Publication date:
20 May 2020
Author:
Eric Parizo

Cisco Tetration: Securing all phases of the hybrid cloud journey

Exploring Cisco's all-in-one solution for full-stack visibility, workload security, and policy compliance

In partnership with:

Brought to you by Informa Tech

Contents

Introduction

A little-known solution with big potential

Cisco Systems offers arguably the industry's most competitive portfolio of best-of-breed enterprise security solutions.

From leading products like Identity Services Engine (ISE) and Firepower that serve tens of thousands of organizations, to innovative solutions like Stealthwatch and AMP, to fast-growing cloud-delivered offerings such as Umbrella and Cisco Threat Response, Cisco has a long history of delivering technology that solves difficult enterprise cybersecurity challenges.

Yet there's a lesser-known Cisco Security solution that doesn't always receive its share of the spotlight, even though its innovation, capabilities, and flexibility rival any other Cisco Security technology.

That solution is called Tetration.

Tetration is a fascinating product; it offers so many unique capabilities that are particularly well suited to help enterprises at *all phases of hybrid cloud transformation*, regardless of whether that journey is just beginning with a few virtual workloads or a small public cloud deployment or encompasses a vast, global data center environment with tens of thousands of workloads across multiple platforms in dozens of locations.

- It can provide **full-stack visibility** across networks, platforms, and applications, offering invaluable insight on the assets and posture of an organization's hybrid data center estate.
- It can **secure workloads** using an innovative combination of communication-control "allow" listing, application segmentation, and software inventory vulnerability detection.
- And it can support **policy compliance** with process behavior baselining and variance detection, detailed asset tagging, and quarantines and communication restriction for non-compliant assets.

This only scratches the surface of Tetration's feature set; it also offers rich capabilities in security analytics, threat detection, and security process automation. Unlike competing solutions that typically require several siloed, standalone products, Tetration delivers all this, and more, in a single solution, which can be deployed on-premises or in the cloud.

Below, we'll explore why Tetration may be the quintessential hidden gem in Cisco Security's portfolio of cybersecurity solutions. We'll detail its multifaceted capabilities and highlight several use case scenarios in which the value of Tetration will be illustrated in how it can solve the real-world enterprise cybersecurity challenges that accompany hybrid cloud data center transformation.

Understanding Tetration's core capabilities

Full-stack visibility

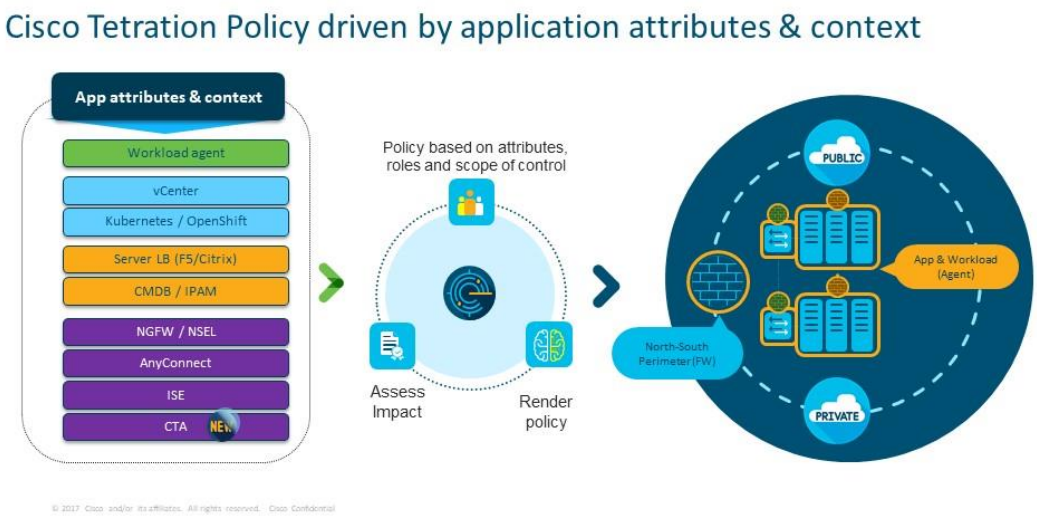
The starting point for any effective hybrid cloud data center security solution must be visibility. True visibility means gathering telemetry to develop an accurate, real-time account for and understanding of the infrastructure's users, devices, networks, applications, workloads, and processes.

