Forcepoint

Solution Brief

Security Solutions for Microsoft Office 365

Solution

- Forcepoint offers full and integrated solutions to enhance Microsoft's integrated security to improve visibility and protection against advanced threats and data loss consistently across Office 365 and beyond.
- Forcepoint DLP provides deeper visibility and control of regulated data and intellectual property across the organization and into the Office 365 ecosystem (and other cloud apps).
- Forcepoint CASB can secure Office 365 and all your other SaaS apps.
- Forcepoint Web & Email Security provides advanced email security and integrated enterprise DLP to ensure more effective threat detection & protection as well as data protection for email users.

Outcome

- Improved Security – extend security beyond the Office 365 ecosystem without putting your agency at risk.
- Greater ROI– maximize returns on Office 365 investments.
- Reduced Risk – deliver strong, extensible security against advanced threats without gaps.
- Streamlined Compliance – maintain consistent compliance into the Microsoft ecosystem and beyond.

Government-wide, agencies are rapidly adopting Office 365, which creates new security challenges as IT remodels its security posture to protect the new ecosystem.

The need for security beyond the Microsoft ecosystem

Microsoft Office 365 includes native security at various levels (depending on your license) and, overall, does a good job securing data within its own ecosystem, providing data protection within the operating system, applications, and documents. Additionally, it provides granular access control for all managed devices within an organization.

But agencies must identify other security gaps inherent in the Office 365 cloud app model and considerations for securing their Office 365 deployment. One key security consideration is what happens when the data is not in the Microsoft ecosystem or when it is shared via a thumb drive or Box. What happens when the data extends to another operating system such as Mac or Linux? And how is access controlled outside of managed devices, which is often the case?

Agencies must take a holistic approach when thinking about Office 365 security. Data will extend beyond the Office 365 ecosystem and be accessed through unmanaged devices. Agencies must be able to identify these gaps and provide a robust solution.

The Formula for successful adoption of Office 365

As agencies adopt Office 365, they must implement a centralized security platform for all cloud applications and infrastructure and enhance Office 365 security in five key ways:

- → **Extend** enterprise-class data protection to cloud apps and application environments across the enterprise—not just the Office 365 ecosystem.
- → **Detect and prevent** advanced threats in email and online file shares.
- → **Gain visibility and control** of managed and unmanaged device access for Office 365 as well as other cloud apps.
- → **Detect and control** high-risk users, including compromised accounts and those with malicious intent.
- → **Reduce operational costs** and configuration risk by reducing security silos across Microsoft and third party cloud app security—as well as existing security ecosystems.

To safely harness your Office 365 investment, Forcepoint offers a full and integrated security portfolio that provides visibility and protection for data moving in and out of Office 365 and other cloud apps. Use this Forcepoint guide to learn more about Forcepoint solutions that improve security effectiveness for Microsoft Office 365 ecosystems.

Enhance Microsoft's integrated data security from Forcepoint

When moving to Office 365, it is important that your data protection strategy ensures you have consistent protection and policies that extend beyond the Microsoft ecosystem. Forcepoint provides deep visibility and control of regulated data and intellectual property across your organization and into the Office 365 ecosystem (and other cloud apps). Forcepoint integrates with Microsoft AIP to maximize investments and eliminate data blind spots. As your use of Office 365 grows, Forcepoint keeps your data safe consistently, without having to recreate policies each time, learn new consoles, or juggle different reporting systems.

And, Forcepoint doesn't stop with Office 365—with Forcepoint your data is protected everywhere. Forcepoint DLP provides security focused on people's interaction with sensitive data across cloud applications, network storage, email, and web. As the industry's most complete data protection platform, Forcepoint DLP is recognized as a market leader by industry analysts for its robust coverage of data discovery, endpoint control, network enforcement, and extension into cloud applications.

And today with less time to decipher disparate data, chase false positives, and manage exceptions, Forcepoint's dynamic data protection solutions go one step further and combine behavioral analytics with DLP technology to provide modern security that adapts to real-time changes in risk. Only Forcepoint offers a risk-adaptive approach that leverages behavioral analytics, unified policies, and orchestration to rapidly identify risk, automate policies, and reduce the quantity of alerts requiring investigation.

