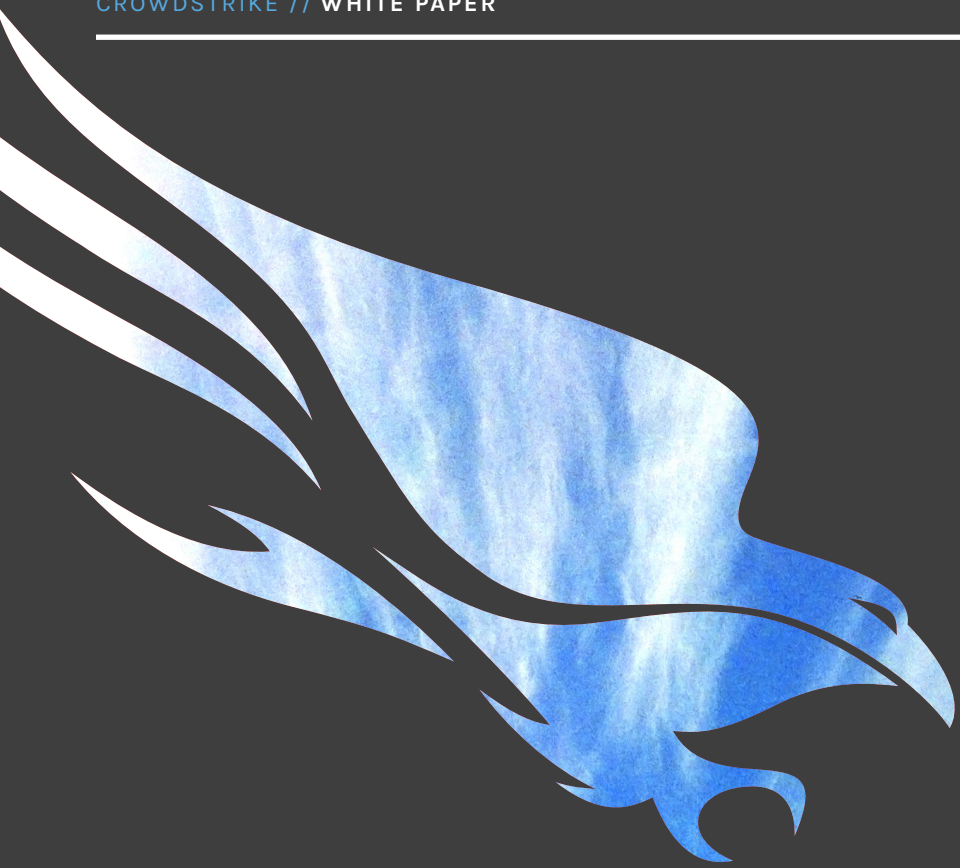

5 REASONS ENDPOINT SECURITY MUST **MOVE TO THE CLOUD**

The radical shift in the scale and economics of cybercrime calls for an equally radical change in how IT protects user systems. Whether it is from phishing attempts, drive-by-downloads, or malware-free intrusion techniques, endpoints are usually at the spear tip of assaults on enterprise networks.

As things stand, the Cloud is already completely revolutionizing the way the rest of IT systems are delivered. Software as a Service (SaaS) tools are making it possible for information workers to share and create documents more effectively than ever, and the ease of use is taking the enterprise by storm. Take collaborative SaaS service Box, for example, which in just a few short years has managed to gain 50 percent of the Fortune 500 as customers. Meanwhile, Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Cloud

offerings are making it possible for developers and operations teams to scale and quickly configure IT environments to satisfy the most immediate IT needs without overbuying compute and storage infrastructure.

According to a recent Harvard Business Review report, 84 percent of enterprises have increased their Cloud usage in the past year. Fueling this major business migration to the Cloud are the well-documented cost savings, integration, visibility and scalability inherent in Cloud architecture.