Without this broad visibility, securing the data center becomes impossible; visibility is critical to making appropriate security decisions. Imagine attempting to secure data center applications without understanding which applications are actually running in that data center, what they are intended to do, and what "normal" application activity looks like. Abnormal behavior, particularly never-before-seen anomalous activity, becomes difficult, if not impossible, to consistently identify without a way to contrast good and bad activity.

Add to this the complexity of today's hybrid cloud infrastructures. Increasingly, enterprise data center environments include bare-metal and virtualized servers on-premises in private clouds in combination with numerous virtual private clouds (VPCs) hosted in one or more public cloud infrastructures, all of which are augmented by a variety of hybrid IT resources, typically as cloud-based applications or compute services. The size and scope of these sprawling, constantly changing environments is difficult to conceptualize, never mind formally visualize, document, and secure. Additionally, roughly three-quarters of data center traffic is now east-west, meaning the majority of traffic is traversing back and forth within the data center. With all this complexity, cybersecurity stakeholders seeking a visibility solution for these environments often don't know where to turn.

Tetration is uniquely capable of providing visibility for hybrid cloud data center environments. Tetration is designed to gather a wide variety of telemetry data; at its core is a big data analytics engine designed to deliver insights on data center security at scale in today's evolving data centers. That engine gathers detailed metrics related to network traffic flow dynamics, interpacket variations within network traffic flows, and server process-execution details *(*see **Figure 1** below*)*.

Figure 1: Cisco Tetration Information sources



Source: Cisco Systems Inc.

It collects this data using lightweight software-based sensors on hosts, embedded sensors in network infrastructure, and even optional ERSPAN-based packet-capture sensors for additional in-depth insights on data-plane traffic. When combined with supplemental source telemetry (asset tagging, load balancers, IP address management, and configuration management systems) and even streaming JSON sources like SSH logs, the result is pervasive data center visibility and insights.

The level of detail Tetration delivers is practically unparalleled from a single solution. Specifically, the data center network insights provided by Tetration can be categorized as follows:

- **Traffic**: Every packet of every flow at all times is detailed across bare-metal, virtual, and containerized workloads in public and private clouds.
- **Context**: Network flows are correlated with system processes and ownership context, vulnerability of software packages, and process behavior.
- **Traversal**: Application traffic paths, from the data center to the initiating server process, are analyzed.
- **Relationships**: Neighborhoods are visually categorized by traffic profile, communication pattern, and other performance characteristics.
- **Forensics**: Historical flows dating back up to a year or more can be searched.

This visibility provided by Tetration in turn empowers enterprises to make intelligent decisions about data center security controls and eases the process of defining and

enabling the policies necessary for enforcement. Tetration does this through powerful features that allow organizations to proactively leverage the insights it delivers, using them as the foundation for dynamic security controls. Consider these examples:

- Tetration's built-in **microsegmentation** capabilities allow for behavior- and attribute-based security policy. This means policies can be assigned dynamically, as needed, based on asset characteristics. The key benefit is enhanced security policy automation, reducing the time spent on routine policy management tasks such as discovering and defining application segments, as well as updating security policies to align with broader organizational business policies.

- Tetration supports **asset tags**, allowing assets to be categorized and security policy to be applied based on any number of attributes. This saves the long hours often devoted to the creation of manual resource lists that frequently serve as the basis for security policies, plus it eliminates human error that often causes assets to go unsecured and left vulnerable to compromise.

- Because each organization has unique data center visibility requirements, Tetration supports **user-defined reports, alerts, and dashboards**. Tetration data points can be combined with external and even internet-based data to develop customized live content, focusing on key attribute categories, metrics, and alerts.

These examples only scratch the surface of how Tetration can deliver real-time visibility across the data center.

Furthermore, Tetration offers support for numerous operating systems, vendor platforms, and cloud environments. With support for Windows Server and dozens of versions of Linux across leading bare-metal, virtual machine, and containerized platforms in public and private clouds, Tetration offers the flexibility to address the challenges of today's data centers, as well as adapt to architectural evolution in the months and years to come.

Workload security

Server workloads are like the pistons in the giant IT engine powering today's digital businesses. While the cloud currently supports approximately 20% of workloads, according to Omdia's *ICT Enterprise Insights 2019/20 – Global: IoT, Cloud, AI, and 5G* survey, core business systems and mission-critical workloads are increasingly transitioning from on-premises data centers to cloud environments.

