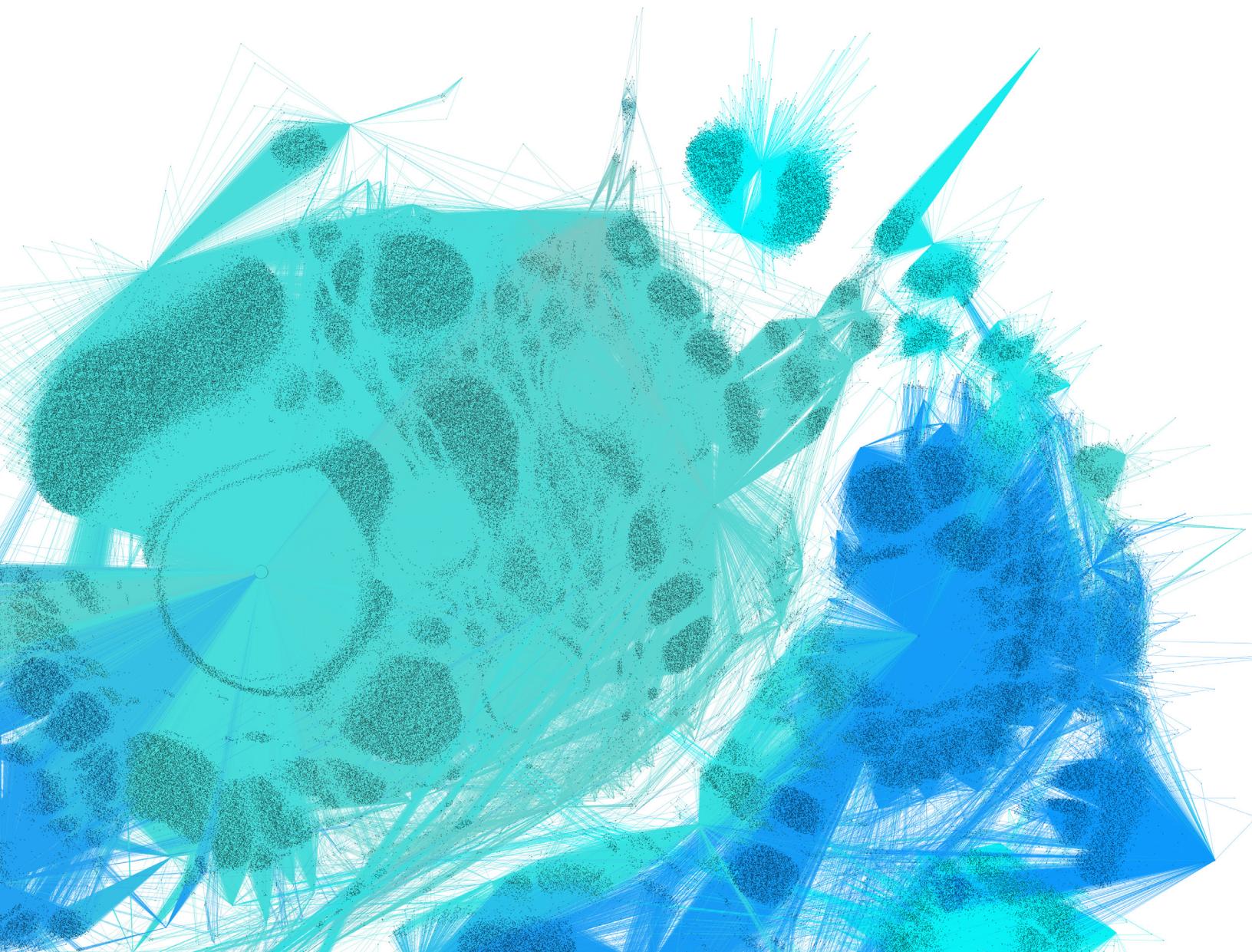


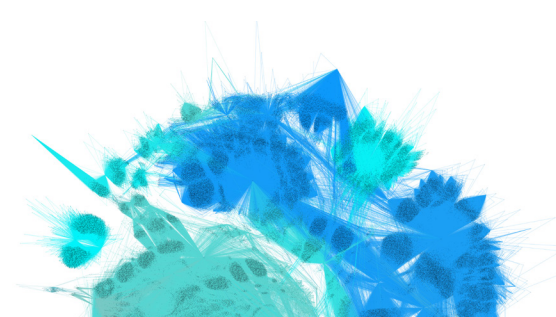
Servers, Servers, Everywhere: How the Hybrid Cloud is a Game Changer for Security



INTRODUCTION

Smarter tools, services, and new ways of working are driving innovation across businesses of all sizes—and the success of these initiatives rests partly on the shoulders of those responsible for securing them. New digital products, better ways to manage data, flexible working policies—everything needs to be developed with effective security in place. That means IT teams must be closely aligned with the strategies organizations adopt to achieve business success over the next few years. The move to hybrid cloud is one of the emerging workplace trends powering this transformation, and IT security teams need the right tools in place to ensure the data stored across it is safeguarded effectively.

This paper examines the dynamics of the hybrid cloud, and what it means for organizations at both the business and technical levels. It also outlines how Trend Micro helps to address real-world problems in ways that can simplify operations and increase the overall security of your data and applications across the hybrid cloud. Giving security teams the freedom to go further and do more. You can find even more information at www.trendmicro.com/hybridcloud.



THE STATE OF PLAY

Organizations today are facing significant challenges as they adopt the latest technologies to power business success. With major shifts from physical to virtual to cloud having occurred in the past 10 years, architectures have changed significantly and the rate of change is not slowing down. Many enterprises have already adopted containers as a key piece of their infrastructure, with containers being actively deployed into production for both legacy and cloud-native applications. Looking beyond containers, serverless functions are on the horizon for broad enterprise adoption, adding a new set challenges for security teams.

In recent years, the average cost of a ransomware attack has increased by 62%.¹ Ransomware has also been bolstered with new abilities; currently, many ransomware families do not just encrypt files, but also steal data. We've also seen a dangerous rise in cryptocurrency mining attacks, which are less visible but still very costly to enterprises. In 2019, Trend Micro Research saw a 71% increase in fileless events, which included cryptocurrency mining attacks.² As cryptocurrency remains top of mind, cybercriminals have taken interest in outsourcing their expensive mining processes to organizations that are using containers from public repositories³ and organizations that aren't properly protected.