CAPABILITY	FEATURE	FORCEPOINT	MICROSOFT
Risk Adaptive	**DLP Policies, Rules and Classifiers Comparison**		
	Number of out of box Policies	284	41
	Number of Classifiers	1100+	100's
	Number of Regions specifically supported	7 Regions, 149 Countries	9 Countries plus general
	Industry Specific Policies	14 Industry specific groups: Education, Entertainment and Media, Finance and Banking, Energy and Infrastructure, Government, Hardware, Healthcare and Pharma, Insurance, Manufacturer, Retail, Software, Telco, Transportation, Other.	
Use Cases			
	SSN, PHI, PII, and PCI Data-in-Motion and in-Use visibility through Endpoint channels (Removable Media, Printing, Endpoint Application)	Yes, complete coverage using Forcepoint One Endpoint.	Only supports Exchange email, SharePoint sites, OneDrive accounts, and Teams/channel messages. Defender ATP required for Endpoint channel detections.
	SSN, PHI, PII and PCI Data-at-Rest visibility on the endpoints (Discovery)	Yes, complete coverage using Forcepoint One Endpoint.	Data at rest scanning for O365 environment (SharePoint/OneDrive) Defender ATP required for Endpoint Discovery.
	Monitor data traffic for encrypted/password protected files	Yes, complete coverage using Forcepoint One Endpoint.	Only supports password protected and file type control via Exchange. More information in the following link.
	Incident Risk Ranking	Yes	No
	Optical Character Recognition	Integrated in the DLP license 30+ Languages OOB and 150+ additional languages with language packs.	No
	Data Labeling and Classification	Yes, OEM of Boldon James, plus DLP integration with MS AIP/IP.	Yes, via Azure/Microsoft Information Protection.

CAPABILITY	FEATURE	FORCEPOINT	MICROSOFT
Use Cases			
	Machine Learning	Yes, ability to build DLP rules based on positive/negative examples of content.	No
	Fingerprinting	Yes	Limited to exact match fingerprinting or full file hash match.
	Third Party Application Coverage	Large number of third-party applications covered with DLP Endpoint: http://www.websense.com/content/support/library/endpoint/v85/dlp_apps/Endpoint%20apps.1.2.aspx	Limited to Microsoft applications today, can be extended to some cloud applications via M-CAS CASB API's.
	File Type Support	Over 500 supported file types, powered by KeyView.	80, mainly focused on Microsoft extensions.
	Integration with Classification	**Label Taxonomy:** Forcepoint Security Manager (FSM) console makes it easy to import 3rd party file labelling systems. Label schemas from Azure Information Protection and Boldon James can be directly imported into FSM. **Classify:** Create custom classifiers based on the needs of your business (i.e.. Public, Confidential, Top Secret). Link file labels to classifiers to facilitate detection of sensitive data via policy. **Automated Labeling:** For misclassified documents, DLP agent detects fingerprinted text (including partial fingerprinting) within a document. Automatically apply the appropriate label when transferred to a removable storage device.	

The bottom line: Whether you're migrating to Office 365 over a long period of time or are 100% all-cloud, Forcepoint gives you the ability to enforce strong and consistent security controls as you evolve your IT infrastructure so that you can reduce point product fatigue and relieve the burden on your already stretched security teams.

Extend enterprise-class data protection to all cloud apps and application environments

Office 365 provides protection for data within the Microsoft ecosystem. But just as data might be shared through various channels, data can also be shared through many cloud applications outside of the ecosystem. This includes popular applications such as Salesforce, Dropbox, Workday, and Marketo; all of these applications could leave gaps in your security solution. In addition, IT is often not aware of the thousands of cloud applications in use by HR, Finance, and Marketing every day. This is a huge gap for IT departments responsible for data privacy and security.

Security policies and protocols should not be created separately for each cloud application. Instead, cloud apps should be governed uniformly to ensure compliance and visibility. Advanced IT security departments want a solution that allows them to enforce procedures, and provides visibility into every application in use within the organization. Limiting security to Office 365 leaves significant security gaps.

Stealing login credentials is one of the most popular techniques to get access to sensitive data stored in Office 365. Forcepoint CASB has pre-defined, sophisticated algorithms to fingerprint devices and learn user behaviors in order to detect data access anomalies (indicating a possible external or insider threat). If an anomaly or account takeover is detected, Forcepoint CASB provides several remediation options, including blocking access or requiring stronger identity verification, to help protect against cyber threats.

The automatic data synchronization (auto-syncing) feature of Outlook, OneDrive for Business, or ActiveSync mobile email app poses serious risk. Forcepoint CASB enables granular access control from BYOD, allowing you to block auto-syncing of email and files in real time to unmanaged devices without the need to install agents on the unmanaged device. This prevents data proliferation and ultimately enhances Office 365 security.