Every organization is on a years-long journey to the cloud, and *no two paths look exactly the same*. It is likely that most enterprises will ultimately manage a heterogeneous environment with a mix of Windows- and Linux-based servers, at least one platform-as-a-service (PaaS) with virtual and eventually componentized application services, and VPCs in public cloud environments managed by multiple infrastructure-as-a-service (IaaS) providers.

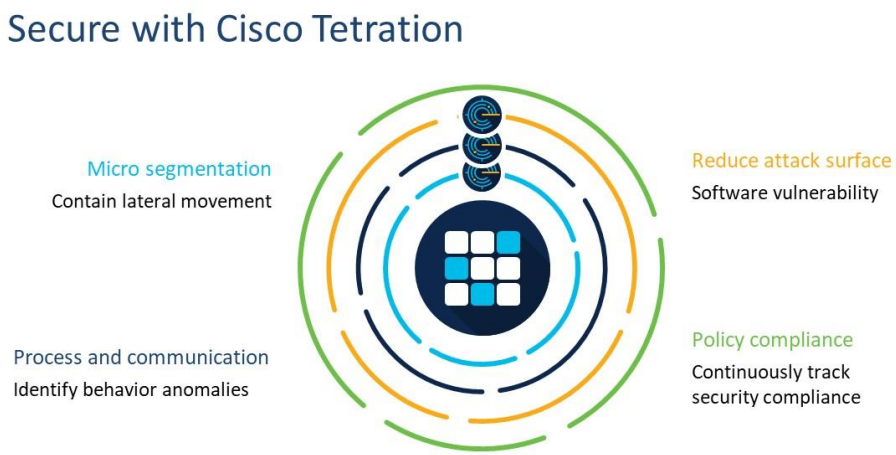
It's no surprise then that server workloads are a top target of adversaries. Not only does each potentially represent a valuable application or data asset to be leveraged, but just one compromised workload can often begin a chain of lateral movements resulting in a

major security breach with disastrous ramifications. Yet it is no small challenge to secure a wide variety of workload types in an ever-changing environment that increasingly exists in cloud environments that enterprises never completely control.

This is why a holistic, multidimensional approach to workload security is essential. Many vendors sell multiple tools providing workload security capabilities across different locations. With Tetration, enterprises get a single solution that applies a single, consistent set of policies and controls across a broad landscape of servers, platforms, and cloud environments.

Tetration stands out against competing solutions because it secures not only the workloads themselves, but also the communications among the workloads. To do this effectively, Tetration incorporates multiple features to provide comprehensive workload protection from the inside out (see **Figure 2** below).

Figure 2: Cisco Tetration holistic approach to workload protection



Source: Cisco Systems Inc.

Those features include the following:

- **Communication control using "allow" listing**: As noted earlier, Tetration's microsegmentation policy model utilizes asset tagging, or metadata-based policy definitions, to govern workload actions. For example, certain tags or even auto-discovered attributes can define which workloads are considered production database servers, and a policy can be set so that database servers can only send and receive communications from other specific internal resources. As new database servers come online with the same attributes, the same policy is automatically applied. This "allow" listing approach – allowing communication only with known, trusted assets – prevents sensitive databases from communicating via the internet, a common scenario in large-scale data breaches.

- **Application segmentation**: Tetration creates virtual communications barriers between workloads, as dictated by policy. The solution can discover and define application segments based on tags or attributes, foster collaborative policy development, secure application segments with automated policy enforcement, and update security policies as often as every 60 seconds. Additionally, Tetration's advanced application segmentation capabilities allow application segmentation policy to span multiple application workspaces. In practical terms, using our previous database server example, this means even if databases are spread out across many unique workloads in a heterogeneous environment spanning private and public clouds, Tetration can apply a single set of application segmentation policy rules across all of the databases. And should a database move from one workspace to another, its policy moves with it. All this ensures consistent security across an entire data center infrastructure.

- **Process behavior analysis and baselining**: Tetration's lightweight on-host sensors take in data on every process executed on a workload; this includes highly granular metrics including process ID, process parameters, the user associated with it, process start time, and process hash (signature) information. Using its big data analytics engine, Tetration creates a baseline for normal or expected activity. Unusual activity or other behavior deviations are instantly mapped against known malware execution patterns, and security events are raised or unknown processes simply terminated based on the outcome. Hence, event sequences in common cyberattacks, such as a privilege escalation followed by a shell code execution, are disrupted because the unknown process would be immediately shut down.