Servers are at the center of this technology shift; they are the workhorse of the enterprise. Gartner, the leading IT research and advisory firm, explicitly points out that, "Servers often host the most critical data in the enterprise and have different functionality than client endpoints."⁴ We believe the challenge is that the architectural shifts have established server workloads in multiple locations and in different formats, which makes securing them more complex than ever before.

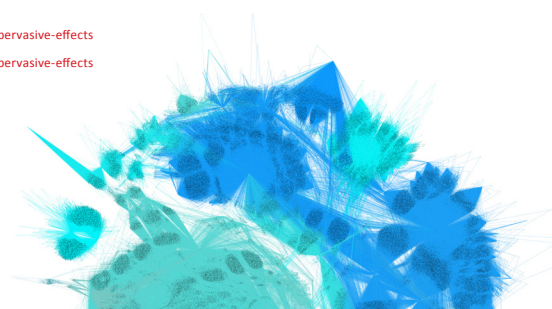
Designed to address the challenges of the hybrid cloud, Trend Micro Cloud One™, a security services platform for organization building in the cloud, includes a broad set of state-of-the-art security capabilities in a single solution, enabling you to reduce the number of tools used and centralize visibility in a single management interface (or with full automation driven via APIs). Leveraging deep integration with VMware, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform™ service, Trend Micro enables you to quickly and easily discover all protected and unprotected workloads, giving you a complete view of your security posture across physical, virtual, cloud, and container environments. Even extending security to your CI/CD build pipeline with container image scanning.

¹ Trend Micro 2020 Midyear Security Roundup. <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects>

² Trend Micro 2020 Midyear Security Roundup. <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects>

³ Goodin, D. (2018, June 13). Backdoored images downloaded 5 million times finally removed from Docker Hub. Retrieved from <https://arstechnica.com/information-technology/2018/06/backdoored-images-downloaded-5-million-times-finally-removed-from-docker-hub/>

⁴ Gartner, Evaluation Criteria for Endpoint Protection Platforms, January 2018. ID G00346995



WHAT IS THE HYBRID CLOUD?

The speed of change in IT architectures over the past decade is unprecedented. The introduction of virtualization technologies from companies like VMware, took the deployment of servers from weeks to days—changing the way data center operations and security teams worked, and resetting expectations of speed for business project delivery. Only a few years later, the public cloud market, driven by offerings like AWS and Azure, enabled the deployment of servers in minutes instead of days, empowering businesses to deliver new applications and projects at speeds that have never been seen before. With new technologies, (containers like Docker and serverless offerings like AWS Lambda or Azure functions), the rate of change for IT is not showing any signs of slowing down.

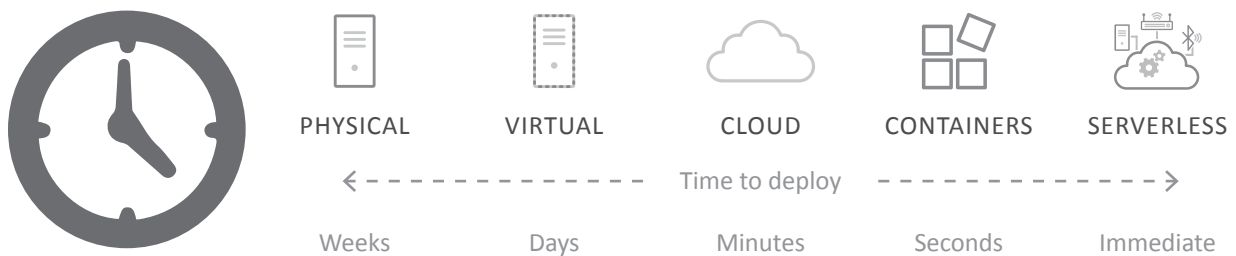


Figure 1: IT Architecture Evolution

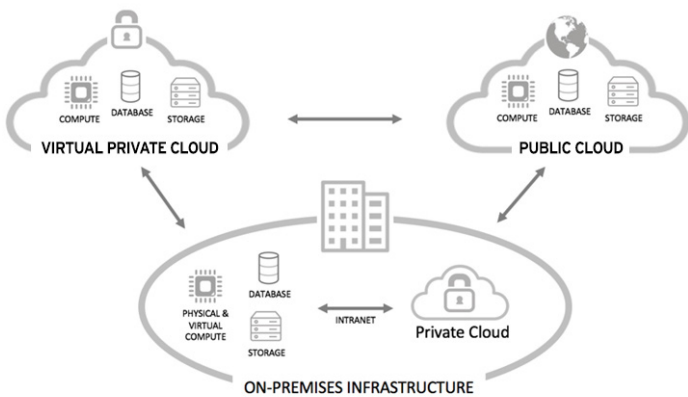
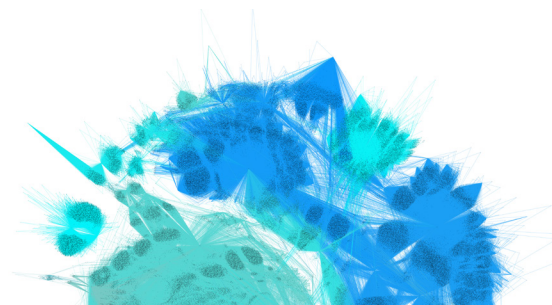


Figure 2: Hybrid Cloud Architecture

With such rapid change, the ability for an organization to simply abandon existing deployments in favor of the latest technology is severely limited. This will result in most organization’s IT architecture spanning multiple deployment environments, with new projects embracing the most modern approaches, but running projects that continue to operate within their existing environments. This concept is what underpins the use of “hybrid cloud” when describing modern IT. Hybrid cloud includes a mix of on-premises, private cloud, and public cloud services, with orchestration between the environments (see Figure 2). In this model, organizations can allow workloads to move between environments as computing needs and costs change, giving businesses greater flexibility, more deployment options, and increased opportunity for cost savings.



MODERN BUSINESS CHALLENGES

The reality of modern times is that every organization has become a technology organization. Businesses leverage new technologies, like virtualization and cloud, to improve the way they run IT. This comes with the goal of speeding time-to-market, addressing capacity changes in economical ways, and dealing with ever-increasing compliance challenges.

THE NEED FOR SPEED

Today's global digital economy introduces both challenges and opportunities. Driven by the goal of speeding new projects to market, leveraging new technologies and approaches like DevOps can be especially attractive at both the corporate and the business-unit level. With compute, database, and storage easily accessible, the public cloud has enabled widespread use for rapid delivery of new projects, including at the business-unit level (often called "shadow IT"). However, organizations can quickly become overwhelmed by the complexity created by constantly deploying the "latest thing" without any central coordination, as well as introducing more security risks based on a continually evolving threat landscape.