Additionally, Forcepoint CASB monitor activities, identifies security and compliance gaps, and helps prevent data leakage. Forcepoint CASB gives you complete visibility into all of your Office 365 users, even contractors and ex-employees who might still have access to your Office 365 instance. Forcepoint CASB monitors all Office 365 activities in real-time, including uploads, downloads, and shares to enable you see what users are doing all the way down to the individual action and data object. Forcepoint identifies sensitive or regulated data stored in OneDrive to ensure compliance with regulations such as FISMA, NIST, and HIPAA. Forcepoint CASB enables agencies to control the sharing of sensitive data and files through granular file-sharing policies. Forcepoint inspects content in real-time, applying comprehensive Office 365 data loss prevention (DLP) policies. Forcepoint CASB includes an ICAP interface to integrate with Forcepoint DLP or third-party DLP solutions. If a policy threshold is triggered, you can display an alert, block the specific action or account, or require two-factor authentication to verify someone's identity.

Forcepoint CASB helps agencies identify and protect all cloud applications in use and to take back control of unsanctioned cloud applications impacting the full adoption of O365. Additionally, integrations with Forcepoint CASB and DLP Cloud Apps enable agencies to extend DLP policies to the cloud.

FEATURE	FORCEPOINT	MICROSOFT
Discover shadow IT	●	●
Protect sensitive info in cloud apps	●	Microsoft only
Built-in anomaly protection policies	●	Basic templates, need customization
Control for managed and unmanaged devices	●	
Endpoint DLP	● Integrated with F1E	Only available with Windows ATP
Log upload	●	●
API deployment	●	● 12 apps
Inline (proxy) deployment	●	
Reverse proxy deployment	●	Yes, Azure AD license required
Agent deployment	●	
User Behavior Analytics	●	●
Data protection policies	●	Only for Microsoft products through Microsoft
Threat protection integration	● AMD	● Defender

The bottom line: Microsoft's CASB supports API protections for Microsoft supported applications, but for support beyond primarily the Microsoft stack, Forcepoint provides complete security for all cloud applications.

Address advanced threats as they happen

Your agency and its data are under constant attack. Traditional security solutions no longer provide sufficient protection. In fact, they can put you at risk for data loss and litigation. Protecting your network and data against advanced threats, crypto-ransomware, and exploit kits are crucial as you adopt Office 365 in an increasingly risky mobile and cloud-connected digital world. In its 2019 "Critical Capabilities for Secure Web Gateways" report, Gartner recommends that security and risk management leaders evaluating SWG solutions look at vendors across three use cases, including support for monitoring/visibility, malware detection and advanced threat defense, and connecting offices and mobile and remote workers. Forcepoint can help in all of these areas.

Most of today's web security solutions do not address advanced threats as they happen and use static rather than dynamic analysis to defend against advanced threats. Forcepoint Web Security enables advanced, real-time threat defense. Forcepoint Web Security provides robust protection through content-aware defenses and cloud app discovery and monitoring, reducing risks to sensitive data for both on-premises, mobile, and remote workers.

Best of all, Forcepoint Web Security easily integrates with other Forcepoint solutions for single, consistent security controls that can protect against inbound and outbound threats with even the smallest of security teams, enabling real-time threat defense that enables agencies to:

- → **Secure every user, everywhere, from advanced threats.** Extend your protection seamlessly to both on-premises and remote workers, wherever they access the network.
- → **Achieve integrated visibility and control.** Discover cloud applications being used within your organization. Monitor usage of those applications to determine and block those that represent the greatest risk.
- → **Reduce security spend while improving operational efficiency.** Quickly discover Shadow IT to ensure risk exposure is managed. Apply controls with full integrated Cloud Access Security Broker (CASB) features as part of the Web Security Gateway for cloud applications supported via inline (proxy).

FEATURE	FORCEPOINT	MICROSOFT
Advanced threat detection	●	
Cloud Service	●	●
Hybrid functionality	●	
CASB	●	●
DLP	●	●
Advanced functionality	●	

The bottom line: Microsoft's CASB supports API protections for Microsoft-supported applications , but for support beyond primarily the Microsoft stack, Forcepoint provides complete security for all cloud applications.

