SOLUTION BRIEF

FortiCWP Threat Detection and Response

Executive Summary

With migration of applications to Infrastructure-as-a-Service (IaaS) and the increasing risk of security threats in the public cloud, organizations cannot easily detect and respond to threats fast enough in their hybrid and multi-cloud environments. FortiCWP provides centralized security monitoring and threat detection, enhanced by global, up-to-the-minute threat intelligence on botnets, zero-day exploits, and more. The result is faster detection and response and improved efficiencies for overstretched security teams.

Multi-cloud Threat Detection and Response

- Centralized visibility of threats
- Predefined and custom threat detection policies
- Automated threat response workflows
- Real-time intelligence on advanced threats

Clouds Drive Gains but Hide Risks

Organizations have embraced the public cloud. Public cloud services are expected to grow by 17.3% in 2019 to $206 billion worldwide.[1] The benefits of the cloud are indeed compelling; they include increased flexibility, faster time to value, the ability to scale up or down on the fly, and cost-efficiency from being able to pay only for resources used.

However, after a decade or more of aggressively adding cloud resources, security teams are struggling with cloud sprawl. Resources from different clouds have been added across multiple regions, all without centralized control. This makes it difficult to distinguish between legitimate activities and those that are not legitimate. FortiCWP offers comprehensive threat policies that come with predefined rules as well as the ability to customize threat policies. Further, leveraging extensive threat intelligence from years of research by FortiGuard Labs, FortiCWP offers predefined threat policies to address the most common misconfiguration and activity-related threats.

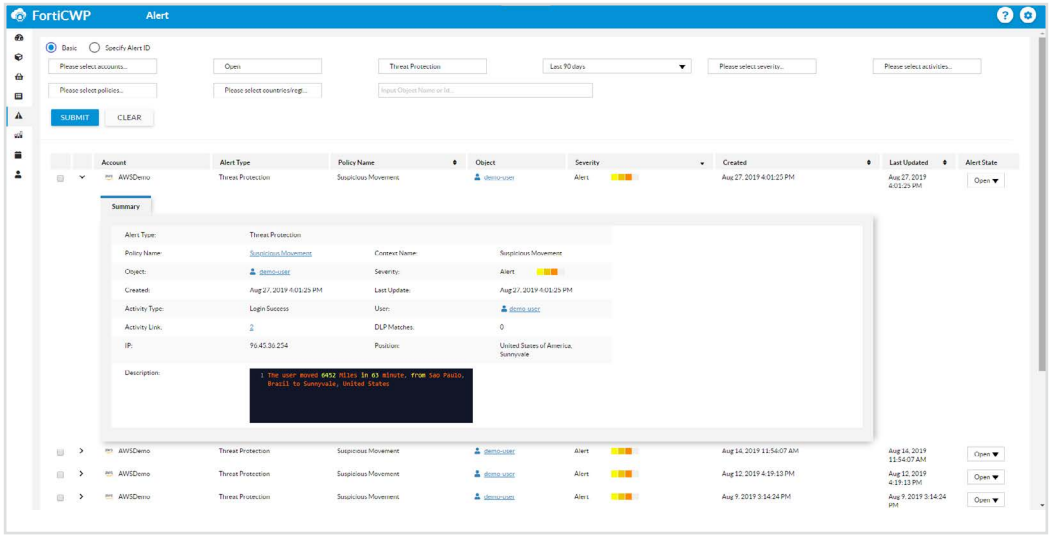

Figure 1: FortiCWP dashboard.

A centralized dashboard integrates security capabilities across multiple clouds with live global intelligence on advanced threats.