A SHIFTING IT LANDSCAPE

Significant investments have been made in data centers, including the relatively recent move from physical to virtual data centers. However, the attractiveness of the cloud and other new technologies are driving organizations to leverage more and more external capacity to manage changing IT needs. While this shift can deliver significant economic benefits, organizations are still faced with supporting existing on-premises deployments, which can introduce purchasing and support complexity, as well as operational and security challenges because of the diversity of environments.

MAINTAINING COMPLIANCE

Verizon's 2020 Data Breach Investigations Report found 157,525 security incidents, of which 3,950 were confirmed data breaches.⁵ Some high-profile data breaches in 2020, include Weibo (538 million records)⁶ and General Electric⁷—the latter of which even compromised information such as passport and bank account numbers. It is clear that attackers will continue their quest to penetrate corporations for financial gain. With threats on the rise, organizations are being mandated by external regulations to protect their IT infrastructure. Regulations like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), the Federal Risk and Authorization Management Program (FedRAMP), and many regional laws are forcing organizations to implement specific security measures in order to be compliant. The European General Data Protection Regulation (GDPR) came into effect on May 25, 2018, and focuses on the protection of EU citizen data, regardless of where in the world that data is being used or stored. With fines up to 4% of global revenue or €20 million (whichever is higher), the ability to stop a business from processing data, and a 72-hour breach reporting requirement, it has established itself as the new highest standard for protecting personal data.

In order to help, frameworks for security, including the SANS/CIS top 20, NIST, and ISO 27002, have been developed as a roadmap to secure deployments. However, the shifting IT landscape has introduced new challenges for compliance. Organizations must now deal with deployments across multiple environments, ensuring that appropriate measures are in place for compliance without overwhelming IT with tasks that are not central to the success of the business.

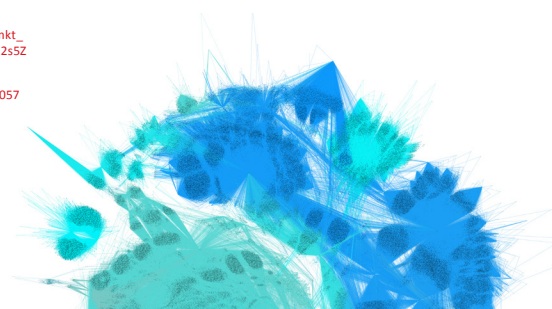
MODERN TECHNICAL CHALLENGES

New technologies like cloud bring tremendous potential gains through the promise of a flexible, on-demand, and metered computing model. However, the rapid evolution of IT architectures and the reality of the hybrid cloud has introduced multiple challenges for technical teams supporting constantly shifting business needs. Inherent in these challenges is the fact that security needs to be looked at specifically for each environment, not generically.

⁵ Verizon 2020 Data Breach Investigations Report, May 2020. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf?mkt_tok=eyJpIjoiWVdJMFluVTBaR1k1TUdKaSIsInQlOiJlZ2VwvHBNXjQ3QmZkZUwvYXNCOEsrMnRlUHRCCTTtZGJleGx5bERJNk5xdFsrRnFaZUSVWE1MUUVduUGtIK2s5Z0MxbFdHRUSpU3U4eFdvNlUOEtlXUVZnWGNkd3BtQ1FCT2xZROVNQVE3QWpMaFdTUGJlbiVlNVE1MSlSM1NurVYfIQ%3D%3D

⁶ Campaign Asia-Pacific Gizmodo, March 2020. <https://www.campaignasia.com/article/china-probes-weibo-data-leak-of-more-than-500-million-records/459057>

⁷ Infosecurity Magazine, March 2020. <https://www.infosecurity-magazine.com/news/general-electric-employees>



MULTIPLE ENVIRONMENTS, TOO MANY TOOLS

While the benefits of new technologies like the cloud are obvious, including purchasing flexibility and deployment automation, most organizations will continue to have physical and/or virtual servers in their data center for the foreseeable future. This means that from both an operational and security perspective, organizations need to be able to deal with multiple environments at the same time, including ensuring connectivity between multi-tiered applications that leverage both data center and cloud for compute, database, and storage services. The result often includes deploying multiple disparate security tools as well as introducing significant complexity and operational cost—especially when tools work only in the data center and not the cloud.

STOP ADVANCED THREATS, SHIELD VULNERABILITIES

In 2020, we saw the start of a new, increasingly focused and sophisticated approach in cyberattacks—with attacks like **Ryuk**, **ColdLock**, and **Egregor** impacting businesses. The evolution of ransomware attacks continues, with the most prominent of the new ransomware families, Nefilim, growing in complexity. There has also been a sharp rise in cryptocurrency-mining attacks, with hackers leveraging a variety of attack vectors, including server exploits and PHP vulnerabilities. With multiple environments to deal with, the hybrid cloud introduces new complexity in dealing with advanced threats and vulnerabilities. As applications migrate from the data center to the cloud, the ability to protect these two environments from both existing and new vulnerabilities is a significant task, especially in the face of increasing compliance requirements. For example, an organization that continues to run Microsoft Windows Server 2003 or 2008 in the data center and AWS Linux servers in the cloud will be subject to different vulnerabilities, but still require a unified and coordinated solution to be protected from advanced attacks.

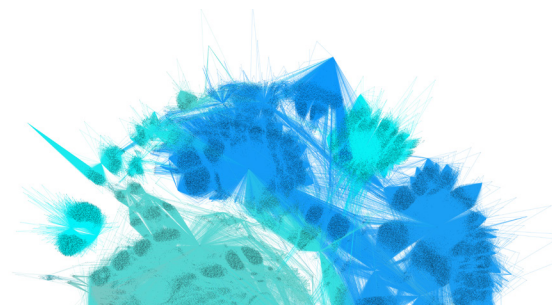
DEVOPS AND THE SECURITY SKILLS SHORTAGE

According to IT market research firm, Forrester, “Lack of skilled technical staff is a major challenge...24% of security technology decision-makers rate lack of staff as a challenge, and 21% find unavailability of security employees with the right skills a challenge.”⁸ With multiple environments that have different security requirements (example: Cloud service providers [CSP] are responsible for just part of the security story), security teams are being stretched thin. This is further worsened by the evolution of operations and the cloud, including the use of DevOps and introduction of the “DevSecOps” role. This role is all about getting things deployed quickly and efficiently in the cloud, including the use of containers such as Docker and serverless cloud functions as well as leveraging orchestration tools and automation to speed application delivery. This means that they are technology focused, not security experts, using multiple disconnected security tools that were not designed for automation will quickly sabotage their success.

