

The complexity of managing sensitive data across hybrid cloud and multicloud environments is ushering in a new era of pervasive data defense and response platforms.

# Pervasive Data Defense Platforms Address Cloud Security Challenges

February 2020

**Written by:** Robyn Westervelt, Research Director, Security & Trust

Organizations are increasingly challenged by a lack of visibility into disparate resources and insufficient knowledge about the effectiveness of their existing security controls when managing data governance across hybrid cloud architectures. Enterprise security teams are also increasingly citing the growing complexity of their security solutions and the difficulty of integrating cloud components with existing security infrastructure. For example, nearly a quarter of the respondents to an IDC cloud security survey said they had changed their data loss prevention solution once or multiple times since first adopting a cloud architecture.

This complexity has driven organizations to invest in converged security products to protect sensitive data regardless of its location, according to a 2020 data security survey conducted by IDC. More than 64% of IT security professionals said they desire tighter integration of their cloud security gateway and data loss prevention platform to reduce complexity and operational costs. Survey respondents indicated that they highly desire one set of policies for all communication channels (e.g., cloud, email, web, endpoints, and storage), calling this strategy critical to preventing data theft or exposure. This requires a set of seamlessly integrated security components that share threat intelligence and contextual information.

Security professionals consistently tell IDC that the weaknesses caused by maintaining multiple sets of data governance policies in a disjointed security infrastructure are often the source of their security incidents and play a key role in data exposure. Cloud has swelled as business leaders eagerly anticipate the potential advantages of public cloud services. But simple mistakes such as misconfigurations in Amazon Web Services (AWS) S3 buckets led to a rash of data breaches including large multinational corporations and federal U.S. agencies. Cloud providers now offer built-in security capabilities with their cloud services. For many organizations, this built-in security may prove adequate. However, cloud providers cannot ensure protection against all forms of threats or other environments, leaving businesses to identify and fill the gaps — a task that is massively complicated for organizations relying on multiple cloud providers, each with varying degrees of protection and different policy engines and interfaces.

## AT A GLANCE

### WHAT'S IMPORTANT

- » Tightly integrated, fundamental security technologies are evolving into pervasive data defense and response platforms.
- » These emerging platforms represent the convergence of cloud security gateways, data loss prevention platforms, and secure web gateway functionality.
- » These converged security solutions show promise in simplifying management of data governance across multicloud and hybrid cloud environments.

Despite technology initiatives that include artificial intelligence, advanced analytics, machine learning, and modern threat detection solutions, enterprises are often hindered by people and process issues that result in inconsistent data governance policies. Compounding that problem is the issue of inadequate malware scanning in cloud file stores enabling attackers to upload and distribute malicious code within "trusted" applications.

## ***Converged Data Defense Eases Hybrid Cloud Complexity***

Solving these challenges requires deeply integrated security components that function cohesively to protect cloud architectures. Enterprise security teams are demanding simplified management and a mechanism to view their existing security posture from a single pane of glass.

The convergence of fundamental security components is transforming into pervasive data defense and response platforms. These security solutions consist of converged cloud security gateway functionality, robust data loss prevention platforms, and secure web gateways. This convergence unifies policy across the entire security stack and provides a single reporting mechanism. Working in sync, these solutions provide much more comprehensive protection and show promise in reducing the complexity of managing data governance policies across hybrid cloud and multicloud environments.

Pervasive data defense and response solutions provide perimeter-free protection of critical data assets and solve the long-standing issues of security enforcement mechanisms disrupting end-user workflow and becoming too unwieldy for administrators to manage. IDC projects this converged security infrastructure will evolve into a single comprehensive data defense platform joined by a single, unified policy engine; a single management console; centralized analytics; and a consolidated reporting framework.

Pervasive data defense and response solutions consist of the following integrated security technologies:

- » A unified policy engine is the glue that tightly integrates existing endpoint data loss prevention functions that provide policy enforcement over desktops, laptops, mobile devices, USB drives, file/storage servers, and other types of data repositories. Pervasive data defense platforms can ingest existing data classification tags to extend detection and prevention of unauthorized use and transmission of confidential information beyond the traditional corporate perimeter. These platforms support a cloud-based global policy store to maintain a single policy language to ensure compliance and make policy updates easier when business processes and workflows change. They also make critical data searchable and trackable regardless of the location of the assets.
- » At the core of pervasive data defense platforms is the cloud security gateway (CSG), which enables cloud data and permission controls, typically via API integrations. CSGs may also enable the enforcement of acceptable use policies and extend advanced malware protection to data located in distributed environments. They monitor all activity during a session via these API connectors and apply dynamic policy enforcement that can shut down a session, apply encryption or masking, identify malicious behavior, and perform other actions in both directions. The CSG enables visibility into various software-as-a-service (SaaS), web, and public cloud environments and may collect cloud-based evidence files to provide context behind triggered violations to reduce false positives. CSGs also typically support the unification of existing email policies to ensure protection is provided over critical data in motion via Exchange Online or Gmail. They may also support application protections for Amazon Web Services, Microsoft Azure, and Google Cloud.

