CROWDSTRIKE

CROWDSTRIKE FALCON - SECURING THE MODERN DATA CENTER

THE NEXT-GENERATION SOLUTION FOR PHYSICAL, VIRTUAL AND CLOUD DATA CENTER PROTECTION

With the advent of virtualization and cloud technologies came the opportunity to store, process and distribute vast quantities of data at the push of a button. Now, a combination of on-premises, virtual, and public cloud data center solutions provide a dynamic environment that poses additional and unique security problems. Your high-value data is spread across an increasingly disparate environment that is susceptible to both commodity and advanced attacks. Scaling physical, virtual and cloud environments can significantly impact protection, visibility, and performance, adding to the underlying issues that teams are dealing with in managing and maintaining their current data center environments. What is needed is an approach that remedies the problems of today, while addressing the future needs of the data center.

The **CrowdStrike Falcon**® platform provides a cloud-native, next-generation approach that includes threat prevention, detection, response, and managed hunting, ideally integrated to protect the modern data center. CrowdStrike Falcon provides turn-key protection for maximum data center protection — whether physical, virtual or cloud-based.

CHALLENGES IN PROTECTING THE MODERN DATA CENTER

VISIBILITY

You can't manage what you can't see. Many companies that move to the cloud, still maintain a legacy approach to security. The Enterprise Strategy Group reports that 92 percent of organizations employ existing security technologies and processes to tackle tomorrow's security threats. This results in organizations deploying a variety of sometimes competing and conflicting agents when trying to protect the systems used in their data centers.

KEY ADVANTAGES

DEPLOYS IN MINUTES BECAUSE FALCON IS A SAAS SOLUTION

OFFERS ONE LIGHTWEIGHT AGENT FOR LINUX AND macOS

OPERATES ON PHYSICAL, VIRTUAL, AND CLOUD DATA ENVIRONMENTS

PROVIDES A SINGLE INTEGRATED MANAGEMENT CONSOLE OFFERING COMPLETE VISIBILITY

DELIVERS UNRIVALED THREAT PROTECTION WITH UNIFIED NEXT-GEN AV, EDR AND MANAGED HUNTING

> "We always look for highly effective solutions that align to our enterprise security ecosystem and cyber defense strategy. CrowdStrike exceeded our expectations. They enabled ADP's Cyber and IT organizations to consistently manage and better protect our data center platforms around the globe while also leveraging our existing investments and resources through innovative technology and advanced API capabilities."
>
> — ROLAND CLOUTIER, CSO ADP

PERFORMANCE IMPACT

Security solutions should not affect your business-critical servers. However, the majority of security products on the market today cause reduced performance and outages in the modern data center. This halts productivity, while driving up costs for organizations looking to streamline their efficiency via the cloud.

DEPLOYMENT DIFFICULTY

Legacy AV solutions exist on-premises and are difficult to deploy to your cloud and hybrid-cloud data centers. Either ports must be opened in firewalls to establish trust between your on-premises security infrastructure and servers in a remote data center, or multiple agents must be deployed in order to satisfy your security requirements. Typically, legacy AV solutions include hardware and software solutions that can take weeks or months to integrate and operationalize. This architecture is cumbersome, resulting in a protracted time-to-value.

SERVERS FACE UNIQUE THREAT TYPES

Your internet-facing servers are vulnerable and adversaries know this. 24/7 exposure to the public internet makes them target beachheads. Internet-facing mass scans gives adversaries a wealth of attack patterns ranging in complexity and better security is required to address these threats.

CROWDSTRIKE FALCON: COMPLETE SECURITY COVERAGE FOR ALL DATA CENTER TYPES

The CrowdStrike Falcon® platform provides the balance needed for today's data centers with unrivaled protection that includes best-in-class prevention, detection and response capabilities. In addition, its cloud-native architecture enables the speed, flexibility, manageability and scalability that IT operations expect from a modern data center.

MAXIMUM SECURITY WITH MINIMAL IMPACT

The lightweight Falcon agent provides a simple, yet comprehensive solution to complex security problems without slowing down your data center's performance. Legacy security solutions bog down server performance with unscheduled reboots, updates and "scan storms" that can cause outages, leading to system downtime and frustration. In extreme cases additional servers were needed to address performance issues, driving up operating costs. At 20 MB and using only

BENEFITS AND BUSINESS VALUE

SCALE AND CONTROL YOUR ENVIRONMENT

Falcon allows you to control and scale your data center environment without sacrificing visibility or protection policy application. The Falcon platform provides cloud-delivered protection, so that as your data center grows and evolves, there is no need for additional controllers or servers to "control your servers." Regardless of whether a server is deployed outside the corporate firewall or network, or whether it is physical, virtualized or cloud-based, Falcon provides complete visibility into your data center from one console. In addition, you can manage user access to the Falcon platform to ensure that accurate permissions and authorizations are assigned. Falcon enables complete flexibility for how protection policies are applied at an individual server, group or data center level.