SECURING THE HYBRID CLOUD

Trend Micro is committed to helping our customers securely navigate their journey through these challenging times for IT. For many years Trend Micro has been delivering new capabilities and security techniques to address threats across the hybrid cloud, while also enabling our customers to deploy them in ways that are optimized for each environment. Instead of using separate, siloed security solutions that do not share information, Trend Micro provides a cross-generational blend of threat defense techniques and a connected threat defense that protects our customers from advanced threats. Powering our Hybrid Cloud Security solution is Trend Micro Cloud One.

⁸ Report: The State of Network Security: 2018 To 2019, Forrester, November 2018

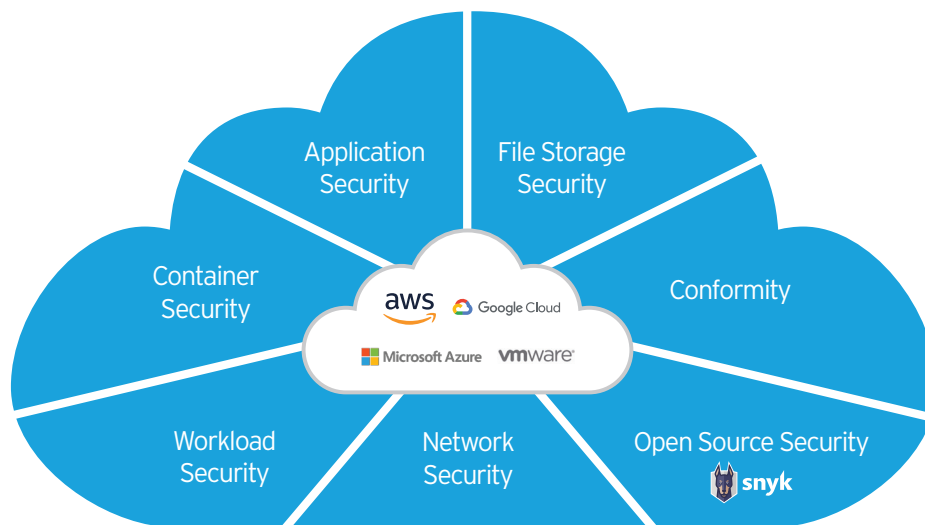


INTRODUCING TREND MICRO CLOUD ONE

With an exploding set of cloud infrastructure services and an increasing number of stakeholders involved in infrastructure and security decisions, the cloud has formed the perfect storm for security. In order to gain the benefits of the cloud and meet business objectives, cloud security needs to be made less complex.

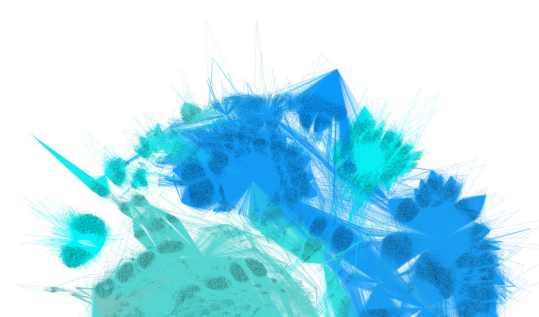
Business requirements and DevOps processes demand faster application delivery. However, if you increase the speed of delivery, everything else must follow suit. A great example of this is compliance, which changes based on industry, geography, and infrastructure, as well as protecting against evolving and increasingly sophisticated threat vectors.

Trend Micro Cloud One delivers the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity.



You no longer have to find point products to meet the unique requirements of your infrastructure or work with the processes you've already implemented. With a comprehensive set of services designed specifically for the cloud, Trend Micro Cloud One secures the different parts of your environment within one simple platform.

With support for all major cloud platforms and solutions that integrate directly into your DevOps processes and toolchain, Trend Micro Cloud One is designed to provide the flexibility you need without slowing down your business or application delivery.



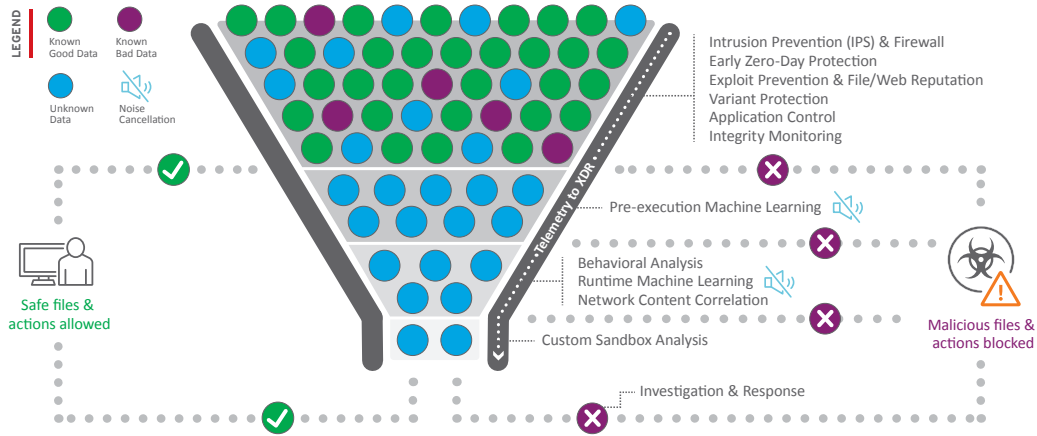


Figure 5: No silver bullets! Protection against advance threats requires multiple cross-generational capabilities

Taking security effectiveness one-step further, Trend Micro Cloud One also has the ability to connect with other Trend Micro security products, sharing information and speeding response time to threats across the enterprise. This includes using information from Trend Micro™ Smart Protection Network™, which has identified and blocked over 41 billion threats in the first half of 2021⁹.



