

PROTECTING LINUX WITH THE FALCON PLATFORM

Falcon unifies the technologies required to protect workloads across all environments

ONE PLATFORM FOR ALL LINUX WORKLOADS

Linux is one of the primary operating systems for a majority of business-critical applications, making Linux servers a frequent attack target. Since Linux servers can be found on-premises or in private or public clouds, protecting them requires a solution that provides runtime protection and visibility for all Linux hosts, regardless of location.

The CrowdStrike Falcon® platform simply and effectively protects Linux workloads, including containers, running in all environments, from public and private clouds to on-premises and hybrid data centers.

KEY BENEFITS

Provides integrated container protection

Defends Linux hosts and containers against active attacks

Enables end-to-end visibility with endpoint detection and response (EDR) for Linux and containers

Reduces complexity by providing consistent protection across all supported Linux distributions and deployments — physical, virtual, cloud and containers

Identifies Linux containers running in your environment, including those running with potentially risky configurations

Enables and accelerates threat hunting and investigation

KEY CAPABILITIES

PREVENTION

- The CrowdStrike® Falcon platform combines protection technologies including machine learning (ML), artificial intelligence (AI), behavior-based indicators of attack (IOAs) and custom hash blocking to defend Linux workloads against malware and sophisticated threats:
 - **ML and AI** prevent known and unknown malware, including those running within containers, without requiring scanning or signatures
 - **On-sensor ML** protects devices while in an offline state
 - **Behavior-based IOAs** block suspicious processes and prevent sophisticated fileless and malware-free attacks
 - **Custom IOAs** enable you to define unique behaviors to detect and block
 - **Hash prevention** allows you to define your own blacklist
- Integrated threat intelligence delivers the complete context of an attack, including attribution
- Managed threat hunting 24/7 ensures that stealthy attacks don't go undetected and that breaches are stopped

INTELLIGENT EDR

The CrowdStrike Falcon platform's intelligent EDR:

- Continuously monitors events to provide visibility into Linux workload activities, including activities running inside containers; a full set of enriched data and event details allows investigations against ephemeral and decommissioned workloads
- Captures unique network events for Linux to identify processes that are making network connections, the protocol used, and local and remote server details and count showing the number of connections made in the last hour — with events recalled for up to 90 days
- Provides unified visibility across all workloads, enabling detection and investigation of attacks that span multiple workload types and cloud environments
- Includes CrowdScore™ Incident Workbench to unravel attacks and improve response time by distilling and correlating security alerts into incidents, automatically triaging, prioritizing and highlighting those that deserve urgent attention
- Provides response capabilities that allow you to contain and investigate compromised workloads
- Accelerates investigation by mapping alerts to the MITRE ATT&CK® framework

FALCON CONTAINER SECURITY

Secures the host and container via a single agent running on the Linux host

Investigates container incidents easily when detections are associated with the specific container and not bundled with the host events

Captures container start, stop, image and runtime information, and all events generated inside the container, even if it only runs for a few seconds

Provides visibility into container footprint — including on-premises and cloud deployments — and shows container usage, including trends, uptime, images used and configuration to identify risky and misconfigured containers

Offers a single management console for host and container security



PROTECTING LINUX WITH THE FALCON PLATFORM

MULTI-CLOUD WORKLOAD DISCOVERY

To provide visibility into the scope and nature of public and hybrid cloud footprints, Falcon:

- Automatically discovers existing cloud workload deployments — without installing an agent — by enumerating existing Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances, Google Cloud Platform (GCP) Compute Engine instances and Microsoft Azure virtual machines
- Provides real-time information about Linux workloads, including context-rich metadata about system size and configuration, networking, and security group information for AWS, GCP and Azure
- Identifies Linux workloads that are not protected by the Falcon platform
- Offers insight into your cloud footprint so you can secure all workloads, uncover and mitigate risks, and reduce the attack surface

SIMPLICITY AND PERFORMANCE

- CrowdStrike's cloud-native platform eliminates complexity and simplifies security operations to drive down operational cost
- It operates without the need for constant signature updates, on-premises management infrastructure or complex integrations
- Installation and day-to-day operations bear zero impact on hosts — even when analyzing, searching and investigating
- Falcon enables proactive threat hunting across all workloads and systems from the same console
- It deploys and is operational in minutes

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Learn more at www.crowdstrike.com

© 2021 CrowdStrike, Inc. All rights reserved.

FALCON PROVIDES BROAD SUPPORT

CrowdStrike Falcon provides comprehensive protection coverage that can be deployed across Linux distributions (Amazon Linux including AWS Graviton processors, Red Hat, CentOS, Oracle, SUSE, Debian and Ubuntu). It is compatible with all public clouds — AWS, GCP and Microsoft Azure.

Broad container support includes Open Container Initiative (OCI)-based containers such as Docker and Kubernetes and also self-managed and hosted orchestration platforms such as GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) and OpenShift.

