CASE STUDY

"Dome9 introduces sanity into my security group management. Managing security groups without the Dome9 Arc platform would be insane. We have worked with Dome9 for years now and have seen firsthand how the Dome9 team continuously expands its solution capabilities to further secure our cloud infrastructures."

Rich Sutton
Vice President of Engineering Social Media, Security and Compliance

DOME9 ARC SECURES PROOFPOINT'S CLOUD-BASED SOCIAL MEDIA PROTECTION SOLUTIONS FOR BRANDS

ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media and mobile security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system.

Proofpoint's award-winning, cloud-based social media protection solutions enable brands to prevent abuse, enhance security and ensure compliance across leading social media channels, including Facebook, Twitter, LinkedIn, Instagram, Google+, YouTube and more. With several fundamental social media security patents completed, Proofpoint has won dozens of industry honors, established industry-first capabilities with every release, and earned the trust of more than 100 brands.

THE PROOFPOINT SOLUTION

Proofpoint's social media innovation is based on the concept that security and compliance for a company's social media activity has to happen inside of the social networks themselves and not at the network perimeter of a company that can be, and is bypassed more than 50% of the time. In fact, the only consistent and viable way to enforce security and compliance controls on social infrastructure (e.g., Facebook pages, Twitter accounts, LinkedIn pages and profiles) is to do so via social network APIs. To ensure effectiveness, the Proofpoint application integrates with each social network API, shares intelligence across platforms and provides a unified report dashboard for users.

As a native cloud-based solution, the Proofpoint social media protection services run completely on Amazon Web Services (AWS), leverage AWS building blocks, fully utilize AWS security and compliance standards, as well as multiple independent security verifications, multiple third party security tools, and, importantly, Dome9 Arc solutions to run a highly-secure cloud network. Visit **www.proofpoint.com/us/solutions/application/social-media** to learn more about Proofpoint's social media protection solutions.

From the beginning, Proofpoint's cloud security team understood that their network security challenges required professional resources for protection. Choosing Dome9 Arc was an important and valuable decision that has enabled Proofpoint's social media protection team to run a robust and secured cloud environment.

Industry:
Security, Social Media

Challenges:
- Manage and secure Cassandra EC2 instance IPs
- Control network security configurations
- Manage and maintain strict access policies
- 24/7 Secure Access

Solutions:
- Dome9 Arc IP Lists
- Lock, Revert and Notify
- Role-Based Access Control (RBAC)
- Dynamic Access Leases

Results
- Reduced the system's attack surface and safeguard its social media protection solution from security breaches.
- Reduced operations team with increased efficiency and effectiveness.

CHALLENGES AND SOLUTIONS

1. Complex Cassandra Clusters

Proofpoint's social media protection and compliance solutions are built on Apache Cassandra clusters, which are groups of nodes that hold the same data and span three AWS regions. Proofpoint embraced Apache Cassandra for its scalable and resilient NoSQL persistence database solution qualities and inherent multi-directional and cross-regional asynchronous replication. Cassandra nodes need to communicate with one another within specific AWS Availability Zones (AZs) as well as across global AWS regions. However, managing Cassandra EC2 instance IPs manually (as raw IPs that have to be applied to every security group that's involved) is onerous, time consuming and error prone.

Solution: Dome9 Arc IP Lists

From the beginning, the social media protection services' development team realized that the Cassandra deployment required protocol and port management with multiple security groups and rules, which posed a challenge. IP addresses changed when the Proofpoint team added or reprovisioned Cassandra nodes in AWS. The Dome9 Arc IP Lists simplified management efforts within the dynamic cloud environment. With Dome9, the Proofpoint team has an IP list that applies to a particular service or port in a security group, and can change it across multiple security groups that reference the IP list. Additionally, Dome9 Arc has enabled Proofpoint to reliably update firewall rules in order to maintain secure, cross-regional communication between nodes.

2. Control Network Updates

Proofpoint's solution in AWS' network includes 10 security groups in three regions, each one of which has seven to 10 rules, including multiple IP lists per port as a single rule. Essentially, Proofpoint's cloud deployment network holds more than 300 rules within a global and constantly changing cloud environment. In general, the probability of accidental incorrect security configurations can increase within highly granular network environments because developers and operations personnel have the rights to change security configurations. For example, rules that reveal services to the internet or harm system functionality may accidentally be configured, ultimately putting the network's security in jeopardy.

Solution: Lock, Revert and Notify

The Dome9 Arc platform continuously monitors security group configurations, stops unauthorized users from modifying security groups and automatically reverts unintended or malicious policy configurations. For example, Dome9 can recognize if an SSH port is left open to the world in a security group, revert it and send the Proofpoint team an alert. In addition, Proofpoint's cloud environment spans multiple AWS regions and benefits from the Dome9 Arc AWS Region Lock capability, which guarantees that no network changes will be made to a region unless they are created via the Dome9 console.