Global Sensor Network: Collects more threat information in more places

- Hundreds of millions of sensors
- 2.5+ trillion threat queries yearly

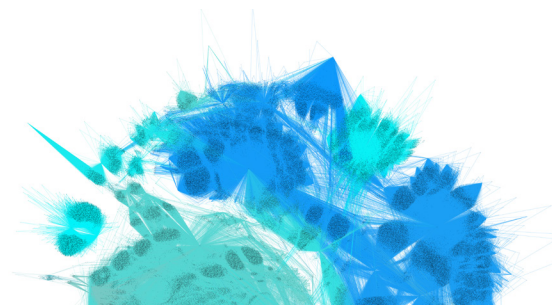
Global Threat Intelligence: Analyzes and identifies threats faster

- 5 billion new unique threats yearly
- Leverages Trend Micro™ Zero Day Initiative™ data for rapid response

Proactive Protection: Blocks real world threats sooner

- 48 billion threats blocked yearly
- Hundreds of new protection rules yearly, including for Microsoft

⁹ Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats, 14 September 2021. Retrieved from: <https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats>



OPTIMIZED FOR THE HYBRID CLOUD

The challenge of the hybrid cloud is that security needs to be applied with a different approach, depending on each environment. The good news is that security strategies, like defense in-depth, remain relevant across all environments—it’s how they are applied in ways that are both effective and operationally efficient that change. For example, for infrastructure as a service (IaaS) deployment, there is a shared security responsibility with the CSP responsible for everything up to and including the hypervisor layer, and the organization responsible for everything they put in the cloud (See Figure 6).

To help with this, Trend Micro Cloud One has been optimized to apply these security techniques across leading environments, including data center-focused technologies like VMware, as well as leading IaaS providers like AWS, Azure, and Google Cloud Platform. This enables organizations to deploy high-performance security across the hybrid cloud and their running containers without the need to purchase and manage multiple products in an already complex operating environment.

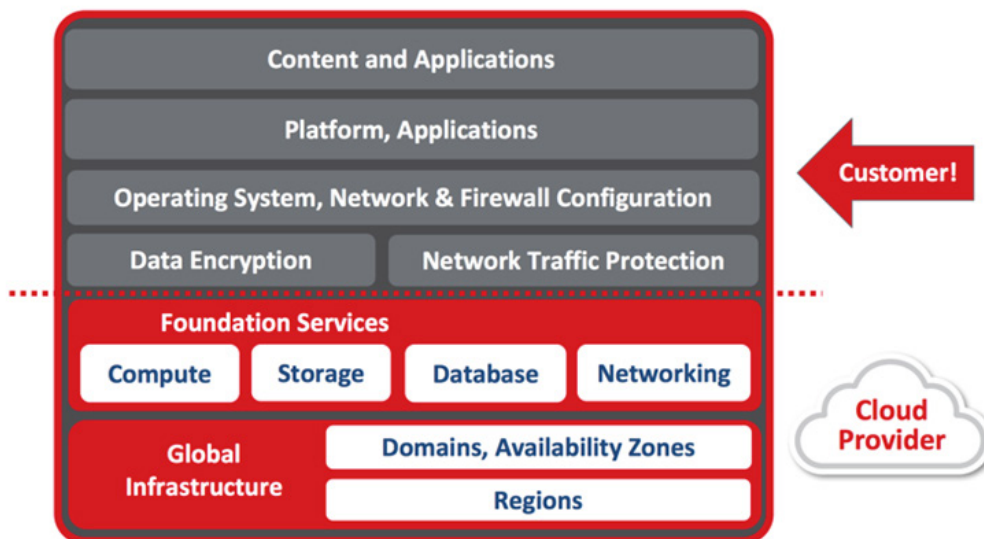


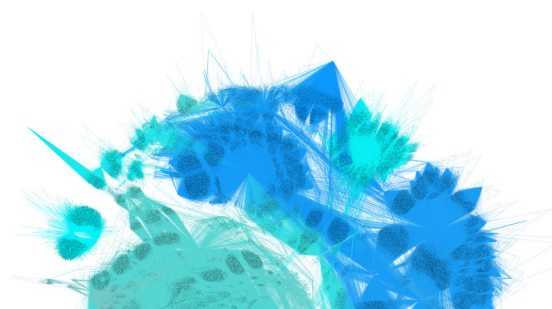
Figure 6: Shared security responsibility for the cloud

FULL-STACK CONTAINER SECURITY

Many enterprises have started to adopt containers to enable microservice application development, building software that is modular, easily scalable, and easy to update. However, like virtual machines and bare metal servers, containers have their own threat vectors, which need to be secured. Trend Micro Cloud One™ – Workload Security runtime protection provides full-stack container security against the latest threats—securing at the host, container platform, orchestration layer, the container itself, and even at the application layer. The solution’s IPS capabilities protect the container platform against new vulnerabilities, while integrity monitoring and log inspection allow for rapid detection and identification of unauthorized changes. Finally, Workload Security monitors for north-south network traffic, as well as east-west traffic between containers to prevent the exploitation of vulnerabilities and malware within the container node. By securing every layer of the stack, from the host up to the application, Workload Security ensures comprehensive protection for runtime containers.

SHIFTING SECURITY TO THE LEFT

While runtime security controls remain critical, organizations must also shift security to the left in order to mitigate threats before they reach production. To address this, Trend Micro Cloud One™ – Container Security provides development teams with automated, continuous build-time and registry scanning of container images to detect malware, vulnerabilities, and indicators of compromise (IoCs) or secrets early in the development cycle. By implementing security early in the pipeline, Container Security provides detection and protection across the entire application life cycle.



“Workload protection must span virtual machines, containers and serverless workloads in public and private clouds. Security and risk management leaders should use this Market Guide to understand the need for protection that spans development and runtime and includes cloud security posture management.”

Market Guide for Cloud Workload Protection Platforms,
Published 12 July 2021 - ID G00725997



SOLVING REAL-WORLD SECURITY CHALLENGES

It is important to remember that every workload in the data center, the cloud, or in a container has a different level of risk. Instead of a one-size-fits-all approach, a wide-range of capabilities need to be available to appropriately protect every workload. While having many state-of-the-art security capabilities in a single product will help with this risk-based approach, they are only applicable if those capabilities help organizations solve real-world security challenges. Let's take a look at a few examples of how Trend Micro Cloud One helps to address hybrid cloud security in multiple, meaningful ways.

PROTECT AGAINST ADVANCED THREATS: RANSOMWARE

Ransomware is malware that installs covertly on an endpoint and mounts an extortion attack by extracting and/or encrypting data, holding it inaccessible until a ransom is paid. While the majority of ransomware attacks leverage social engineering and email to gain access to an enterprise, servers are a prime target given the types of data and applications they hold. Figure 7 illustrates a typical attack sequence for ransomware.

