

Security Operations Center (SOC)-as-a-Service

Gateway to a secure cloud market

This Deloitte solution is a customized, **multi-vendor cloud-based SOC architecture** that can be applied across government and commercial spaces to enhance cyber operations in the cloud.



A need:

 **Data transfer costs:** The traditional approach of piping application and security monitoring data in and out of the cloud to a traditionally-hosted SOC can negate the cost-savings associated with migration.

 **Cloud Service Provider (CSP)-specific tools can lead to inflexibility:** Cloud providers have varying protection models with a varying depth of features, often hampering a multi-tenant strategy unless CSP-agnostic tools are natively integrated with CSP-specific ones.

 **Migration is coming:** The push to migrate workloads to the cloud is rarely met with a cost-appropriate and efficiently architected model for providing compliant and effective cyber defenses in the cloud - consistently.

A Solution:

The SOC-as-a-Service (SOCaaS) solution provides a **rapidly deployable cloud architecture** to establish an environment within a public or community CSP that supports the provision of cybersecurity for cloud-based applications. This solution is designed to help organizations address the complexities of applying cloud-based cyber defenses to cloud workloads, saving the time and expenses associated with using a traditional, on-premise environment for this purpose.

 Deloitte’s architecture can enhance the ability to **identify, protect, detect, respond to, and recover from** cyber incidents while simultaneously reducing the costs associated with maintaining infrastructure and transferring data in and out of the cloud for security processing.

 The cloud infrastructure provides a **scalable, highly redundant, highly available architecture** which lends itself to a powerful analytics capability, enhancing the detection and response ability of a SOC.

 Deloitte has engineered how to **natively integrate security tools** in the cloud environment, with CSP native features to provide a comprehensive security picture, that also supports a multi-vendor strategy. This cloud-based SOC deployment facilitates expedient and effective incident response.

Specific differentiators

- ✓ **Distinctive** cloud-based, **multi-vendor** platform applicable across federal and commercial spaces, allowing for flexibility
- ✓ **Easy and expedited adoption** for new customers using automation
- ✓ **Rapidly deployable** cloud architecture has been **tested and** successfully deployed in both government and commercial environments

Organizations who can benefit from SOCaaS

 **Government organizations** looking to establish a cloud production environment.

 **Commercial organizations** looking to strengthen their cloud security program or meet regulatory or compliance requirements.

 Organizations wanting to use **industry leading practices** for defending data and applications in the cloud, whether it operates as a managed service or protects its own applications.

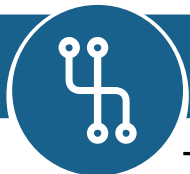
 Organizations looking to reap the benefits of cloud but needs **assistance navigating the unique challenges** with securing data and workloads in the cloud.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2019 Deloitte Development LLC. All rights reserved.

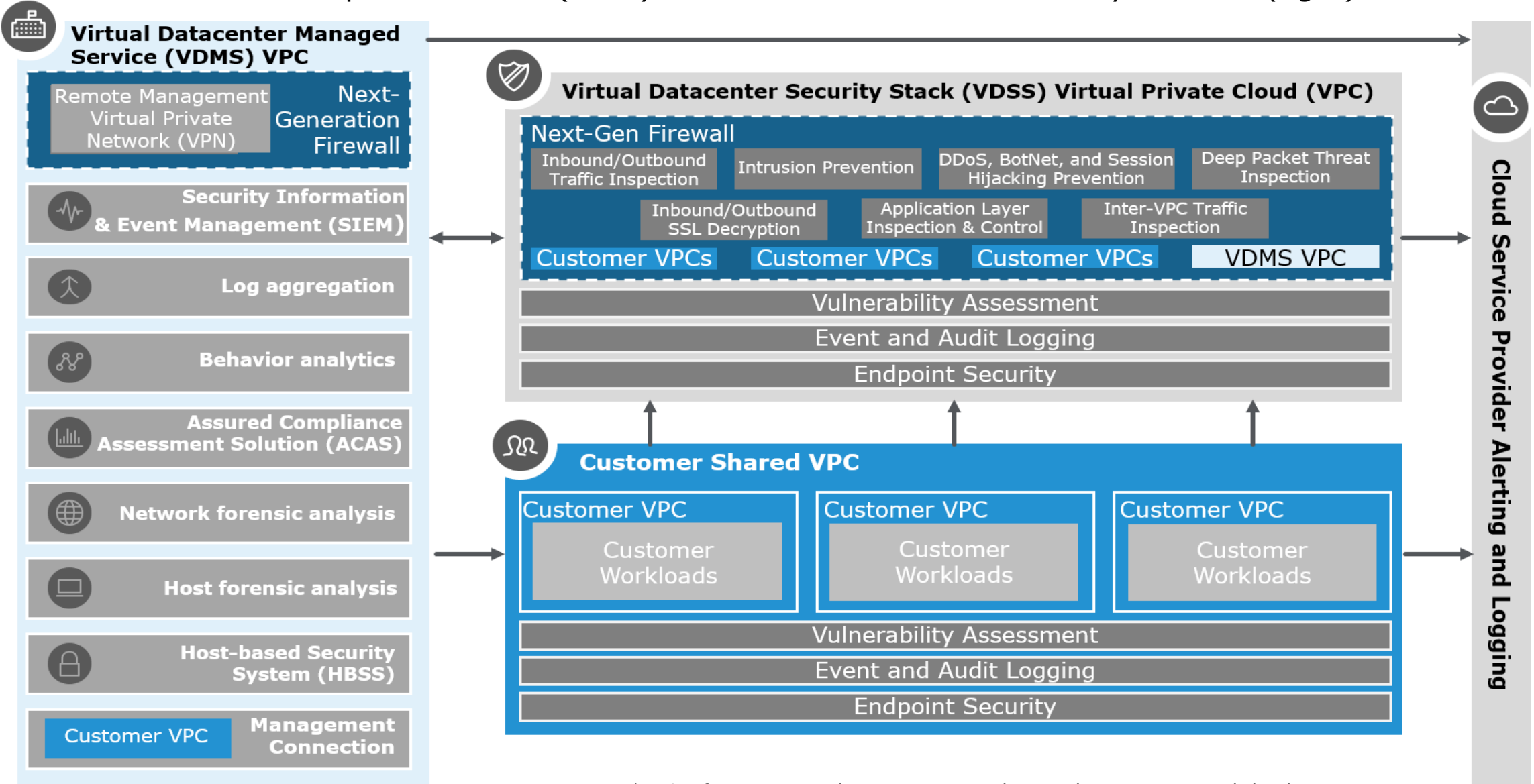
Security Operations Center (SOC)-as-a-Service