With the kind of IT makeover Cloud has enabled elsewhere, it only makes sense that this delivery model will also transform the way we protect the enterprise. Here's why Cloud makes it possible for security teams to regain control over endpoints.

#1

KEEP TABS ON AND LEARN FROM ADVERSARIES AS THEY TEST ATTACK STRATEGIES

Before we even get to the obvious Cloud benefits of agility, elasticity and affordability, let's talk about the elephant in the room. Today's attackers are working with some seriously deep pockets.

The most prolific and effective attacks today are bankrolled either by nation-states seeking to gain information to fuel their commercial and political interests, or by well-funded and organized criminal groups that have made an art of making money from cybercrime. In both cases, these adversaries are putting their money where their mouths are and investing in the future success of their attacks.

In order to ensure they take the right tack, these attackers are buying up traditional security system software, network boxes and any other on-premises solutions they can get their hands on to figure out how they tick. By recreating mock networks and endpoint protection systems of victims they're seeking to target, they find all the ways they can bypass these technologies. These adversaries are able to run dozens or hundreds of mock attacks in their labs without anyone knowing what they're doing. From there, that information turns into a blueprint to execute attacks in the real world.

Fundamentally, every single on-premise technology will fail in response to that type of attack, because if someone has unlimited time and resources to find a vulnerability, chances are that they will ultimately find it.

The Cloud disrupts this attack model. With a Cloud security solution the adversaries may be able to acquire the endpoint sensor software, but when they install it in the lab and run mock attacks, the security provider can see every single attack. It's possible, then, to observe the attackers' tactics before they're ever launched in the wild. The first time they run an attack, it's recorded, analyzed and shared with sensors on every defenders' machine, preventing that attack from being used again.

In this way the Cloud model changes the fundamental offensive-defensive asymmetry and flips the advantage from the attackers to the defenders.

#2
EVERY ATTACK FEEDS INTO NEW DEFENSES FOR ALL

Perhaps more important than stopping adversaries from endless experiments, Cloud architecture provides the ability to record and learn from new attacks, effectively crowdsourcing intelligence about attack techniques across the entire kill chain on a massive scale and in real time.

Everyone benefits from contributing to the Cloud – except the attacker. The more information and data fed into a Cloud security system, the better insight it provides. This ultimately yields better security for every community member. If one organization is being attacked, intel derived from the attack can be quickly and effectively shared to protect every endpoint across the community.

Some traditional on-premise endpoint security providers may argue that they already take advantage of Cloud benefits by having their software send intelligence to their own internal Cloud repositories. However, this is a flawed and limited approach that does not come close to taking full advantage of the Cloud. In a native Cloud solution, it is possible to do much more than simply store signature-based threat information in the Cloud. While this may improve the efficacy of reacting to known threats and malware, it does not utilize the Cloud's ability to support real-time, behavioral analysis and response to address previously unknown threats.

With conventional defenses, even when attackers are unsuccessful, they learn from the process. For example, attacks are typically carried out in multiple stages. An attacker can determine at what point their attack was detected, and adapt their methods to circumvent the detection, reusing the undetected steps that got them to that point. Having full visibility into the endpoint via Cloud architecture allows analysis of each stage of the attack, not just the point at which a signature was available and could trigger a detection. Using an adaptive security model, defenses can be created in real-time to counter each stage of the attack, forcing adversaries back to the drawing board. This ability enabled by the Cloud to see events across the kill-change, in context and in real-time, moves the advantage back to the defender.

#3 SAFEGUARD SENSITIVE CUSTOMER INFORMATION AT ALL COSTS

Let's face it—the prospect of crowdsourced security data scares the average infosec professional. It is the data being collected and the manner in which stored that should be of greatest concern.

The next generation of Cloud endpoint security must limit data collection to just the bare essentials for delivering effective protection. This means transmitting and storing only endpoint activity meta data (such as process start/stop times, network connection activity, etc.) and, to the extent possible, ignoring potentially sensitive data residing on the endpoint.

