CASE STUDY

Goulston & Storrs Elevates Security of Client Data with Zscaler™ Workload Segmentation

Private and public clouds are data-rich targets for cybercriminals. After the initial breach, attackers gain a foothold on an internal system, introduce malicious software, and move laterally to accomplish next-hop exploitation. These environments are often secured with firewall-based controls. Address-centric controls allow malicious communications to piggyback on permitted network policies because they lack visibility beyond primitive network attributes.

Goulston & Storrs is an Am Law 200 law firm, with offices in Boston, New York, and Washington, DC. With more than 200 lawyers across multiple disciplines, the firm is well known as a real estate powerhouse with leading-edge corporate, capital markets and finance, litigation, and private client and trust practices.

Since partnering with Zscaler, the firm has kept pace with the demands of its modern application environment and has secured its network beyond the visibility and control offered by traditional firewalls. The company has experienced benefits from:

- A significantly reduced attack surface, greatly lowering the risk of client data exfiltration
- Operational efficiencies created by machine learning, reducing work associated with protection policy creation and management
- Faster time-to-value since deployment of Zscaler Workload Segmentation does not require changes to applications or network infrastructure

Zscaler Workload Segmentation Use Cases:

- Cloud/Data center workload protection
- Visualize workload risk
- Zero trust networking

Challenges:

- Need to continually increase the level of protection from evolving threats
- Operational inefficiencies due to security
- Outdated security mechanisms that did not align with modern applications
- Complicated policy management

Business Impact:

- Application-level enforcement and continuous trust assessments for gap-free security coverage
- Fast and automatic policy building for greater business agility
- Provided equal protection to client data with zero trust networking
- Visibility into exposure risk to reduce the attack surface

Why Zscaler Workload Segmentation

In the past five years, the legal industry has experienced a movement supporting superior information security standards. Firms, regardless of their size or IT complexity, have become ripe for malicious actors looking to exfiltrate sensitive data. In the new cloud era, there has been considerable change in the data exchange between attorneys and clients. What was once a sensitive document sent by courier is now an emailed PDF, housed in a document management system and other cloud-based collaboration tools and servers. While the challenge of maintaining privacy has always existed, the best-effort protections are pushing firms like Goulston & Storrs to find modern ways to ensure sensitive client data remains inaccessible to attackers.

Zscaler Workload Segmentation brings a level of security sophistication that wasn't available before," explains John Arsneault, Chief Information Officer at Goulston & Storrs. Unlike perimeter defense security mechanisms available to firms, Zscaler Workload Segmentation has modernized network security by using Trusted Application Networking to protect the cloud and data center where traditional methods are ineffective.

> "Zscaler Workload Segmentation has the potential of being the de facto product for every company in the world. With all of the purpose-built security tools existing today, I would still say Zscaler Workload Segmentation supersedes their protections by a tremendous factor. And what's even better is that it does so with incredible ease of use."
>
> **John Arsneault**
> CIO
> **Goulston & Storrs**

Reducing The Attack Surface

To enhance its security posture and protect client data, Goulston & Storrs wanted a solution that mitigated two major risks—exposure of credentials and penetration of the network perimeter. The obstacle in protecting against these threats is that the area of infrastructure or application that an attacker penetrates is often not the ultimate target. Instead, it is used as a jumping-off point to move laterally in the environment to accomplish next-hop exploitation.

"With Zscaler Workload Segmentation's topology mapping, I have an accurate representation of our ever-changing environment and can eliminate potential attack paths that place client data at risk," explains Arsneault. Where attackers could exploit pathways to move laterally before, Zscaler Workload Segmentation automatically measures visible attack surface, quantifies exposure risk and recommends application-centric policies to maximize protection.

Critical Application Security

Traditional security constructs allow application communications based on "trusted" addresses, while being blind to the true identity of the communicating software. Using Zscaler Workload Segmentation's Protect functionality, Goulston & Storrs was able to safeguard its most valuable applications and financial software with a new trust model that approves communications based on the trustworthiness of software, hosts, and users. "Since application identities are continually evaluated, I no longer have to worry about the continuity of client data protection," said Arsneault.

Broad Protection, Small Policy Set

Security often means choosing safety over convenience. According to Arsneault, "Before, to have effective security, there would need to be daily interaction. Now with Zscaler Workload Segmentation, I have one-click enforcement of automatically generated policies, which drastically reduces the time it takes to implement zero trust."

Goulston & Storrs is no longer burdened with balancing security and business agility priorities. In less than 72 hours, machine learning automatically modeled the firm's application communication patterns and generated optimal protection policies to cover 99.99 percent of the network attack surface. "There is practically zero upkeep. Compared to other security deployments, the ease of implementation and maintenance make it a no-brainer," said Arsneault.

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.

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