CASE STUDY

Jefferson Health Migrates to a Cloud-First Model with Zscaler Workload Posture to Measure and Control Risk

Jefferson Health

Location: Philadelphia, Pennsylvania, USA

Industry: Healthcare

Customer Size: 34,500 employees across 14 hospitals in three states

Jefferson Health is a rapidly-expanding, multi-state non-profit health system with locations in Pennsylvania, New Jersey and Delaware. Established in 1825, the system's flagship is Thomas Jefferson University Hospital, which also serves as one of the system's 14 teaching hospitals. Jefferson Health is considered a top facility on *U.S. News & World Report*'s annual listing of the best hospitals and specialties.

As one of the fastest-growing health systems in the U.S., Jefferson Health began adopting a cloud-first strategy to facilitate achieving its patient care and business goals. With this transition came the need to modernize its cybersecurity posture approach.

"In addition to being a large regional healthcare center, we also support the needs of our research operations and Thomas Jefferson University students," explained Mark Odom, vice president and CISO for Jefferson Health. "Although healthcare is a tightly regulated industry, higher education is collaboration-centric. Balancing these distinct organizational needs requires us to adopt agile systems that allow us to minimize risk and have a strong understanding of our cybersecurity posture."

Controlling risk with CSPM in the cloud

To support its organic and inorganic growth while retaining its patient care excellence, Philadelphia-based Jefferson Health takes a highly quantitative approach to managing risk. Measuring everything helps the institution focus on evaluating a technology's effectiveness, rather than IT industry hype, and assists the security team with quantifying investments in their program.

This analytical process led the healthcare system to accelerate its cloud-first, multi-cloud, adoption, including Amazon AWS, requiring Odom's security operations team to swiftly deploy zero trust cloud security services. It was also critical to ensure cybersecurity posture was maintained while supporting organizational agility for embarking on new development and strategic ventures.

CHALLENGE

- Support rapid institutional growth, a cloud-first strategy and M&A activity in the highly regulated healthcare industry

SOLUTION

- Zscaler™ Workload Posture

OUTCOMES

- Achieved visibility and automated metric generation on the first day
- Doubled compliance scores and established a governance baseline within the first four weeks
- Achieved immediate risk assessment and continuous automated remediation capabilities
- Gained visibility into known and unknown cloud workloads to quickly apply governance policies
- Enabled business innovation, rapid growth and a cloud-first approach
- Established secure workload posture across multiple clouds including AWS

"Zscaler Workload Posture enabled us to establish a common language to drive cybersecurity collaboration."

– Mark Odom
Vice President and CISO
Jefferson Health

Upon evaluating a variety of cloud security posture management (CSPM) solutions, **Zscaler's Workload Posture** quickly rose to the top. "Although Zscaler was fast and effortless to deploy, the game-changer was the ability to provide accurate metrics within the first day," Odom said.

Workload Posture accelerates cloud security maturity

Using Zscaler Workload Posture, Jefferson Health receives continuous visibility of security, compliance, and risk posture; the ability to enforce standards via guided and auto remediations; and governance automation by setting policies, exceptions, and integrations with other IT and risk management solutions.

The company can also go beyond simply identifying misconfigurations by using Workload Posture's ability to prevent them from happening in the first place. Provided coverage spans IaaS, PaaS, SaaS and Kubernetes container environments.

In addition, organizations with regulated cloud workloads like Jefferson Health are able to get instant visibility into their security posture, along with the capability to enforce compliance with applicable regulations, data protection laws, and security standards. This assists with adhering to strict Health Insurance Portability and Accountability Act (HIPAA), Protected Health Care Information (PHI) guidelines and other regulations.

Further, Jefferson Health can leverage Workload Posture's ability to compare SaaS and public cloud application configurations to industry and organizational benchmarks. It also receives granular violation reports and can automate remediation according to established best practices.

High value returns with minimal resource requirements

With Workload Posture deployed, Jefferson Health more than doubled its compliance scores during the first four weeks. "After creating a governance baseline, within a month we improved our compliance scores significantly by working with cross-functional teams on remediations," said Odom.

"We're gaining a high value return from Workload Posture's reporting and monitoring, while dedicating minimal security team resources," he added.

Sage advice for starting a cloud security journey

According to Odom, migrating to an all-cloud security model can be smooth and seamless with the right partner and solution. Establishing a strategy early and implementing an advanced risk posture management solution provides peace-of-mind and simplifies logistics.

"We learned from partnering with Zscaler that the key is starting the cloud security transformation process early," said Odom. "As the future is all cloud, our advice to others is to begin developing your cloud security skills and initiate your journey now."

> "Although Zscaler Workload Posture was fast and effortless to deploy, the game-changer was the ability to provide accurate metrics within the first day."
>
> **– Mark Odom**
> Vice President and CISO
> **Jefferson Health**

Odom also recommends investing in a unified, scalable solution that enables cross-functional teams to collaborate on security improvements. "It's critical for your functional teams to collaborate because security posture isn't about just SecOps, engineering, GRC or DevOps, it's about all of those teams," he said.

"By focusing your efforts on establishing governance controls and process flows, you'll be able to move from reactive to proactive security verifications very quickly," added Odom.

Fueling business innovation, supporting M&A and getting sleep at night

No matter which applications Jefferson Health moves to the cloud, its cybersecurity team has the agility to empower rapid business innovation and support business acquisitions while maintaining regulatory compliance.

"Workload Posture has enabled us to establish a common security collaboration language and provide business users with greater flexibility," Odom said. "We no longer have to tell users they must change their processes to conform to security technology limitations."

What's more, as a university business unit, Jefferson Health now has the visibility into whatever cloud workloads appear next, easing cybersecurity burdens. "Like any university, there are always unknown workloads being spun up," said Odom. "With Workload Posture we can now identify them and begin the process of reducing risk."

> "With visibility into known and unknown workloads, we're beginning the process of reducing risk."
>
> **– Mark Odom**
> Vice President and CISO
> **Jefferson Health**

Striking a balance between regulation and collaboration

Drawing on the power of a cloud-first strategy and zero trust cloud security posture management (CSPM) enabled rapidly-expanding Jefferson Health to enhance patient care, boost staff productivity and measurably reduce risk in a highly regulated industry while also enabling the collaborations that result in healthcare advances and the ability to improve people's lives throughout Pennsylvania, New Jersey and Delaware.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com