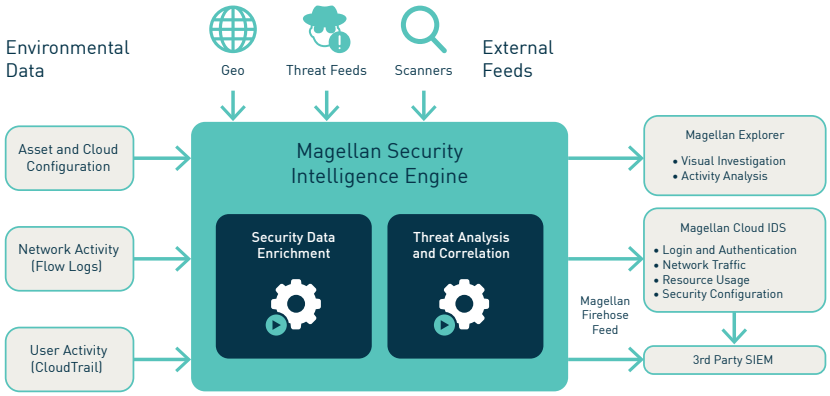
Check Point
SOFTWARE TECHNOLOGIES LTD

FEATURE BRIEF

# CLOUDGUARD DOME9
# MAGELLAN CLOUD-NATIVE SECURITY INTELLIGENCE

Cloud security is fundamentally different from datacenter security. Tools and approaches that worked well in the datacenter are inadequate to secure the public cloud.

- Traditional threat detection tools are left blind to ephemeral serverless and microservice based applications
- These tools are unable to spot cryptojacking in public-cloud infrastructure accounts in time, costing tens of thousands of dollars in a matter in hours or days
- Legacy SIEM and traffic analysis tools struggle to collect, contextualize, and map cloud-based network flow logs




CloudGuard Dome9 Magellan is a cloud-native security intelligence technology that delivers cloud intrusion detection, network traffic visualization and user activity analytics. Magellan's object-mapping algorithms combine cloud inventory and configuration information with real-time monitoring data from a variety of sources including VPC Flow Logs, CloudTrail, Amazon GuardDuty, AWS Inspector as well as current-threat intel feeds, IP reputation and geo databases.

The outcome is rich contextualized information that is used within the CloudGuard Dome9 platform for enhanced visualization, querying, intrusion alerts and notifications of policy violations. It can also be piped to third-party SIEM solutions.

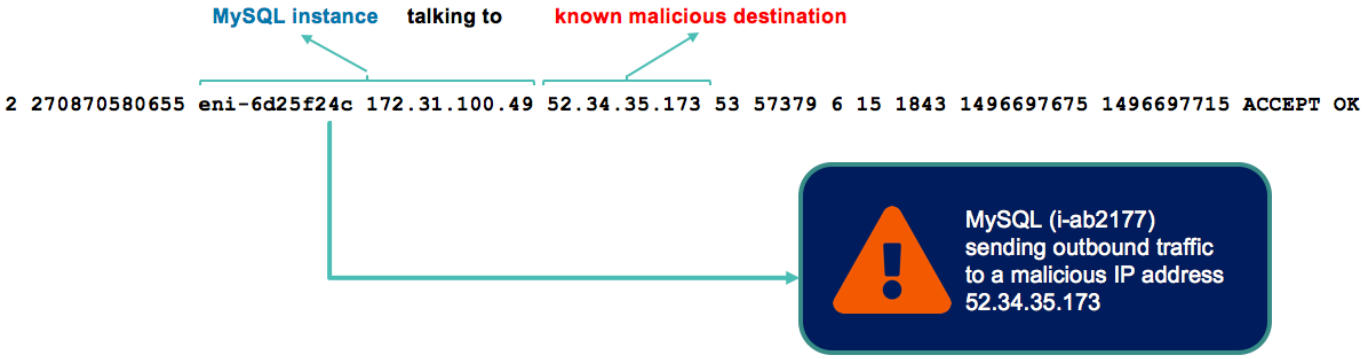
Magellan is the only platform that attributes network traffic to cloud-native ephemeral services such as Amazon Lambda functions as well as other cloud-native platform components (RDS, Redshift, ELB, ALB, ECS) to provide a complete snapshot across time of your cloud infrastructure.