Prepare for sophisticated attacks

Most large-scale cyberattacks originate from email, using advanced, coordinated tactics, such as socially engineered lures and targeted phishing. As these multi-stage threats blend web and email elements throughout attacks, they present a "Kill Chain" of opportunities to stop them before the breach occurs. Office 365 has limited abilities to detect or block today's sophisticated attacks as well as limited features around sandboxing and behavior analysis. As you adopt Office 365, it is important to consider Zero-day, Phishing, and Ransomware attacks and ensure you have a strategy to enhance native Office 365 security with additional threat isolation capabilities. Forcepoint's advanced threat protection is a proven market leader, enabled with a simple checkbox. Forcepoint provides these additional security controls needed over the basic email hygiene services that can be enabled within Office 365.

Forcepoint Email Security provides advanced email security and integrated enterprise DLP to ensure more effective threat detection and protection, as well as data protection for email users. Advanced malware defenses detect threats and protect Office 365 users against malware attacks in email and on-line file shares. From inbound attack activity to outbound data theft or botnet communication attempts, Forcepoint Email Security secures mixed environments with content-aware defenses, protecting email communications as part of a complete and connected defense system against Advanced Persistent Threats (APTs) and other types of advanced threats. Forcepoint Email Security helps identify targeted attacks, high-risk users, and insider threats, while empowering mobile workers and the safe adoption of new technologies like Office 365. This will enhance native Office 365 protections that give visibility into many threats to the Microsoft stack. Forcepoint also provides an enterprise-wide view across other applications or data stores, which is necessary in order to be effective against coordinated or even slightly advanced attacks. Forcepoint can provide visibility and protection over the entire enterprise, covering Web Security, Email Security, DLP, Cloud Security, User Behavior Analytics, and more.

CAPABILITY	FEATURE	FORCEPOINT	MICROSOFT
Email Security			
	Antimalware, Antispam	●	●
	Sandboxing	●	●
	Email Data Loss Prevention for PII, PCI, PHI	●	● Not available in E1
	DMARC, DKIM, SPF	●	●
	Encryption	●	●
	Service Level Agreement	99.999% availability, 99% spam detection and 100% threat protection.	99.9% availability, 99% spam detection (English language emails only), Microsoft limits payment to a 25-percent service credit, even after multiple infections in a month.
AntiMalware, AntiSpam			
	Real-time Antivirus Scanning	●	●
	Real-time Spam Prevention	●	●
	Sandboxing	● Via Advanced Malware Defense	● Limited in file scope
	Real-time Protection against Zero-day Threats and Advanced Malware	●	Yes, basic scanning and blocking capability, but not the 10,000 analytics that the ACE engine delivers.
	Phishing Protection	●	●
	Advanced Email Encryption	●	●
	URL Sandboxing	●	●
	DMARC, DKIM, SPF	●	●

CAPABILITY	FEATURE	FORCEPOINT	MICROSOFT
AntiMalware, AntiSpam			
	Threat Intelligence	**Yes,** Forcepoint and Microsoft share some threat intelligence as part of a partnership agreement.	●
	Phishing Education	●	●
	Phrase, Single word based detection	●	Yes, but requires Data Protection addon for Office 365.
	Predefined Compliance Rules	**Yes,** PCI (Credit Card Numbers) and SDPL (Social Security Numbers).	Yes, HIPAA, PCI, PII, Gramm-Leach Bliley and Illegal Drugs templates, but requires Data Protection addon for Office 365.
	Regex-based Detection	●	Yes, but requires Data Protection addon for Office 365.
	Integration with on-premises/ enterprise DLP	**Yes,** via DLP Protector hosted in customers Azure instance.	Yes, via redirect to third party DLP (no additional capabilities from Microsoft).
	Redirect to Encryption	●	Yes, using OME (requires Information Protection addon or minimum of E3 license).
License Comparison			
	Email Security	●	●
	Email Policy Based Encryption	●	●
	Email ATP (Sandboxing)	●	●
	CASB Audit	●	●
	CASB Saas and IaaS (API)	●	●
	CASB SaaS and IaaS (Inline)	●	
	DLP Suite (Endpoint, Storage, Network)	●	
	Enterprise Cloud Email and Web DLP	●	
	DLP OCR	●	
	Web Security Service	●	
	Malware Analysis Service (Sandboxing)	●	
	Endpoint Encryption		●

The bottom line: To prepare for advanced threats, Forcepoint provides the additional security controls needed to effectively detect or block today's sophisticated attacks.

forcepoint.com/contact