- **Software inventory baselining and vulnerability detection**: Another common struggle in heterogeneous data centers is software version tracking. Ensuring every workload is running an up-to-date, secure software package is nearly impossible, creating an opportunity for adversaries to easily gain a foothold by exploiting known vulnerabilities. Tetration creates a constantly updated inventory baseline of software packages, versions, and patch levels, and those findings are checked against National Institute of Standards and Technology (NIST) national vulnerabilities database (NVD) to identify vulnerable software in the environment. When a newly vulnerable workload is discovered, Tetration can quarantine the instance or block certain types of communications until the insecure software is updated. This feature is invaluable when a major new software vulnerability is discovered, such as the recent Spectre and Meltdown flaws, as enterprises require only a few seconds to identify whether their data center is affected, avoiding time-consuming manual checks that could last hours or days.

Tetration's comprehensive set of layered workload protection features work together to reduce the complexity that comes with workload security in heterogenous data centers. As enterprises evolve those environments to take advantage of opportunities for improved performance, resiliency, and cost savings, Tetration provides consistent, effective, and reliable workload security.

Policy compliance and attack surface reduction

The devil is often in the details; such is the case with IT policy compliance. The objective is consistent, effective enforcement of policy controls – based on security best practices, business rules, and compliance mandates – to reduce and mitigate risk. A key objective from a security standpoint is usually a reduction in the "attack surface," or the areas of opportunity that an adversary may exploit.

Unfortunately, operational policy compliance in most organizations is a massive challenge. Primary and supporting controls are typically provided in the form of a disjointed mix of siloed tools. Monitoring is difficult, measurement and validation is often a best-guess exercise, and non-compliant systems and processes commonly go unnoticed until long after an adversary could have breached the data center environment. Add in the constant change that comes with a data center transformation journey, and suddenly policy compliance goes from challenging to impossible.

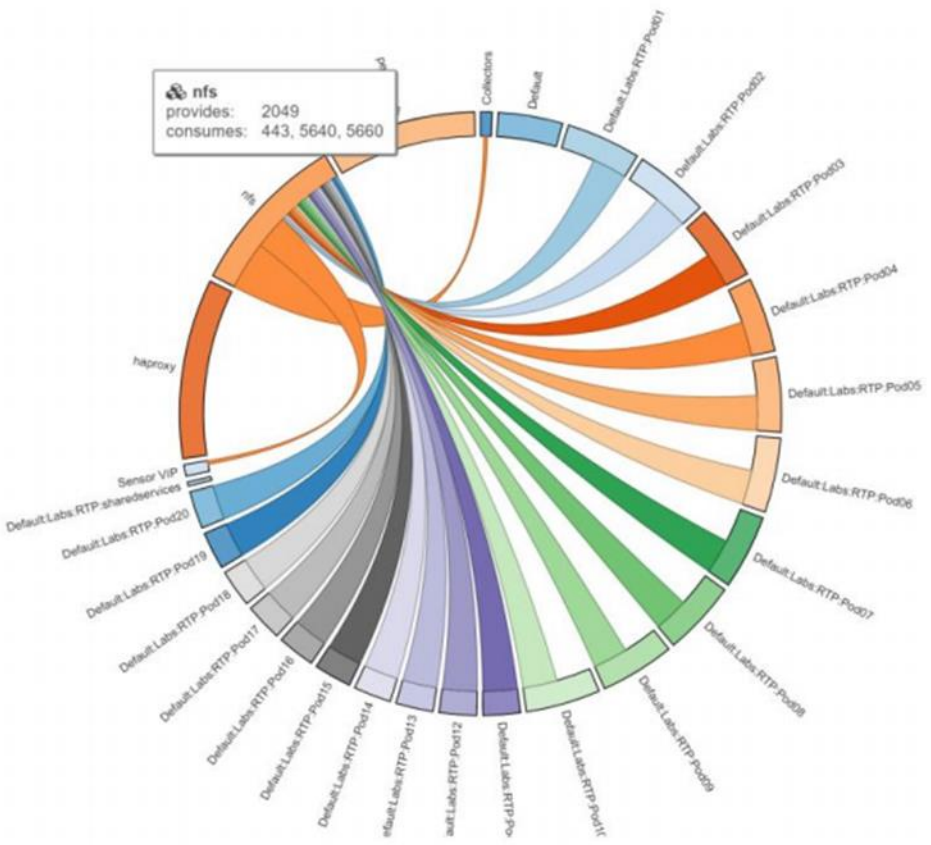
Cisco Tetration, however, offers several key features that make the policy compliance lifecycle easier for all types of data center environments. Not only does Tetration enable enterprises to consolidate and simplify management of data center policy compliance controls and validations, but it also simultaneously reduces the organization's attack surface.