- » Pervasive data defense and response services also integrate secure web gateway (SWG) functionality from either a web gateway cloud service or an on-premises secure web gateway to provide policy enforcement to long-tail and shadow cloud applications that don't publish public APIs. This integration supports inline content inspection of outbound and inbound traffic and can dynamically scale to support SSL decryption for visibility into encrypted traffic. In addition to providing URL filtering, threat protection, and activity-based controls, SWG capabilities enable risk profiling of frequently used web and cloud applications. The additional telemetry from SWGs enhances data protection by incorporating the source ID and destination of network traffic to improve detection of potential policy violations. This convergence of SWG and CSG threat information into one reporting platform gives security teams a complete view of their cloud access and risk posture that disparate solutions are typically unable to provide.

Pervasive data defense and response services may support an open framework to enable integration and interoperability with third-party security products. Other features that may be supported natively or via third-party integration are incident management and classification tuning, DNS filtering, firewalling, browser isolation, sensitive file encryption, disk encryption, information rights management, backup and recovery software, and an integrated endpoint protection agent. Security vendors may also support tunneling or add integrated virtual private network (VPN) alternatives to ensure secure connectivity of remote offices and mobile users to cloud-based corporate resources.

The resulting benefits of pervasive data defense and response services are data protection and automated responses at critical policy enforcement points. Pervasive data defense platforms enable organizations to implement the same security and policy controls regardless of where users connect. Security administrators can use existing data classifications or choose to classify data once and apply a consistent set of policies that are enforced at critical points across distributed environments. This convergence also creates cohesiveness by enabling the shared telemetry from once siloed security solutions to provide increased context behind newly detected threats and reduce false positives.

## Considering McAfee Unified Cloud Edge

IDC has evaluated McAfee's Unified Cloud Edge solution and found that it meets the key requirements of pervasive data defense and response platforms. It provides cloud-native security that enables consistent data and threat protection controls from devices to cloud services. It consists of three core technologies that are converging into a single solution: Web Security, Data Loss Prevention, and Cloud Security Gateway capabilities. McAfee Unified Cloud Edge centralizes policies and reporting to provide data protection and threat prevention across hybrid environments. The solution combines policy enforcement and access control over managed and unmanaged devices, includes unified incident management to support automated and guided incident response, and simplifies compliance initiatives by leveraging API integrations to cloud services. McAfee MVISION Cloud, the CSG component, recently received FedRAMP certification. The solution was improved with extended threat protection using the machine learning-based web gateway antimalware engine as well as protection for container environments.

## Challenges

McAfee Unified Cloud Edge marks a significant improvement in the McAfee portfolio, but this is a highly competitive space requiring buyers to evaluate the thoroughness and vision of other unified cloud data protection solution providers and their ability to provide pervasive data defense and response solutions. Some competitive approaches converge native user behavioral analytics and information rights management capabilities to make data protection ubiquitous. This may add various degrees of complexity, appealing to a narrower set of enterprises with unique data protection requirements.

## Conclusion

Pervasive data defense and response services can assist enterprise security teams by providing the following benefits:

- » **Regain control over unstructured data.** Pervasive data defense and response services provide greater visibility and control over intellectual property and sensitive data shared internally or externally regardless of location. They capture all the interactions with secure content within the organization, including file types, active devices, files accessed by domain, and files secured.
- » **Reduce hybrid complexity risks.** Increased complexity associated with cloud adoption and managing data governance across hybrid environments results in poorly configured and maintained security infrastructure. Pervasive data defense and response services are a set of integrated and interoperable components to leverage policies from existing data and web security products to help extend policy enforcement across hybrid environments.
- » **Increase security awareness.** Pervasive data defense and response services enforce data governance policies regardless of the location of sensitive corporate data. In addition to reducing the risk of data exposure, extending enforcement mechanisms demonstrates the organization's commitment to data security and privacy, improves employee productivity, and up-levels the ability to detect threats from single environments to hybrid cloud and multicloud architectures.

This approach provides a comprehensive set of risk mitigation mechanisms by combining long-standing siloed data protection capabilities. At its core are data governance policy enforcement mechanisms that protect sensitive data regardless of the environments in which that data resides. Cloud risks increasingly require pervasive data defense for a complete view of cloud-native threats.

Enterprise security teams are demanding simplified management and a mechanism to view their existing security posture from a single pane of glass.

## About the Analyst



### ***Robyn Westervelt, Research Director, Security & Trust***

Robyn Westervelt is a Research Director within IDC's Security & Trust group. She leads IDC's data security practice and provides insight and thought leadership in the areas of encryption, tokenization, data loss prevention, and other data protection, risk mitigation, and compliance technologies. She also contributes thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT).

## MESSAGE FROM THE SPONSOR

**About McAfee UCE**

McAfee Unified Cloud Edge (UCE) is a cloud-native security platform that enables organizations to protect users and data from device to cloud. By converging leading CASB, Web, and DLP components, UCE enables you to apply consistent data protection and threat prevention policies across control points in hybrid environments as your organization transforms to the cloud.

1. Comprehensive visibility and consistent controls over data from device to cloud
2. Consistent threat protection with unified management, and investigations
3. Direct-to-Cloud (AKA 'Internet Breakout') architecture with enterprise scale and resilience

To find out more, please go to [www.mcafee.com/unifiedcloud](http://www.mcafee.com/unifiedcloud).



**The content in this paper was adapted from existing IDC research published on [www.idc.com](http://www.idc.com).**

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2020 IDC. Reproduction without written permission is completely forbidden.

**IDC Corporate USA**

5 Speen Street  
Framingham, MA 01701, USA  
T 508.872.8200  
F 508.935.4015  
Twitter @IDC  
[idc-insights-community.com](http://idc-insights-community.com)  
[www.idc.com](http://www.idc.com)