RAPID7 + Office

INTEGRATION BRIEF

Increase Security and Transparency for Office 365

With Rapid7 InsightIDR

Solution Overview

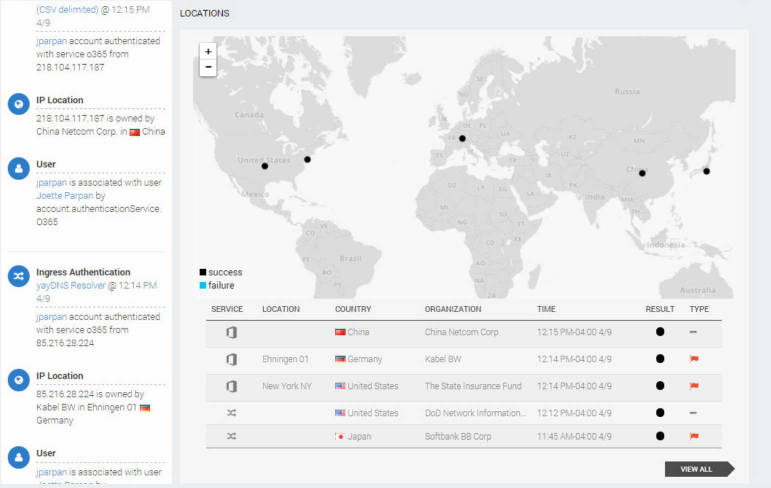
As Office 365 and other cloud services extend the security perimeter to the individual user, it's a challenge to identify intruders moving across your on-premise, cloud, and mobile sections of your network ecosystem. By using stolen credentials, the number one attack vector behind breaches, attackers are able to remain undetected for months. Today's monitoring solutions have no way to detect malicious lateral movement and data exfiltration.

Rapid7 is an early access partner with Microsoft, integrating the new Office 365 Management Activity API with its intruder analytics solution, InsightIDR. InsightIDR builds a baseline understanding of a user's behavior in order to identify changes that would indicate suspicious activity and help security professionals detect an attack. By collecting, correlating, and analyzing data across all users and assets, including cloud applications, InsightIDR automatically identifies suspicious behavior. Some examples of potential threats that can now be detected within Office 365:

- **Advanced attacks:** InsightIDR automatically correlates user activity across network, cloud, and mobile environments. InsightIDR can detect advanced attacks such as lateral movement from the endpoint to the cloud, including Office 365.
- **Privileged user monitoring:** Privileged users are often the ultimate target for intruders. InsightIDR monitors Office 365 administrator accounts and alerts the security team of suspicious activity.
- **Geographically impossible access:** A key to protecting the environment is to be able to unify network, mobile, and cloud environments. For example, a customer would receive an alert if an employee's cell phone synchronizes email via Office 365 from Brazil within an hour of the same user connecting to the corporate VPN from Paris, clearly one of the connections cannot be legitimate.
- **Account use after termination:** InsightIDR detects when a suspended or terminated employee accesses their Office 365 account, helping to stop stolen intellectual property and other business-critical information.
- **Access to Office 365 from an anonymization service:** InsightIDR correlates a constantly-updated list of proxy sites and TOR nodes with an organization's Office 365 activity, detecting attackers that are trying to mask their identity and location.

Integration Briefs

1. Complete visibility into your users' authentication activity, inside and outside the network perimeter.
2. Detect the attacks you're missing across the entire network ecosystem, from the endpoint to the cloud.
3. Monitor authentications into Office 365 from suspicious locations.
4. Monitor ingress into Office 365 from malicious locations or anonymized sources.



(CSV delimited) @ 12:15 PM 4/9

jparpan account authenticated with service o365 from 218.104.117.187

IP Location

218.104.117.187 is owned by China Netcom Corp. in China

User

jparpan is associated with user Joette Parpan by account.authenticationService.O365

Ingress Authentication

yayDNS Resolver @ 12:14 PM 4/9

jparpan account authenticated with service o365 from 85.216.28.224

IP Location

85.216.28.224 is owned by Kabel BW in Ehningen 01 Germany

User

jparpan is associated with user

SERVICE	LOCATION	COUNTRY	ORGANIZATION	TIME	RESULT	TYPE
		China	China Netcom Corp.	12:15 PM-04:00 4/9	●	–
	Ehningen 01	Germany	Kabel BW	12:14 PM-04:00 4/9	●	🚩
	New York NY	United States	The State Insurance Fund	12:14 PM-04:00 4/9	●	🚩
		United States	DoD Network Information...	12:12 PM-04:00 4/9	●	–
		Japan	Softbank BB Corp	11:45 AM-04:00 4/9	●	🚩

Figure 1: InsightIDR identifying multiple country authentications to the same Office 365 account over an impossibly short time period.

Once suspicious behavior is detected on Office 365 or anywhere on the network ecosystem, security teams and incident responders can investigate the users and assets involved, and determine the impact of the attack. With InsightIDR's visual investigation capabilities, customers can combine asset and user data on a timeline to quickly investigate and contain the incident.

Rapid7 InsightIDR

Rapid7 InsightIDR is an intruder analytics solution that gives you the confidence to detect and investigate security incidents faster. Only InsightIDR gives you quality alerts without the noise, enables your entire team to investigate an incident, and add user context to your monitoring solutions. Unlike other solutions, InsightIDR monitors activity not just on your network, but across endpoints, mobile devices and cloud. InsightIDR gives you instant visibility into user activity across your infrastructure and monitoring solutions. Rapid7's unique understanding of attacker methodologies is the key for producing these highly accurate analytics.

How It Works

Rapid7 InsightIDR uses the Office 365 Management Activity API to ingest the authentication data for users across the organization. These logs are analyzed and combined with network, endpoint, mobile, and attacker methodology, to detect intruders and risky internal behavior. Incident alerts are automatically generated in InsightIDR.

1. Set up Rapid7 InsightIDR
2. Set up InsightIDR's collector to take Office 365 API feeds

What You Need

Rapid7 InsightIDR	**Microsoft Office 365**

About Microsoft Office 365

Microsoft Office 365 delivers the power of cloud productivity to businesses of all sizes, helping save time, money, and free up valued resources. Office 365 combines the familiar Microsoft Office desktop suite with cloud-based versions of Microsoft's next-generation communications and collaboration services—including Microsoft Exchange Online, Microsoft SharePoint Online, Office Online, and Microsoft Skype for Business Online —to help users be productive from virtually anywhere through the Internet.

About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,400 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

Support

Please contact Rapid7 for support or assistance at +1.866.380.8113, or through our Customer Portal.

Customer Portal