First, as noted earlier, Tetration's microsegmentation model supports policy based on asset tags or attributes, as well as process behavior analysis. This enables a single policy with consistent enforcement in a heterogeneous environment across private and public clouds.

But what if an organization is struggling to manage data center policy collaboration across IT and business groups? Tetration is the only solution of its kind that fosters broad data center policy collaboration. Various stakeholders, each with different roles, can all contribute policy intent actions; Tetration can then combine the intent to create a single policy.

While a “allow” list approach to policy can seem daunting to implement for fear of breaking applications or keeping the policy up to date when changes occur, Tetration addresses this with automated policy recommendation and simulation. The system can generate a policy recommendation based on an automatically created application discovery map, which visualizes host dependencies and communications. Tetration discerns which systems are talking to which others, and even visualizes key details like what ports and protocols are being used (see **Figure 3**).

Fig. 3: Cisco Tetration example policy discovery visualization



Source: Cisco Systems Inc.

From there, it can perform an impact analysis before implementing a policy. Using historical or real-time flow data, Tetration can simulate how actual application traffic would be affected and which flows would be compliant or non-compliant.

Tetration also utilizes role-based access control (RBAC) so that users can be limited to certain roles, or sets of capabilities, as well as scopes of grouped assets and permitted actions. This means different types of users can be assigned to defined role types to work together on a policy: a business stakeholder can view some systems and request a policy change, a manager can approve the change, an administrator can enact it, and an auditor can validate the implementation of a policy as a control.

Because it is constantly monitoring data center environments, after a policy is implemented, Tetration can immediately identify any policy deviation in real time. When found to be out of compliance, these flows can be blocked or flagged for remediation, or even invoke workflows to update policy.

Because policy changes can be implemented in as little as one click, even across heterogeneous environments, Tetration is constantly helping organizations reduce the surface that may be vulnerable to attack. Even when workloads and applications shift dynamically across on-premises and multicloud locations, fine-grained policy

enforcement thwarts the lateral movement that adversaries depend on to move between assets and successfully execute a breach.

These rich policy-compliance lifecycle-management capabilities are supplemented by ongoing software vulnerability detection. Using its software inventory baselining and vulnerability detection feature, noted above, Tetration can correlate vulnerable software packages to policy compliance, enabling administrators to prioritize remediation of high-risk software flaws while also quickly limiting opportunities for attackers.

Finally, policy compliance monitoring notifications can be delivered to stakeholders on a minute-by-minute basis. As an open platform, Tetration integrates with a wide variety of existing customer workflows for alerting and remediation. Alerts can be monitored in the Tetration user interface, as well as transmitted through a Kafka-based messaging broker and consumed by a SIEM or a variety of other third-party collaboration tools such as Slack or IT service management (ITSM) solutions including ServiceNow.

Tetration in practice: Customer scenarios

Because of its wide array of features, Tetration can be considered as a solution for a variety of different customer scenarios. Below, we discuss several example hypothetical customer use cases. While the companies and individuals in these scenarios are fictitious, they are designed to highlight the very real and practical ways in which Tetration meets the security needs of enterprises at all different stages of the hybrid cloud journey.

Scenario one: The legacy acquirer

Ruby Roof Supply is already one of the largest building-products distributors in North America, but it is getting even larger. Its acquisition of a top regional rival means not only an additional $500 million in annual revenue, but also more than 2,000 new employees, additional office locations, and a scattered mix of legacy IT assets.

While Ruby Roof may be on the leading edge of the wholesale building materials industry, its IT architecture is anything but. Its primary data center remains on-premises at its corporate headquarters, with a modest backup site hosted by a co-location provider. Cloud computing usage is still limited to a handful of software-as-a-service (SaaS) applications. The IT assets of its former competitor are even less advanced: with no central data center, workloads are spread out among a collection of regional sites.

