Powering clients to a future shaped by growth

A Frost & Sullivan Executive Brief

Beyond the Cloud:

Navigating the Dangerous Waters of a Rapidly Digitizing World

With people, infrastructure and information spread out over wider perimeters than ever before, cloud attacks present a growing cybersecurity risk. Amidst this evolution, intelligent and automated security is becoming the first line of defense.

FROST & SULLIVAN

Contents

The Modernization Catalyst: Cloud Migration and its Impact on the Enterprise

Staying relevant and ready within a growing digital landscape

The last decade has seen a whirlwind of change, with digital technologies scaling and bleeding into every fabric of life. Today's consumers communicate, collaborate, work, and live in a staggeringly large digital ecosystem that would be unrecognizable to their predecessors.

Over the past year, in-person interactions at workplaces have almost entirely been replaced by chats and virtual calls through platforms such as Zoom, Microsoft Teams and Cisco WebEx. With travel restrictions leading to an abrupt drop in business travel, collaborative sessions with geographically dispersed groups have moved online, powered by tools such SharePoint, Box, and Dropbox. The impact of virtualization has even extended to the day-to-day minutiae such as signing documents, scanning paperwork or easily digitalizing handwritten notes with applications powered by optical character recognition (OCR). While initially borne out of sheer necessity, some of these newly virtual capabilities have brought significant cost savings and increases in efficiency, and might be here to stay. As a result, enterprises of all shapes and sizes have experienced a modernization overhaul by embracing a sliding scale of virtualization and adaptive new working methodologies. The expectations and innovations that have shaped the modern digital landscape revolve around a few key pillars:

- ***The urgency of simplification:*** By embracing flexibility, businesses are finding it easier to adopt out-of-the-box solutions to maintain service standards during volatile times. C-level leaders are increasingly championing efforts to break down complex, siloed legacy technology stacks to smaller, modular application layers.
- ***Allowing data democratization to power critical business insights:*** As a function of digital transformation, an unprecedented volume of data is being recorded at the network edge and being stored and processed in the cloud. Technologies such as the internet of things (IoT), artificial intelligence (AI), big data and machine learning (ML) are powering business decisions by boosting competitive insight efficiencies.
- ***Reinventing service delivery for a cloud-first world:*** Businesses who focus on customer-centric service agility are in a better position to navigate current and future uncertainties. Strategies within this customer-centric mindset can range from migrating customers to self-serve channels, to allowing seamless movement between different digital channels, providing data-driven personalization, radically simplifying product portfolios, or streamlining pricing structures.

Navigating the expanding attack perimeter of cloud deployments

Due to the enormous explosion of devices brought into the enterprise ecosystem, today's security leaders are faced with a new challenge: the necessity of extending cybersecurity boundaries beyond corporate firewalls:

- Endpoints are among the most vulnerable segments of cloud environments, making it all the more necessary for enterprises to adopt uniform security solutions that support all of their individual cloud infrastructures. These endpoint security tools need to be firmly rooted in zero trust models to be effective, in addition to being centralized.
- Security teams are increasingly focusing on one of their biggest sources of risk - their employees. Moving away from centralized office structures has led to an amplified reliance on a vast network of unsecured devices, often running unapproved applications (aka shadow IT) away from the reign of IT control. As a result, it has become all the more necessary to adopt cross-organization policies that encourage a security-first mindset.

As organizations reimagine their supply chains, spin up more digital experiences, and brace themselves against the realities of expanded remote workforces, threat actors are aggressively focusing on all the new vulnerabilities being exposed.

Examining the Most Urgent Threats Facing the Digital Workforce

Brute force attacks, Sharepoint/OneDrive phishing, malicious third-party apps and OAuth app abuse: The growing threat vectors within an intelligent attack environment

In an evolving environment with increasingly distributed workforces with a host of unsecured enterprise tools and devices, securing access to the ever-expanding application ecosystem is all the more critical. Three of the biggest threats faced by cloud applications today are:

- ***Brute force attacks:*** Proofpoint cloud threats research showed that in the first half of 2020, 97% of organizations came under brute force attacks and 30% of them had at least one compromised cloud account. This research revealed massive cloud attacks targeting legacy protocols and credential dumps, allowing brute force account compromises that are executed both faster, and at a larger scale.
- ***Sharepoint/OneDrive phishing:*** Microsoft 365 and Google Workspace accounts are heavily targeted by cyber criminals because they hold the key to business communication and valuable data. Research conducted by Proofpoint in 2020 revealed that over 16 million email messages were shared with malicious SharePoint Online and OneDrive links. These messages made up only 1.7% of the total sample of messages with malicious URLs, but represented more than 17% of user clicks. Most importantly, Proofpoint research revealed that users were seven times more likely to click on malicious SharePoint Online and OneDrive links that were hosted on legitimate Microsoft domains.

- ***Malicious third-party apps and OAuth app abuse:*** An OAuth app is an application that integrates with a cloud service and may be provided by a vendor other than the cloud service provider. Most OAuth apps request permission to access and manage user information and data and sign into other cloud apps on the user's behalf. Given the broad permissions they can have to a user's core cloud applications, OAuth apps have become a growing attack surface and vector. In a 2020 study of their 20 million (and counting) active cloud users, Proofpoint researchers learned that 10% of organizations had malicious OAuth apps in their cloud environments.

It is becoming increasingly critical for organizations to actively govern access levels, user habits and OAuth applications in order to minimize risk and accidental exposure risk.