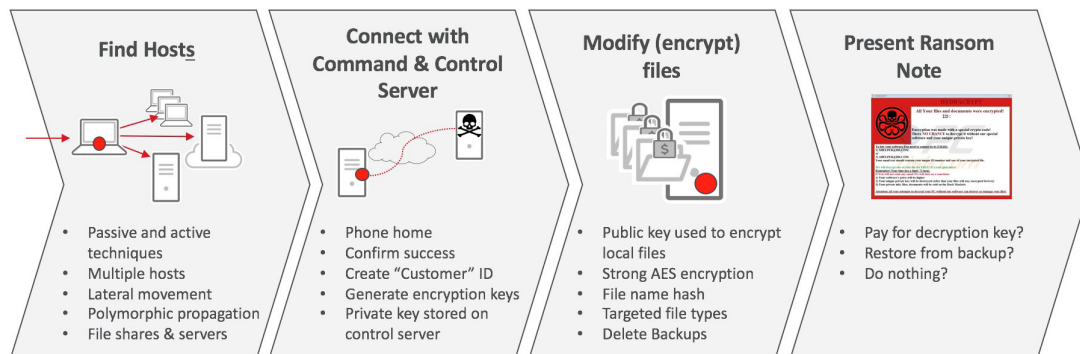
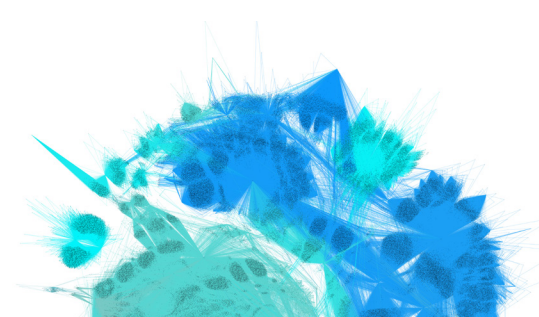


Figure 7: Ransomware attack sequence



Logically, the first step in the process is one of the most important points where security should be focused. Trend Micro delivers multiple state-of-the-art techniques that can help to stop ransomware as it attempts to move across the enterprise:

- **Shield servers from external attacks and lateral movement:** Once ransomware is in the enterprise, it will attempt to spread and achieve maximum damage. With a host-based IPS and thousands of protection rules that can be automatically and intelligently applied based on each specific machine context, the available attack surface is significantly reduced for both the external and internal attack vectors. Trend Micro’s smart rules can detect and prevent lateral movement as ransomware attempts to spread, including leveraging behavioral and heuristic data to catch unknown ransomware variants. Specific to situations where an end-user machine has been compromised and mapped drives to file servers, Trend Micro can detect attacks over server message block (SMB), including encryption commands and file renaming thresholds, and be used to immediately shut down the connection and alert that ransomware is attempting to spread.
- **Block ransomware from running:** If ransomware somehow ends up on a server, its first task is going to be to establish itself and start encrypting files. With application control, organizations can create a safelist of authorized applications, ensuring that ransomware embedded in an unauthorized application cannot execute.










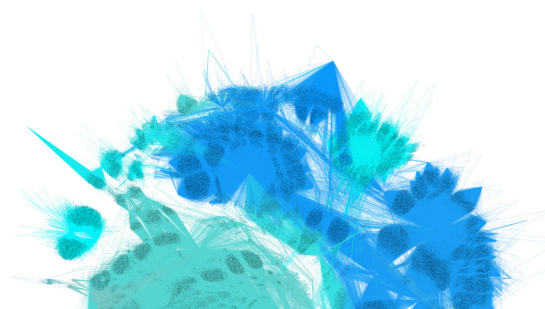
	Name ▲	Application Type
	1006994 - Downloaded Executable File Through SMB Share	Windows Service
	1006995 - Remote Add Job Through SMBv1 Protocol Detected	Windows Service
	1007017 - Remote Schedule Task 'Run' Through SMBv2 Protocol Detected	Windows Service
	1007020 - Remote CreateService Request Detected Through SMBv1 Protocol	Windows Service
	1007021 - Remote Registry Access Through SMBv2 Protocol Detected	Windows Service
	1007032 - Remote Schedule Task Create Through SMBv1 Protocol Detected	Windows Service
	1007033 - Scheduled Tasks Via SMBv1 Protocol Detected	Windows Service
	1007035 - Remote DeleteService Request Through SMBv1 Detected	Windows Service
	1007037 - Remote Add Job Through SMBv2 Protocol Detected	Windows Service

Figure 8: Smart rules detect and stop ransomware spread

- **Stop command and control (C&C) traffic:** Without the ability to “phone home”, many ransomware variants are rendered harmless, as they have no means to receive the encryption key. Trend Micro’s smart rules detect both known and unknown C&C traffic on a server, stopping communication and alerting administrators of a potential attack.
- **Detect and block ransomware:** Attackers are innovative and determined, meaning that there is always a chance that a piece of malware will end up on a protected server. Trend Micro’s anti-malware capabilities include behavioral monitoring with real-time memory scanning that can detect and block suspicious activity. This includes backing up files before they are encrypted, and once the malicious process has been stopped and quarantined, restoring them with minimal damage.



SHIELD WORKLOADS FROM VULNERABILITIES

Trend Micro’s network security controls can shield enterprise servers against known and unknown vulnerabilities—for example WannaCry (Microsoft Windows SMB), Erebus (Linux), Shellshock, and many other data-stealing attacks—from being exploited. Leveraging IDS/IPS, Trend Micro includes thousands of proven rules that apply to network traffic in layers two to seven. Using a recommendation scan to enable contextual security, these rules can be automatically applied based on a deployment environment to protect unpatched, network-facing system resources and enterprise applications. Protection applies to both the underlying operating system, as well as common enterprise applications deployed on those servers—even the container platforms like Kubernetes and Docker. Trend Micro includes out-of-the-box vulnerability protection for hundreds of applications, including database, web, email, and file transfer protocol (FTP) servers, defending against the most common web attacks, including Structured Query Language (SQL) injection, cross-site scripting, and other web application vulnerabilities. In addition, it provides zero-day protection for known vulnerabilities that have not been issued a patch—typically in under 24 hours from disclosure—and unknown vulnerabilities using smart rules that apply behavioral analysis and self-learning to block new threats.