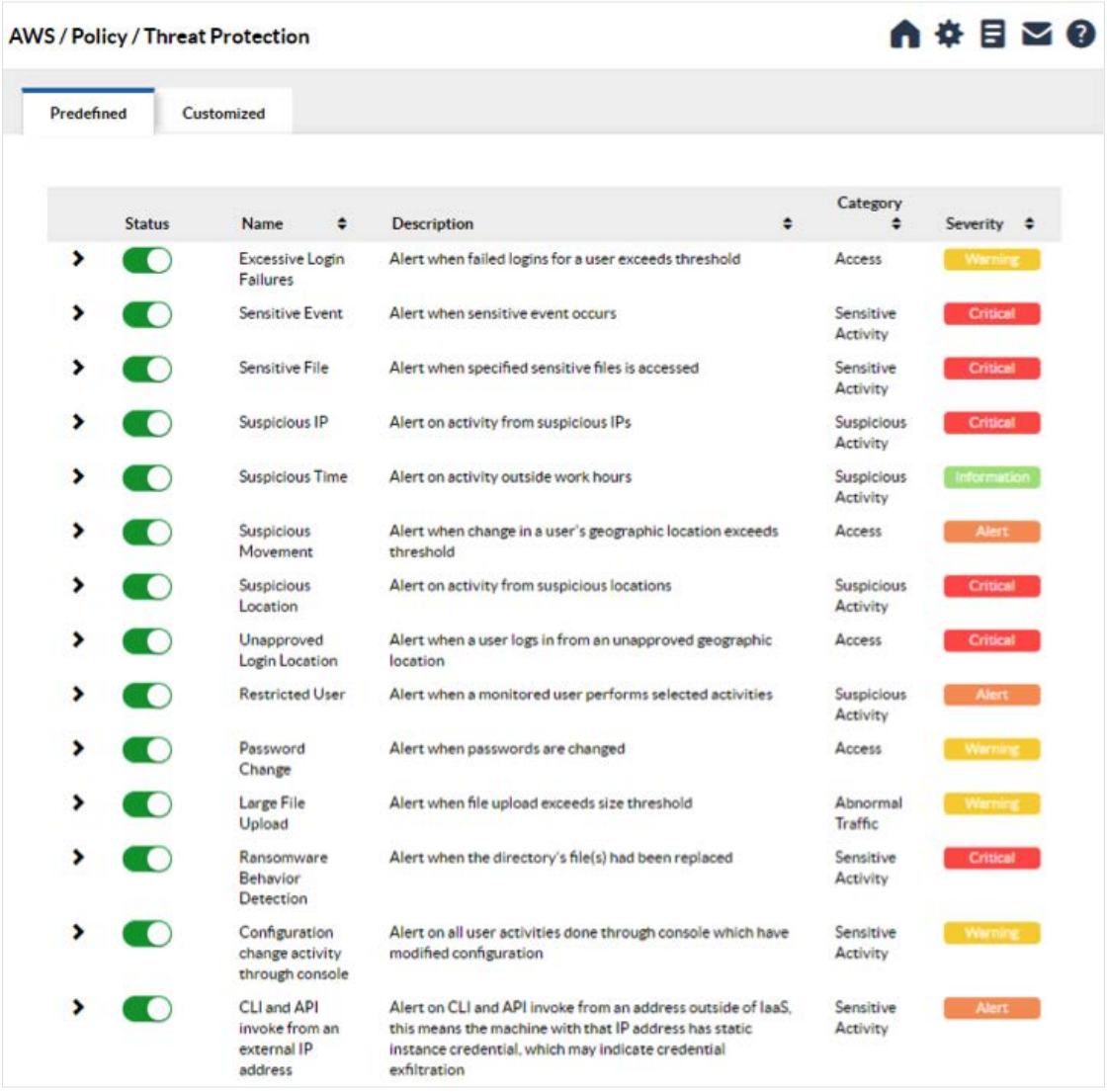

Figure 2: Predefined policies targeting the most common misconfigurations are available in FortiCWP.

FortiCWP allows for configuring custom threat policies that relate to the specific behavior of an organization and the cloud operational model. The threat policies can be defined based on severity, offer a wizard that helps define custom policies triggered by custom content associated with custom activity, and can then be invoking custom notifications including AWS SNS/SQS messages that can potentially trigger automatic remediation routines.