In addition, providers of Cloud-based security solution should be held to the highest standards for security, availability, processing integrity, confidentiality and privacy. By adhering to SOC2 compliance requirements, these providers can address any concerns and allay any fears.

In addition a Cloud security provider, by rights, must provide a robust multi-tenant environment that isolates information gleaned from each customer while still maintaining the privacy of attack data affecting those customers.

#4
PROTECTION ON OR OFF THE NETWORK

In today's BYOD mobile workforce, users are frequently working from home and on the road. Few people are behind the VPN 24/7 anymore. But most on-premise solutions are unable to accommodate that not-so-new fact of life because the management console itself is behind the VPN. The endpoint software that organizations have installed on devices has to connect to the management console via the VPN to work, making it unsuitable for supporting today's road warrior workforce.

By contrast, endpoint security delivered through the Cloud makes it possible to manage remote assets as easily as those on the network, and relieves the enterprise from having to protect the console or worry about details like the database overflowing. The Cloud provider takes care of the details.

#5 THE PRACTICAL SIDE OF THE CLOUD

The reason Cloud architecture has replaced on-premise solutions in so many areas of the enterprise is driven largely by the ubiquity, simplicity and scalability inherent in this emerging compute model. Examples of how these advantages are manifested in a Cloud security offering include enhanced manageability, unlimited scalability, and the capability of protecting assets on or off the network.

For instance, consider the upgrade process with a traditional solution versus a Cloud-based platform. With the on-premise endpoint security model, update cycles are slow to come from the vendor and painful for the enterprise. Today, major antivirus vendors are subject to an extremely laborious process for creating updates, which can last from six to 12 months as they develop and test classifiers. Once this arduous process is completed, there are typically additional delays as the client upgrades to the new release. As the months tick by, the attackers are refining techniques daily. The result is that every update is months out-of-date from the get-go.

Conversely, a Cloud security provider can update machine learning in the Cloud itself. The most updated version of protection is always available on-the-fly and algorithms are adjusted constantly. Even better, enterprises can get off the upgrade treadmill and eliminate the time-consuming update process entirely.

Incident response is another area where Cloud presents distinct advantages. In the event that an intrusion does occur, on-premise solutions tend to require a delay of at least several days to respond, as vendors must ship controllers to customer sites. When dealing with moving physical equipment and technicians to interact with it, there are many types of mishaps that can hold up the process. The culmination of the situation tilts the advantage to the attackers, as it takes that much longer to contain an incident and mitigate risks.

With a Cloud endpoint solution, it is possible to get remote incident responders the right information immediately. No need for shipping equipment or booking flights. Instead, the analysts can start work right away and respond much more swiftly when time is of the essence.

Scalability represents an additional advantage to Cloud architecture. On-premise endpoint security solutions have a difficult time scaling to meet increases in node counts and attack volume. Consider large government organizations that may have millions of nodes to contend with, and potentially hundreds of servers to manage them. This kind of infrastructure grows very complex very quickly and lends itself to management silos.

Cloud architecture makes it possible to keep information aggregated without the same on-premise solution problems. Information is centralized and access controls make it possible to ensure only the right people can see the data they need to get their job done. Everything scales dynamically so that an organization always pays only for the security firepower that it needs, without ever feeling that it has outgrown the solution. The cost savings alone can often justify the move from an on-premise solution to the Cloud.

CROWDSTRIKE'S **CLOUD ADVANTAGE**

CrowdStrike's founders saw that traditional cybersecurity systems were no longer effective against sophisticated adversaries and attacks, and unable to protect organizations against sustained breaches. A new approach and architecture was needed to provide real-time visibility and protection of endpoints on a continuous basis -- not simply at a single point in time. The new architecture also needed to unburden the endpoint to provide greater end-user productivity, allow for storage and ongoing analysis of a massive and growing data set in real time, while creating a means of crowdsourcing information across a vast user community, and fortifying it with the best threat intelligence and incident response capabilities available.