Figure 9: Network security shields servers from attack across the hybrid cloud

Attacks

Attacker attempts to exploit a vulnerability at the OS or application level over the network

Network Protection

Trend Micro Cloud One blocks malicious attacks at the network level, shielding servers from new and existing threats

Across the Hybrid Cloud

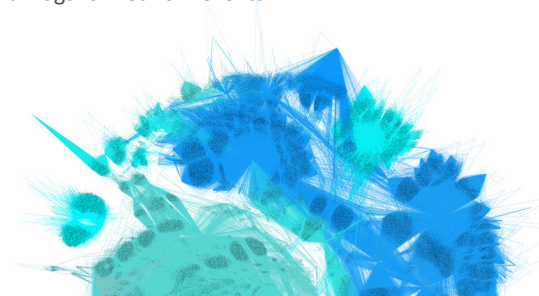
Trend Micro Cloud One protects applications and workloads from attacks across physical, virtual, cloud, and containers

“Trend Micro’s virtual patching... lets us react quickly to a zero-day outbreak instead of working on a patching scheme that may take a week or a month to get in place.”

William Crank, CISO,
MEDHOST

MEDHOST®

To help with enforcement of IPS rules, Trend Micro leverages its built-in, bi-directional and stateful firewall. The enterprise-grade firewall can also help to control communication over the ports and protocols necessary for correct server operation and blocks all other ports and protocols. This can further reduce the risk of unauthorized access to a deployment that includes end of support servers, like Microsoft Windows Server 2003 and Microsoft Windows 2008. The host firewall can also help with key compliance requirements from regulations like PCI DSS and HIPAA, particularly in cloud deployments where there is no access to the cloud provider firewall logs for network events.



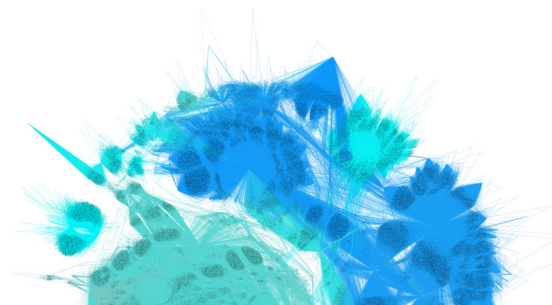
AUTOMATE AND INTEGRATE SECURITY AT SCALE

Changing infrastructures, evolving cyberattacks, and accelerating development cycles can be overwhelming for security and risk teams to deal with, not to mention the continually growing skills gap in the security industry. Automation is the critical piece of the puzzle and can enable security teams to move and scale at the same pace as their DevOps teams. Trend Micro's RESTful APIs allow security and development teams to integrate security with their current toolset, including extensive API capabilities for deployment, policy management, health checks, compliance reporting, and more. Security experts can now automate security deployment and protection at scale, while DevOps teams can leverage security as code to build security into their delivery pipeline without slowing down their processes. Visit the [Automation Center](#) for more on automation, as well as example-driven automation guides, use cases, and direct engagement from the Trend Micro team.

ACCELERATE COMPLIANCE

More compliance requirements are placed on businesses every day. GDPR, PCI DSS, HIPAA, and FedRAMP are good examples of regulations that require organizations to implement multiple security controls and be able to report against them. Trend Micro Cloud One helps to accelerate the process of compliance, delivering:

- **A state-of-the-art product to address multiple security requirements:** From network shielding to change detection to mandated anti-malware protection, Trend Micro Cloud One includes the capabilities to address multiple compliance needs through a single agent. For example, it delivers multiple ways of protecting citizen data across the data center and cloud, which is critical for GDPR compliance.
- **Single point of reporting:** Reporting is a big part of maintaining compliance, especially with regulations like the GDPR that require breach reporting within 72 hours. Trend Micro Cloud One not only consolidates reporting across multiple security controls, it also includes templated and customizable reports for easier audits. Powerful options include the ability to report based on smart folders, which can easily give information on servers across the data center and cloud, based on details that make sense for the compliance need—for example, all in-scope servers running a particular application.
- **Built-in automation:** Compliance is not just about a point in time; it needs to be a continuous process. Trend Micro Cloud One enables continuous compliance with easy-to-understand automation features, including automated script generation for use with orchestration tools like Chef, Puppet, and Ansible. It also enables the ability to deal with dynamic cloud activities, like auto-scaling in AWS, without creating security or compliance gaps.
- **Broad platform support, including end of support systems:** With IT environments continually evolving, you need the ability to protect systems that are in-scope for audit, without unreasonable cost or complexity. Trend Micro Cloud One includes built-in protection for **end-of-support systems** systems like Windows Server 2003, Windows Server 2008, Microsoft Windows XP, and more, without the need to purchase expensive extended support contracts or upgrade faster than what is right for the business.



STREAMLINE SECURITY OPERATIONS AND MANAGEMENT

With multiple environments to deal with and a steady stream of new applications being developed to help the business, it is critical that security can be addressed in a scalable way, especially considering a global security skills shortage. Trend Micro Cloud One includes a broad set of security capabilities that enable you to reduce the number of security tools used and gives you full visibility of your hybrid cloud in a single interface. Built on deep integration with VMware, AWS, Azure, and Google Cloud Platform, Trend Micro Cloud One lets you discover all workloads across physical, virtual, cloud, and containerized environments, and applies protection based on server context.

Smart folders also enable you to easily view servers in ways that make sense to your operational processes, providing visibility across multiple environments based on criteria set by you. For example, they can be set up to show web servers across the data center, AWS, Azure, Google Cloud Platform, and container workloads. Plus, with automated recommendation scans for new and deployed workloads, new vulnerabilities can be highlighted and protected immediately.