Anita, Ruby Roof's chief security officer and deputy CIO, has been tasked with assessing and securing this newly combined IT environment. She is fortunate to have the support of her company's executive team and board of directors, but with so many outdated systems and a clear need to begin transitioning to the cloud soon, Anita is worried about choosing a data center security solution that will help her assess and secure the current environment, while also being capable of adapting to still-unknown security demands once Ruby Roof begins its data center transformation process.

Fortunately for Anita, Cisco Tetration is built exactly for securing complex, nebulous data center scenarios just like the one facing Ruby Roof. Let's examine how Anita can employ Tetration to address her top priorities:

- **Visibility**: Anita has worked hard to manually identify and map Ruby Roof's existing and newly acquired IT assets, but the two companies used different sets of applications with their own toolsets for managing and securing them. Anita needs to know what's really happening, both on the network level and the host level. Tetration offers just that; its ability to gather telemetry from a wide variety of sources provides Anita with the granular detail she needs, including application interdependencies, east-west traffic flow patterns, and the critical context necessary to start optimizing and securing the environment based on current and expected future business requirements.

- **Asset tagging**: Anita was surprised to discover that several of the acquired firm's legacy database servers were accessible from the internet. Fortunately, Tetration not only discovered and flagged this issue quickly, but by combining automated asset tagging with suggested policy remediation, in a few clicks Anita was also able to implement a new security policy using microsegmentation. This ensured mission-critical production database servers would remain isolated from any direct internet communications while allowing them to continue operating as normal. Thanks to Tetration, an unexpected, high-severity security risk was discovered, analyzed, and mitigated in a matter of minutes without a disruption to critical business processes.

- **Consistency**: While Anita's legacy data center is fully mapped and secured, the need to scale in support of the company's rapid growth will soon mean an accelerated transition to a hybrid cloud model. Of course, Tetration can support this evolution as well. Anita's current mix of on-premises bare-metal and virtual Windows and Linux servers are fully supported by Tetration, and when her organization executes its plan to add containerized instances in a public cloud environment, Tetration can scale with her to support this new use case. Tetration's multidimensional workload-protection features, policy model, and management system functions seamlessly in evolving hybrid data center environments spanning private and public clouds. The technical and workflow processes Ruby Roof has built using Tetration can serve as the foundation of the company's hybrid data center security program for years to come. With Tetration, Anita and her bosses can rest assured, knowing they have invested in a solution that provides the consistency they can count on as their data center security needs grow and change.

Tetration's flexible deployment options even suit an evolving environment like that of Ruby Roof. For a relatively small data center, the best fit is often Cisco Tetration Virtual, where software can run on-premises using customer-owned hardware in environments with fewer than 1,000 servers. As Ruby Roof moves to the cloud, Anita can add Tetration SaaS, a software-only cloud-based solution that scales to tens of thousands of sensors and is fully compatible with a mix of on-premises, private cloud, and public cloud workloads.

Anita's situation is challenging, but it is hardly unique; many organizations like Ruby Roof find themselves searching for a single, comprehensive data center security solution for an evolving environment. Tetration addresses the security needs of today's legacy data centers, as well as an unknown and evolving set of security needs for tomorrow's cloud-driven environments.

Scenario two: The fast-growing manufacturer

In business, unexpected opportunities usually bring unexpected challenges.

Medixtend, a medical equipment manufacturer, has enjoyed healthy, predictable growth for several years. However, almost overnight, an unexpected global health emergency has exponentially increased demand for its products. Supporting this rapid growth from a technology standpoint means scaling up nearly all aspects of its IT operations, including its server workload environment.

Bryan, Medixtend's senior director of global IT infrastructure, abruptly finds himself tasked with doubling the workload capacity of his data center as quickly as possible, with a standing order to be prepared to double it again on a moment's notice. Fortunately, Medixtend's digital transformation is already well underway: the organization has been running workloads in the public cloud for several years, so the processes are in place to scale up quickly using on-demand resources. However, in a matter of hours, the composition of the environment changed from having fewer than 50% of workloads in a single IaaS environment to now having more than 90% of its workloads spanning multiple public clouds.

The workload security challenges that come with this sudden and unexpected shift are numerous. Fortunately, Bryan had already deployed Cisco Tetration to manage the security of his growing environment. Hence, he is ready to bring its rich security features to bear to address his key security problems.