The obvious answer was to create a new security architecture based entirely on the Cloud.

Moving to the Cloud provided CrowdStrike with a number of distinct advantages over conventional on-premise defense architectures, including:

CONTINUOUS REAL-TIME DETECTION, PREVENTION AND RESPONSE.
What enterprise organizations want is fast and unobstructed visibility across all their endpoints, allowing them to continuously detect and prevent sophisticated attacks in real time and block persistent adversaries from compromising their environments and stealing data. CrowdStrike has harnessed the Cloud to deliver these powerful capabilities via an intelligent lightweight sensor at the endpoint, working in concert with a potent and scalable Cloud-based backend. As a result, organizations finally have the ability to get ahead of adversary activity, and stay ahead.

Recent data collected by CrowdStrike's Incident Response Services team indicates that on average, adversaries targeting specific organizations attempt to reinfect the networks within two days of initial remediation. This underscores the requirement for continuous prevention and protection against advanced persistent threats. This level of integrated end-to-end, around-the-clock detection, prevention and response -- delivered in real-time via a single unified platform and all-in-one user interface -- is made possible by CrowdStrike Falcon next-generation endpoint security platform, which was engineered specifically to take advantage of scalable Cloud-based architecture.

CROWDSTRIKE'S CLOUD ADVANTAGE (CONT'D)

THE ABILITY TO SUSTAIN A MASSIVE THREAT GRAPH IN THE CLOUD -- and conceal it from bad actors. The CrowdStrike Cloud analyzes incoming real-time data on a massive scale, crowdsourcing billions of endpoint events as they occur across the global CrowdStrike community. This stream of real-time threat information drives CrowdStrike's organic Threat Graph, dynamically scrutinizing event-based data to detect anomalous behavior based on Indicators of Attack (IOAs). Unlike systems that rely solely on Indicators of Compromise (IOCs), which appear only after a breach has already occurred, IOAs are effective regardless of whether malware is present. This allows customers to detect and prevent attacks while they are still in progress, before data is exfiltrated. By analyzing all this data at scale in its Threat Graph, CrowdStrike keeps its threat intelligence and processes safe from the prying eyes of potential attackers, unlike traditional on-premise architectures which are easily obtained by adversaries to exploit weaknesses.

DEVELOPMENT OF A LIGHTWEIGHT SENSOR - FINALLY, DELIVERING THE PROMISE OF SPEED AND POWER TO THE ENDPOINT. CrowdStrike engineers knew that the last thing security and IT teams wanted was to deploy another heavyweight client to the endpoint. The new architecture allowed them to spread the load between the client and the Cloud – with the Cloud taking on the heavy lifting, as needed, in the background. The resulting endpoint client is both nimble and discreet -- and at the same time, powerful enough to offer detection and prevention directly at the endpoint level. This singular ability to provide customers with both detection and prevention capabilities via an integrated Cloud and sensor model is unique to CrowdStrike.

CrowdStrike's sensor provides superior monitoring and reporting capabilities, transmitting event-related data to the Cloud in real time, and its clever design accomplishes all this without burdening the endpoint or disrupting the end user. CrowdStrike's unique lightweight sensor and Cloud architecture ensures complete and detailed oversight of everything that is happening on the endpoints in real time, and offers sustained vigilance over long periods of time. In this way, the system instantly identifies threats that conventional platforms can't see, and provides a complete and searchable forensic record of endpoint events as they occur, at any point in time. The lightweight sensor also is highly scalable, and when needed, can be deployed to hundreds of thousands of endpoints in a matter of hours, not days, weeks or months.