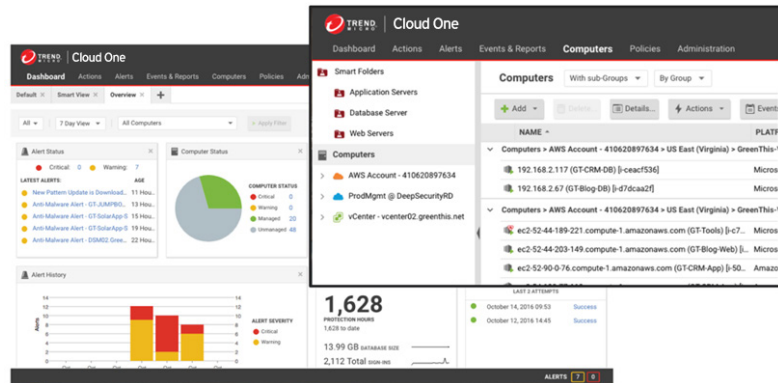


Figure 11: Single dashboard with visibility across the hybrid cloud

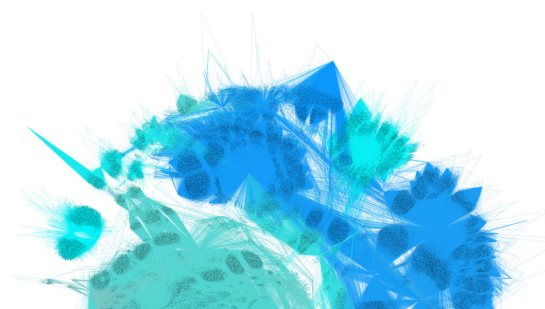
Even with multiple security capabilities, there is only ever a single security agent to be deployed, which simplifies deployment and management. The agent can be automatically deployed via scripting or orchestration tools like Chef, Puppet, Ansible, and SaltStack, and only deploys security components dictated by the policy—streamlining the size of the agent and maximizing workload performance. The Workload Security agent can also automatically update to the latest version in order to deal with any kernel incompatibility that may arise due to a new operating system version. This allows organizations to leverage the operating system version needed for the business, without adding additional work to the taxed IT team.

Embracing the CI/CD model, Trend Micro Cloud One also includes the ability to integrate security into the application development pipeline with continuous build phase scanning. This enables DevOps and rapid development teams to bake security into their CI/CD pipeline, leveraging automation and integration with tools like Jenkins and GitHub. Development teams can maintain their speed and agility without compromising security.

SUPPORT AND EMPOWER INCIDENT RESPONSE TEAMS

As attacks increase in sophistication and breaches become more costly, enterprises may find themselves needing advanced detection and response (EDR) capabilities for their server and workload environments. This involves correlating threat and telemetry to monitor for attacks, respond to detections, and investigate threat severity and impact. Trend Micro Cloud One™ – Workload Security includes the XDR capabilities of Trend Micro Vision One™.

Leveraging XDR, security and incident response teams have powerful capabilities for detection, response, and investigation, including the ability to detect indicators of attack (IoA) and lock down suspicious applications and processes. Trend Micro also integrates with leading security information and event management (SIEM) platforms to analyze telemetry for advanced threat hunting and IoC sweeping, as well as security orchestration and automation response (SOAR) tools for security orchestration. For teams that do not have the resources to investigate, remediate, and threat hunt, Trend Micro also provides many of these functions as a managed service, with Trend Micro™ Managed XDR.



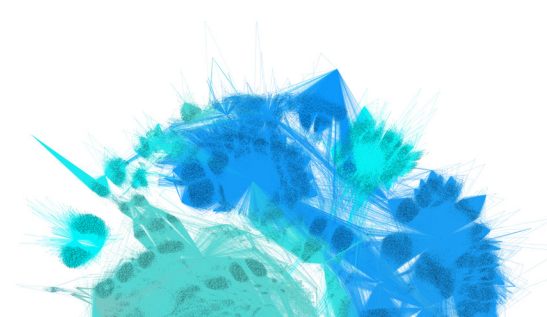
SIMPLIFY SECURITY ACQUISITION

With multiple security controls that can be deployed across the hybrid cloud, Trend Micro enables organizations to reduce the number of security vendors they need to manage. Recognizing that the way you buy IT infrastructure changes depending on where it is, Trend Micro Cloud One is priced and sold in ways that further simplify procurement.

In the data center, per server pricing makes sense; however, in the cloud, you are paying based on what you use and by the hour. Working closely with leaders like AWS and Azure, Trend Micro Cloud One can be purchased in both traditional data center approaches, as well as by the hour, which is aligned to the cloud. Finally, Trend Micro Cloud One can be deployed in two different ways, giving maximum flexibility while also offering further simplification through options like purchasing through AWS or Azure marketplaces for a single-invoice cloud billing experience.



Figure 12: Multiple purchase options for securing hybrid cloud deployments



SUMMARY: SECURING THE HYBRID CLOUD

Embracing hybrid cloud to gain benefits like increased agility and rapid application delivery makes good business sense. What it means to you depends on your organization and its goals, but hybrid cloud can play a central role in helping you improve flexibility, drive scalability, and reduce costs. But these beautiful outcomes can only be achieved if your hybrid cloud strategy is properly implemented and secured effectively. With increasingly sophisticated threats combined with ever-growing attack volumes, protecting the important data residing on server workloads across the hybrid cloud has never been more critical. And with challenging regulations like GDPR and PCI DSS that demand the use of state-of-the-art security approaches, organizations must secure their servers and applications—or risk facing substantial fines and penalties.

With thousands of customers and millions of servers protected, Trend Micro is designed for the hybrid cloud. The solution delivers a cross-generational blend of threat defense techniques in a single product that has been optimized for securing physical, virtual, cloud, and container workloads. Delivering multiple capabilities in a single product, including protection from advanced attacks like ransomware, Trend Micro allows for vendor consolidation—simplifying operations without compromising security.

Trend Micro has been ranked #1 in IDC's 2020 [report](#), "Worldwide Hybrid Cloud Workload Security Market Shares"¹⁰, and has been named a leader in the 2019 Forrester Wave™: Cloud Workload Security [report](#).¹¹ Additionally, Trend Micro has assessed it meets 8 of 8 recommendations in the 2021 Gartner Market Guide for Cloud Workload Protection¹², helping you to feel confident in choosing Trend Micro to protect your hybrid cloud deployments.

Find out more today at www.trendmicro.com/hybridcloud

¹⁰ IDC Worldwide Hybrid Cloud Workload Security Market Shares, 2020: Time to Shift Left. (Published June 2021)

¹¹ The Forrester Wave™: Cloud Workload Security, 2019

¹² Gartner, Market Guide for Cloud Workload Protection Platforms, 12 July 2021



Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. Our connected solutions are optimized for cloud workloads, endpoints, email, IoT, and networks and deliver central visibility across the enterprise, enabling you to detect and respond to threats faster.

With over 6,800 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. Trend Micro's "Trenders" are passionate about doing the right thing to make the world a safer and better place. www.trendmicro.com.

• **TREND MICRO INC.**
• U.S. toll free: +1 800.228.5651
• phone: +1 408.257.1500
• fax: +1408.257.2003