- **Adaptation**: If Bryan is certain of one thing, it's that his environment is going change a lot over the coming weeks and months. VPCs will likely need to be spun up, reallocated, and retired frequently. When change is a constant, security controls can struggle to keep up, resulting in restrictions that break business processes, or gaps that create opportunities for adversaries. With Tetration, before Bryan confirms changes to his security policies, he can conduct a full simulation of that change, using real or simulated network traffic, to predict the effects of that change over weeks or even months. This enables Bryan to allow his data center environment to evolve as it needs to, even in unexpected ways, without any security policy guesswork.

- **Automation**: Bryan needs to know that any new workloads or virtual private clouds (VPCs) he creates are secure, but the organization's top priority is getting badly needed IT resources provisioned quickly. Using his existing policy models in Tetration, Bryan can count on Tetration to automatically identify and categorize new application workloads as they're created and apply “allow” list policies to securely segment applications. Plus, because Tetration ensures policies stay with workloads by default, there are no policy enforcement gaps – even when workloads move from bare-metal servers to virtual environments and even as environments scale to add hundreds of new VPCs with thousands or even tens of thousands of workloads.

- **Inventory baselining**: While Bryan's environment is scaling quickly, much of it is doing so in support of Medixtend's mission-critical legacy applications, a number of which have strict operating system and application-component dependencies. Keeping track of which workloads are running which software builds in support of which processes is nearly impossible to do manually. Yet to maintain security, it is critical to ensure that software builds are as current as possible while applying additional controls to reduce risk when older builds are necessary. Fortunately, Tetration's inventory baseline features check software packages, versions, and patch levels continuously, highlighting any vulnerabilities and their severity. This allows Bryan to immediately spot high-risk software instances by applying quantifiable CVE data. This feature is critical to help Bryan determine whether he should encourage a business owner to patch a high-risk application vulnerability, or whether the risk is low and additional controls or monitoring are appropriate. And if a major new software vulnerability comes to light, Bryan can use Tetration to determine if his environment is at risk in a matter of minutes.

Medixtend, like many other enterprises, relies on its hybrid cloud data center environment to be the heart of a scalable, flexible IT infrastructure. When speed and agility are essential for capitalizing on business opportunities, security must be an enabler, not an inhibitor. Tetration offers the capabilities to support organizations that are embracing the hybrid cloud model as quickly as possible but can't afford to sacrifice workload security.

Scenario three: The siloed conglomerate

Doorstop Hotels is a multinational accommodation and experience provider with several thousand properties around the world. Many years of growth, organically and through acquisitions, has created a multibillion-dollar company with a sprawling IT architecture. Its data center assets are highly distributed and highly heterogeneous – dozens of unique applications and operating system versions are in use. While public and private cloud usage is pervasive, it is not centrally managed or coordinated. Instead, each business division has autonomy to make its own IT decisions.

Unfortunately, a series of devastating, high-profile data breaches has shined a spotlight on the organization's inability to limit its attack surface as well as apply and enforce policy compliance controls.

Cynthia, Doorstop's new chief information security officer, was hired to secure the environment and prevent any further data breaches. As if the IT challenges weren't daunting enough, Cynthia has also encountered territorialism within Doorstop – business groups resisting change or even collaboration with the security team for fear of losing influence or control. In the data center, that means Cynthia will be limited in her ability to reduce server sprawl and consolidate down to a handful of key platforms.

Cynthia needs a hybrid cloud data center security solution that can manage security for thousands of workloads in dozens of locations, reduce the attack surface, and provide the policy compliance backstop the organization desperately needs. Luckily, one of her industry colleagues told her about Tetration. Cynthia thought Tetration was merely a server performance-management product, but she quickly discovered that Tetration can address a wide array of enterprise data center security use cases.

Here's how Tetration aligns with Cynthia's key requirements:

- **Collaboration**: It didn't take long for Doorstop's stakeholders to understand that Tetration provides comprehensive full-stack visibility for heterogeneous hybrid cloud data centers, and that its microsegmentation-based controls effectively secure all types of workloads. The problem, however, was that dozens of business and IT stakeholders throughout Doorstop's various divisions needed visibility into how Cynthia's proposed new security policies would affect their applications. But with Tetration's built-in workflows, Cynthia demonstrated how the solution allows business groups to collaboratively define and implement policy across even the most diverse multicloud environments. Using its built-in RBAC support, business leaders could have read-only access to obtain visualizations of their environments and comment on policy, while data center administrators could be granted a granular mix of privileges based on their roles, the risk posture of their VPCs, and other factors. These features allowed Cynthia to position Tetration as a collaborative approach to

data center security, allowing her to obtain buy-in from reluctant stakeholders much more quickly.