ENABLE INTEGRATION ACROSS ENDPOINT SECURITY, INTELLIGENCE-GATHERING AND INCIDENT RESPONSE (IR) CAPABILITIES. Key in CrowdStrike's new approach to endpoint security was the need to share data, insights and experience across its technology platform and in-house threat intelligence and IR teams. The Cloud enables the seamless aggregation, sharing and operationalization of this information to ultimately provide CrowdStrike's 'continuous response' to today's sophisticated and sustained attacks, while providing remediation capabilities in hours and days, not weeks or months.

LEVERAGE THE 'POWER OF THE CROWD'. Another unique value of CrowdStrike bringing security to the Cloud is the `community immunity' that the model affords, where endpoints around the globe are contributing to a shared knowledge base of real-time threat information. This approach provides complete oversight

CROWDSTRIKE'S CLOUD ADVANTAGE (CONT'D)

for all endpoints and in doing so, gives the attackers no place to hide. And while aggregated threat intelligence feeds into constant security refinements, CrowdStrike never accesses or stores sensitive customer data. All of this adds up to an intelligent and safe security Cloud, correlating billions of events and petabytes of data in real time without ever putting customer data at risk.

ELIMINATION OF UPDATING AND MAINTENANCE CYCLES. The Cloud allows simultaneously, eliminating the need to patch and maintain on-premise software and hardware. This dramatically simplifies and improves the ability to always address the latest threats and stay ahead of the adversary, while reducing management overhead, cost and security resources required by customers.

HARNESS THE CLOUD'S INHERENT SCALABILITY AND COST-EFFECTIVENESS. CrowdStrike's scalable Cloud architecture flexes with the demands of customers and provides enormous storage and compute power to drive real-time protection at lower cost. Additional resources can be provisioned as needed by simply scaling-up in the Cloud. This relieves the customer from the responsibility, cost and potential redundancy of having to plan, prepare and provision hardware and software to keep pace with changes within their business and with the unpredictable threat landscape.

IN SUMMARY

As organizations grow and become more distributed, adding more endpoints across the enterprise, they provide an increasingly broad attack surface for sophisticated adversaries targeting their data and IT infrastructure. The success of such attacks has been well documented in recent years, showing the inherent vulnerabilities in conventional on-premise, network- and malware-centric defenses.

The Cloud offers a new means of providing pervasive protection throughout the enterprise – securing data, people and assets, both on-premise and off – and it can do so with lower cost and reduced management overhead while offering significantly increased performance, agility and scalability. In addition, the real-time and highly scalable nature of the Cloud model lends itself to creating community immunity by crowdsourcing information about evolving threats and supporting large-scale data models that can recognize and prevent attempted intrusions before they succeed. Finally, Cloud-based solutions can be constructed that maintain the highest levels of data privacy and security, while at the same time, preventing adversaries from obtaining and reverse-engineering the technology and processes used to keep them out.

As informed security teams investigate more effective alternatives for protecting their organization's networks and end users without impeding business operations or hindering productivity, they must inevitably turn to the next generation of native Cloud security solutions for the answer.

ABOUT CROWDSTRIKE

CrowdStrike™ is a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services. CrowdStrike Falcon is the first true Software as a Service (SaaS) based platform for next-generation endpoint protection that detects, prevents, and responds to attacks, at any stage - even malware-free intrusions. Falcon's patented lightweight endpoint sensor can be deployed to over 100,000 endpoints in hours providing visibility into billions of events in real-time. CrowdStrike operates on a highly scalable subscription-based business model that allows customers the flexibility to use CrowdStrike-as-a-Service to multiply their security team's effectiveness and expertise with 24/7 endpoint visibility, monitoring, and response.

REQUEST A DEMO OF CROWDSTRIKE FALCON

Learn how to detect, prevent, and respond to attacks at any stage - even malware-free intrusions.
www.crowdstrike.com/request-a-demo

AUTHORED BY DAVE COLE,
CHIEF PRODUCT OFFICER OF CROWDSTRIKE

CROWDSTRIKE | 15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618

WWW.CROWDSTRIKE.COM | @CROWSTRIKE