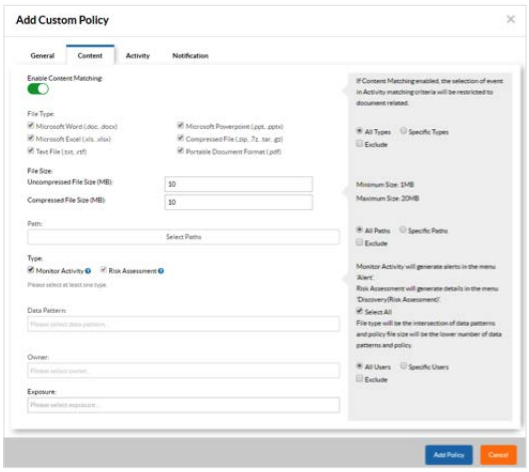

Figure 3: Security administrators can configure custom threat policies in the FortiCWP console.

To truly detect complex threats in public cloud environments, centralized visibility with comprehensive behavior and configuration-based policies are necessary. Threat intelligence also needs to be leveraged in real time for threat detection and prevention, regardless of which cloud the threat targeted. In cloud environments, suspicious activity and compromised accounts need to be blocked throughout. Threat intelligence powered by advanced artificial intelligence (AI) and machine learning (ML) methodologies such as indicators of compromise (IOCs) from FortiGuard Labs helps identify and prevent the propagation of new threats.

Centralized Multi-cloud Threat Visibility and Response

FortiCWP, a Fortinet-developed cloud security management product, mitigates these challenges by providing:

- **Continuous and centralized security monitoring** of security elements such as configurations, user activity, traffic flow logs, and data storage in public cloud environments.
- **Out-of-the-box, predefined threat policies** that identify potential threats such as malicious traffic, suspicious user activity, and vulnerable configurations. The policies are a force multiplier for security teams, given a global shortage of cybersecurity professionals and the breadth of cloud infrastructures being used.
- **Custom policies** are leveraged to best suit the unique organization's needs. FortiCWP delivers policies that are customizable based on relevant organizational needs, risk tolerance, and potential threats an organization is facing.
- **Faster investigations** due to alerts and detailed data analysis with full contextual details that shorten time to resolution.

Leveraging Global Threat Intelligence

FortiCWP receives live updates from FortiGuard Labs, which is staffed with 200-plus researchers working to provide real-time protection against advanced threats.[2] This award-winning team combs through a constant stream of data from 4.4 million sensors and hardware deployed around the world. The network combines original research from strategic global security agencies, key technology partners, and cybersecurity alliances. All this information is fed back into FortiCWP, providing up-to-the-minute protection from zero-day threats, botnets, viruses, and other malicious exploits. FortiGuard Labs databases used by FortiCWP include:

Zero-day exploits. More than 680 zero-day exploits have been identified and profiled by FortiGuard Labs researchers to date. Integration of FortiCWP with FortiSandbox, which is available in multiple form factors, provides additional protection from zero-day threats.

Live updates from FortiGuard Labs are powered by a constant stream of data feed from 4.4 million sensors and hardware deployed globally.

IOCs. FortiCWP also monitors for IOCs extracted from analyzing half a million malware samples on a daily basis. ML techniques capture malicious IP addresses, domains, and URLs.

Botnet IP data. FortiGuard Labs uses aggregated botnet data to block 32,000 botnet command and control attempts every minute of every day.

DevOps exploit data. FortiCWP identifies suspicious DevOps activity or possible compromised accounts and alerts DevOps and security teams via email or notifications generated by services such as AWS Simple Queue Service (SQS) and Simple Notification Service (SNS).

Spotlight Threats in the Cloud

FortiCWP safeguards the business advantages of a multi-cloud environment by addressing threats effectively and quickly via centralized visibility, insight, and threat protection. To recap, FortiCWP provides critical protection advantages, including:

- Monitoring of ongoing cloud operations, configuration changes, and overall activity
- Correlation of data to identify nefarious and dangerous activity
- Predefined threat prevention and detection policies to address common cloud threats
- Customized threat prevention policies
- Faster investigation of threats and suspicious activity

[1] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.

[2] "FortiGuard Labs," Fortinet, accessed March 15, 2019.

September 21, 2019 8:08 AM

377322-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiCWP threat detection\sb-FA-forticwp-threat-detection-and-response\sb-FA-forticwp-threat-detection-and-response