- **Compliance**: Following several data breaches, it became a priority for Doorstop's board of directors to prevent any such future incidents. They needed to know that Cynthia's team could rapidly identify and act on any unauthorized event affecting sensitive data and applications across their multicloud data center environment. Cynthia was able to show them how Tetration monitors the data center in real time, identifies any policy compliance violation or anomaly that differs from normal baseline activity, and responds in any number of ways, from alerting on the problem to blocking communications and quarantining workloads until they can be investigated. It can even summarize workload protection posture with overall risk scoring and measures of other key metrics covering vulnerabilities in the environment, network anomalies, and segmentation compliance. Tetration met the board's goals by providing insight on security posture, reducing the organization's attack surface, and being able to quickly identify potentially malicious activity.

- **Communication**: In a large environment like Doorstop's, when security incidents arise, any number of different business or IT groups may be involved in the investigation and remediation. When Tetration identifies a problem, the right groups need to learn of it quickly, in a context that works for them. With Tetration, Cynthia has the power to provide made-to-order alerting. Its built-in Kafka-based message broker can submit configuration or compliance issues through direct integration with ServiceNow, while anomalous events requiring forensic investigation can be sent to the security operations center (SOC) team as an alert in Slack. Other teams can choose to receive alerts via Syslog, email, or even directly to SIEMs or other data analytics solutions such as AWS Kinesis. Some of Cynthia's Tetration power users even discovered that the solution supports custom data-gathering applications developed in Python, Scala, or Spark QSL, and built their own microservices apps to query Tetration's data lake for custom security and performance metrics.

With Tetration, Cynthia gained the granular visibility and control she needed to secure Doorstop's complex hybrid cloud data center environment as well as the supporting collaboration, compliance, and communication capabilities to get buy-in from business leaders and organizational stakeholders.

Conclusion: Many features, countless use cases, one solution

The "journey to the cloud" isn't simple, isn't linear, and isn't without risk; to stave off worst-case scenarios, security must be a critical consideration every step of the way. Cisco Tetration is the multifaceted hybrid cloud data center security solution to secure every point in that journey.

Tetration provides **full-stack visibility** into workload identity, context, and behavior. It can categorize and learn what's happening in a data center, how activity changes over time, and what constitutes abnormal behavior.

It provides multifaceted **workload security**, with a comprehensive set of capabilities including application segmentation and “allow” listing, process behavior analysis and baseline deviation detection, and software inventory cataloging and vulnerability detection.

Tetration also facilitates **policy compliance and attack surface reduction** with not only the capabilities mentioned above but also business-friendly features such as risk scoring, policy collaboration, policy change impact simulation, and an open platform supporting customized reporting and data sharing.

Customers of other Cisco Security solutions can derive even more value from native integrations with Tetration's sister products, including Identity Service Engine for endpoint and user context.

Finally, one of Tetration's best features is that it can be deployed wherever customers need it: as a customizable, high-performance on-premises appliance; as a flexible virtual appliance; or as a SaaS solution for organizations already well on their way to the cloud.

Take the time to explore Tetration's rich features. It’s the one hybrid cloud data center security solution made to fit every journey to the cloud, today and tomorrow.

Appendix

Methodology

Omdia's research methodology for this report may encompass any of the following: detailed technical briefings with applicable vendors, analysis of supplemental information obtained from vendor literature and other online resources, Omdia surveys, and Omdia's data products and market forecasts. The report adheres to Omdia's standards for data accuracy and research quality.

Author

Eric Parizo
Senior Analyst, Cybersecurity
askananalyst@omdia.com

`

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Cisco Systems

Cisco Systems is a leading global provider of networking, telecommunications, and cybersecurity products and services. Founded in 1984 and based in San Jose, California, Cisco has nearly 76,000 employees. The company trades on the NASDAQ (CSCO) and earned nearly $52 billion in revenue in 2019. Its cybersecurity business group, Cisco Security, provides enterprise cybersecurity hardware, software, and services to tens of thousands of customers globally. Cisco Security solutions work together to deliver effective network security, incident response, and heightened IT productivity through automation.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.