3. Access Management

Although Proofpoint's team wants to enable its engineers with freedom of access, it prefers not to reveal secret keys that are required to directly access AWS accounts. As the team expanded its responsibility and headcount, Proofpoint realized it needed robust role-based access control (RBAC) management to maintain strict access policies for different groups of instances (i.e., security groups). This was a best practice as the outcome of not tightly tracking permissions leads to widespread administrative access to the heart of a solution's AWS infrastructure.

Solution: Role-Based Access Control (RBAC)

In addition, Dome9 Arc allows the Proofpoint team to grant and revoke privileges to end users, on demand. The Dome9 team not only recognizes the need for access control in AWS environments, but develops innovative ways to ensure that access is monitored and controlled. In addition, Dome9 allows Proofpoint to simply deprovision users so that they can no longer access AWS rather than manually chasing down each location and security group rule that granted access for a specific individual. The Dome9 Arc platform also provides a two-factor authentication option for end users, which Proofpoint utilizes across its entire user base.

4. 24/7 Secure Access

Proofpoint's social protection development team is responsible for the 24/7 service uptime. Therefore, each individual team member needs to be able to quickly enter and troubleshoot the service's cloud infrastructure from anywhere in the world.

Solution: Dynamic Access Leases

Dome9 Arc's Dynamic Access Leases provide Proofpoint with open, secure, on-demand access, whenever. When new developers and operations engineers join Proofpoint's team, they are provisioned accounts in Dome9 Arc and use the platform to access staging and production environments from their locations.

By using their Dome9 account consoles, the team members receive time-based access to their AWS environment. This approach allows the team to take a closed by default stance, meaning that all administrative (i.e., SSH) ports are closed to the world, including internal networks. The social protection services IT team members are currently using Dome9 Arc, two-thirds of which are developers who use it in their staging environments. One-third of the team is from operations and uses the Dome9 Arc platform to access their production environment.

RESULTS

Dome9 Arc's network security management capabilities play a critical role in hardening Proofpoint's AWS production environment in order to reduce the system's attack surface and safeguard its social media protection solution from security breaches.

> *"Dome9 introduces sanity into my security group management. Managing security groups without the Dome9 Arc platform would be insane. We have worked with Dome9 for years now and have seen firsthand how the Dome9 team continuously expands its solution capabilities to further secure our cloud infrastructures."*
>
> **Rich Sutton**
> Vice President of Engineering
> Social Media, Security and Compliance
> Proofpoint

Dome9 Arc is an important and valuable tool that has enabled Proofpoint's social media protection team to keep the size of its operations team streamlined with increased efficiency and effectiveness.

Proofpoint's social media protection solutions are used by some of the largest companies in the world and need to adhere to the highest security standards. Dome9 plays a key role in supporting Proofpoint's stringent processes in order to ensure that all security and compliance requirements are met.

DOME9 ARC KEY BENEFITS

Agentless, Cloud-native Architecture for Today's Cloud
The Dome9 Arc platform uses the native security controls provided by public clouds such as AWS to protect all cloud resources, including built-in services such as AWS RDS, ELB and Lambda, meeting the needs of today's public clouds that agent-based solutions cannot address. Dome9 Arc allows you to protect multiple cloud environments by combining cloud-agnostic policy automation with cloud-native security capabilities. You can specify policies once across multiple clouds, and the system uses underlying cloud controls to implement the policy on each cloud.

Faster Tme-to-Value with Dome9 Arc SaaS Platform
With no software to install and no agents to manage, you can secure your environment with Dome9 Arc in under five minutes. You never have to worry about software updates and scaling problems. Dome9 Arc integrates with your AWS accounts leveraging innovative cross-account trust policy to gather security information, rather than sharing keys and credentials.

Remediate in Place - Find It, Fix It, Stay Fixed
Dome9 Arc is not just a monitoring solution. In addition to powerful visualization capabilities that allow you to review security posture in real-time to discover any vulnerabilities, compromised workloads, open ports or misconfigurations. Dome9 Arc also allows administrators to take the necessary actions to rapidly mitigate risk through remediation from a single platform. No more patchwork of tools needed for monitoring, remediation, or enforcement, thus bringing agility to the security and compliance lifecycle.

ABOUT DOME9 SECURITY

Dome9 delivers verifiable cloud infrastructure security and compliance to all businesses at all times across all public clouds. The Dome9 Arc platform leverages cloud-native security capabilities and cloud-agnostic policy automation to bring comprehensive network security, advanced IAM protection and continuous compliance to every public cloud environment. Dome9 offers technologies to assess security posture, detect misconfigurations, model gold standard policies, protect against attacks and insider threats, and conform to security best practices in the cloud. Businesses use Dome9 Arc for faster and more effective cloud security operations, pain-free compliance and governance, and Rugged DevOps practices.
Learn more at www.dome9.com.

CONTACT US
Dome9 Security, Inc.
701 Villa Street
Mountain View, CA 94041
+1–877-959-6889
www.dome9.com
contact@dome9.com

For a free security assessment or trail, please contact:
US Sales: +1-877-959-6889
International Sales: +44-20-3322-3209

DPCS09122018