MAINTAIN SYSTEM PERFORMANCE, VISIBILITY AND PROTECTION ACROSS ALL ENVIRONMENTS

Falcon endpoint protection updates eliminate reboots and prevent system downtime with customer-facing systems. The cloud-native architecture eliminates invasive updates, and new functionality can be added in the cloud without having to take resources from or disrupt servers in your data center. Falcon is signatureless, so data centers never incur disruption or performance impact from having to deploy signatures updates on a daily or hourly basis. Falcon's machine learning and pre-execution prevention completely eliminate the need for AV scans that cause performance degradation on data center servers.

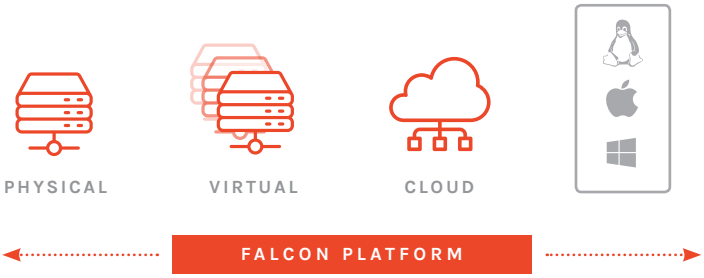
PROTECT YOUR ENTIRE DATA CENTER

CrowdStrike Falcon provides comprehensive protection coverage that can be deployed across Windows, Linux and macOS and is compatible with AWS, Azure, and Google Cloud. In addition, Falcon works with any hypervisor, including V-sphere, Hyper, etc. Behavioral analysis enables Falcon to determine indicators of attack (IOAs), preventing today's stealthiest and most sophisticated attacks. IOAs focus on the unique attacks that internet-facing servers experience, stopping web and SQL shell attacks that evade legacy

one percent CPU, the Falcon agent's minimal system footprint eliminates this problem.

DEPLOY AND SCALE IN MINUTES

Deploying the Falcon agent to the servers in your data center is effortless, taking only seconds to install, and with no reboot, it is up and operational immediately. Because Falcon is delivered as a SaaS platform, there is no complex security infrastructure to add or manage.



SEAMLESSLY PROTECTS ALL DATA CENTER ENVIRONMENTS

The Falcon agent can be deployed across all data center types to protect your heterogeneous environment. The agent sits at the kernel level across your on-premises, virtual, and cloud data centers. It seamlessly spans across cloud platforms, including Amazon AWS, Google Cloud Platform and Microsoft Azure. CrowdStrike also supports hypervisors such as Vsphere and Hyper and protects your virtual data center.

COMPLETE VISIBILITY

The Falcon management console provides a unified view across all the servers in your data center, whether they are physical, virtual or cloud-based, allowing you to search across your environment and data at the touch of a button. This means that if you want to search for an IOC and need 100,000 endpoints over a six-month period, or 60 days or even one day, Falcon can return your request in five seconds. Protection policies are set and controlled from the console and role-based access control (RBAC) ensures a further level of control and coordination.

BETTER PROTECTION

Your internet-facing servers are constantly under attack. CrowdStrike provides protection against all attack types, from commodity, opportunistic attacks to those that are highly-targeted and sophisticated. The Falcon platform provides protection against the threats that standard AV and application whitelisting miss by covering the entire attack kill-chain, effectively stopping the mega-breach.

security. Falcon OverWatch™ 24/7 managed threat hunting provides an additional layer of oversight and analysis to ensure that threats don't get missed and ultimately to prevent the data center from being breached.

MONITOR YOUR LINUX SERVERS

Linux servers are often high value because they host business-critical applications. However, the protection available for those servers is far behind the security coverage offered for other operating systems. CrowdStrike provides the visibility necessary to monitor activities on Linux servers in real time and detect attacks before they cause irreparable damage.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. The CrowdStrike Falcon platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from day one. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator of attack (IOA) based threat prevention to stop known and unknown threats in real-time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 40 billion security events from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches. Learn more: **www.crowdstrike.com**