## KEY FEATURES

- **Magellan Explorer** is a visual exploration tool that allows you to analyze the network activity and traffic traversing in and out of your cloud environment. Customers can choose from an extensive set of predefined queries or craft custom ones using CloudGuard Dome9's expressive yet concise query language. The Explorer visualization feature lets you see every element and traffic in your VPC at a glance, and from there, zoom into the relevant entity or connection.
- **Magellan Cloud Intrusion Alerts** use security best practices of signature detection, built-in rules, threat intelligence feeds and existing traffic flow to create a baseline of your network and user activity. Magellan then uses AI and anomaly detection algorithms to spot potentially unauthorized or malicious activity within your cloud environments. Magellan can provide real-time policy violation and intrusion detection alerts based on user-defined criteria to the security admin team.
- **Magellan Firehose** is a connector that feeds the enriched log traffic in a highly contextualized JSON format to various SIEM products for further investigation using the customer's preferred tools.

## DIFFERENTIATION

- **Rapid Threat Detection:** Identify and investigate incidents in your network quickly without lengthy investigations across multiple systems
- **Context-Rich Insights:** CloudGuard Dome9 correlates infrastructure security posture and compliance requirements, along with traffic analysis to provide in-depth context and patterns of anomalous activity.
- **Continuous Threat Monitoring:** CloudGuard Dome9 uses powerful AI and other algorithms to continuously monitor traffic flows from serverless applications.
- **Quick Deployment:** CloudGuard Dome9 is a turnkey solution that integrates with your cloud infrastructure, and provides value within minutes.




*Existing flow log converted to enriched data stream*

## USE CASES

1. **Streamline Network Security Operations:** With Magellan you can conduct network operations such as:
   - Security architecture review based on real-time traffic analysis
   - Gain visibility into your traffic flow
   - Troubleshoot and identify misconfigurations that are causing intrusions/policy violations
   - Identify unusual activity based on user/account behavior
   - Detect malicious sources that are sending traffic to your assets
2. **Reduce Mean Time for Threat Detection:** On average, it takes about 200 days for incident responders to detect a breach. With Magellan, you can identify and zoom in on a suspected asset and understand the full context from both a configuration and traffic activity perspective, thereby reducing your mean time to detect threats.
3. **Detect Privilege Escalation/Credential Compromise:** CloudGuard Dome9 has full context of your account activity and the types of assets in your environment. Using Magellan, you can create a lists of asset types that shouldn't be instantiated. If someone obtains unauthorized privileges to launch an expensive EC2 instance that is perhaps used for crypto mining operations or to steals API keys and now is being misused, Magellan can detect such unauthorized IAM changes or specific EC2 type traffic and immediately provide detailed alerts.
4. **Detect Compliance Policy Violation:** The CloudGuard Dome9 Compliance Engine lets customers validate their compliance posture from a configuration view, but with Magellan Alerts they can now analyze their posture from a real-time traffic perspective and be alerted if violations have occurred (ex. expose PCI instances that are communicating with the outside world).
5. **Expedite Compliance Validation:** Using Magellan Explorer, customers can see a live action replay of their traffic that can be used to prove that their environment is adhering to various compliance standards (Control effectiveness).

## ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

**CONTACT US**
Check Point Software Technologies Ltd.
959 Skyway Road, Suite 300
San Carlos, CA 94070
USA +1-800-429-4391
**www.checkpoint.com**

**For a free security assessment or trial, please contact:**
US Sales: +1-866-488-6691
International Sales: +44-203-608-7492



**CDMPB12102018**