The three biggest security considerations in the age of cloud transformation

With cloud transformation having changed the ways in which enterprises collect and share sensitive data, every stakeholder in the ecosystem - suppliers, partners and end-customers - now demands a higher level of security compliance. For most enterprises, the path to a truly secure cloud perimeter is paved by three key checkpoints:

- ***What are the blind spots in my application ecosystem?*** With multiple cloud providers, an enterprise has to live in multiple ecosystems. While each cloud provider that works with an enterprise might have a well-planned, seemingly airtight security strategy, plugging security gaps over multi-cloud infrastructures becomes much more complicated.

- ***How can I automate processes so that risks are caught faster?*** Despite the threat landscape growing more intelligent day by day, enterprises do not always have the resources to manually detect and patch compromised systems. Instead, security solutions with intelligent automation capabilities are replacing tedious, error-prone human tasks to free up skilled resources for more important analytical functions.

- ***What are my most important assets? What are my most at-risk assets?*** Key considerations here revolve around using the right data and access controls built around an enterprise's very attacked people (VAPs). In particular, understanding which users are being targeted by high-priority threats, which attack techniques are the most common, and which users are the most prone to clicking on malicious links is critical. Organizations can map these learnings to focused controls in order to defend against hybrid attacks like SharePoint and OneDrive phishing, gaining visibility across both email and cloud threat vectors.

What Comes Next? Devising the Optimal Security Blueprint for Cloud Applications

Keeping user accounts and data safe using a people-centric, threat-aware approach

In today's reality, simply repurposing generalist security solutions for cloud environments is not sufficient. Effective security leaders are championing security strategies – both technologies and processes - that target the specific needs of cloud-based businesses. Some initial steps to begin laying out clear groundwork for a dynamic, cloud-ready security posture revolve around:

- ***Adaptive controls for both access and data:*** Static security and compliance controls are applied in the same way to every user, and every kind of data. While exhaustive in theory, this increases the burden on lower-risk users, creates an ineffectively high volume of potential false positives, and unintentionally drives employees to seek alternative solutions with unsecured shadow IT. In contrast, access controls enabled by Cloud Access Security Broker (CASB) solutions are adaptive. Security teams can zero in on the most important threats by applying risk-based controls to high-risk and high-privilege users, including step-up authentication, managed-device policy rules and VPN enforcement.
- ***Enforcing single pane visibility:*** To centralize the highly critical process of security monitoring, enterprises need to point the collective strength of their security products over all their constituent cloud services so that aggregated security data can be actioned on in one spot.
- ***Gaining cross-organization sponsorship:*** Security-first companies are starting to build cybersecurity right into their organizational fabric: into their customer relationships, manufacturing and production lines, and vendor procurement processes. The most successful tactics build cybersecurity right into the business value chain, embracing agile technologies to enforce security from the ground-up: from code to consumer.

The critical must-haves of a one-stop information security solution

Business users access and share massive amounts of sensitive data through a variety of SaaS applications such as Microsoft 365 and Google Workspace. Attackers have leveraged this to create targeted attacks on cloud applications, stealing account credentials and taking advantage of vulnerable users through advanced phishing campaigns. Moreover, these attacks are becoming increasingly sophisticated: attackers are even able to coordinate intelligent attacks to bypass multi-factor authentication (MFA).

This is where CASB solutions come in. CASB solutions are designed to provide broad visibility into an organization's users, data and cloud applications, all of which now extend far beyond network perimeters. The most effective CASB solutions leverage a single foundational truth: today's attack landscape targets people, not systems. With the right blend of governance, security and compliance, CASB solutions can transform cloud applications into powerful business enablers, instead of unwitting risk-heavy security blind spots. The three powerful capabilities brought on board by CASB solutions include:

- ***Content awareness*** – To allow easy identification of sensitive data in the cloud, using techniques such as data classification, labelling/tagging, multi-column exact data matching, dictionaries, proximity matching and more
- ***Behavior awareness*** – To enable efficient monitoring and identification of user activity, driving better understanding of user intent for easier threat mitigation
- ***Threat awareness*** – Leveraging cloud and email threat intelligence and/or telemetry to triage compromised accounts

About Proofpoint CASB

Proofpoint provides the only CASB to meet the needs of security people serious about cloud threats, data loss and time-to-value. Your journey to people-centric cloud security starts with IT-approved applications that contain your most valuable assets. We secure Microsoft 365, Google Workspace, Box, Dropbox, Slack, ServiceNow, AWS, Azure and more. Proofpoint CASB protects organizations from account compromise, oversharing of data and compliance risks in the cloud. Our solution combines:

- account compromise and post-compromise activity detection and automated response,
- protection against malicious files in the cloud,
- data security including data loss prevention (DLP),
- cloud and third-party apps governance,
- cloud security posture management and
- adaptive access controls

People-centric visibility to email and cloud threats helps you identify very attacked people (VAPs) and protect their data and cloud accounts. Proofpoint CASB is integrated to our broader Information Protection platform, which allows you to deploy consistent DLP policies across email, cloud, and endpoint. And by aggregating DLP, threat and user behavior alerts on a single console, you can assess and respond to user and data risk more efficiently.

With modern cloud-native platform architecture built for enhanced scale, analytics and extensibility, Proofpoint's solutions can empower enterprises to simplify and accelerate their security infrastructure within weeks instead of years.

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?