Gateway to a secure cloud market

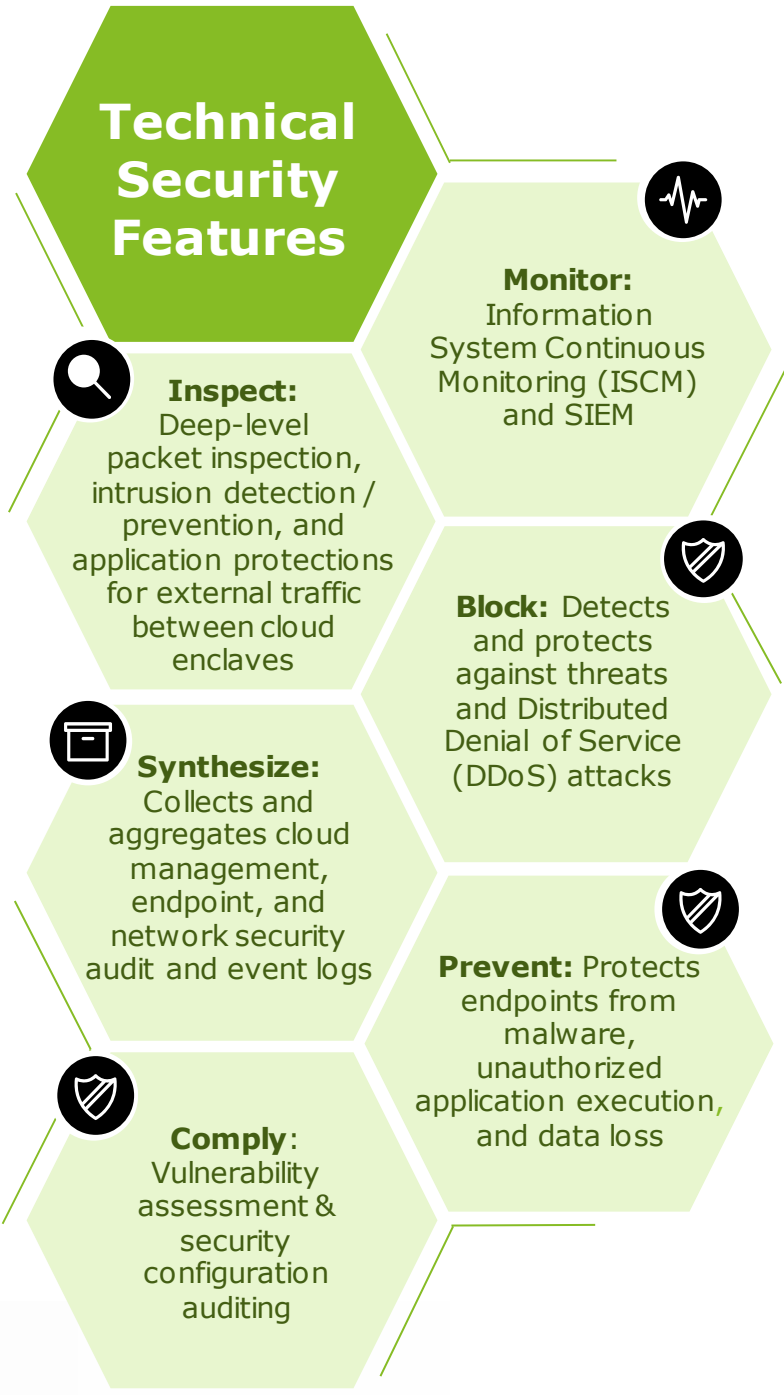


High-level design and security features

The diagram (below) demonstrates how the individual tools integrate within the architecture and how information flows between the different virtual private clouds (VPCs) to achieve the technical security features (right).



*VPC refers to a provider-agnostic virtual network in a commercial cloud environment



Get started by contacting Deloitte's SOCaaS leaders:

Deborah Golden

Principal | Deloitte Risk and Financial Advisory
Federal Cyber Risk Services Leader
Deloitte & Touche LLP
debgolden@deloitte.com

Mark Masone

Principal | Deloitte Risk and Financial Advisory
Advisory Cyber Risk Services
Deloitte & Touche LLP
mmasone@deloitte.com

Aaron Brown

Partner | Deloitte Risk and Financial Advisory
Advisory Cyber Risk Services
Deloitte & Touche LLP
aaronbrown@deloitte.com

Mason Evans

Specialist Leader | Deloitte Risk and Financial Advisory
Advisory Cyber Risk Services
Deloitte & Touche LLP
masevans@deloitte.com

Temi Adebambo

Senior Manager | Deloitte Risk and Financial Advisory
Advisory Cyber Risk Services
Deloitte & Touche LLP
tadebambo@deloitte.com