CLOUD-NATIVE CYBER DEFENSE

Securing the Future of Work
At the start of the COVID-19 pandemic, many organizations switched to remote work, believing that they would go back to the office in a few months. As the pandemic persists, organizations increasingly realize that work from home (WFH) or hybrid work policies where employees choose whether to telecommute or go to the office are likely to be the new normal for some time to come. Workers who can no longer collaborate in person are increasingly being directed to use cloud-based collaboration platforms and mobile-chat channels so they can work remotely with co-workers.

These new work styles have opened up fresh cybersecurity vulnerabilities. Ever opportunistic, criminals are increasingly targeting personal devices used by remote workers, VPN coverage gaps, and collaboration apps, resulting in record numbers of attacks.

This white paper describes how and why cybersecurity must adapt to the changing network attack surface, and how CrowdStrike and SafeGuard Cyber work together to help organizations coordinate their response to threats across all their managed endpoints.
The COVID-19 pandemic is expected to have an ongoing impact on the way companies work in the coming month and beyond. During the pandemic, remote work became the rule rather than the exception. Ongoing safety concerns and the productivity and revenue gains employers have realized from telework have encouraged many organizations to extend WFH or adopt hybrid policies. A recent Gartner survey found that 74% of CFOs and finance leaders plan to move at least 5% of their previously on-site workforce to permanently remote positions post COVID-19. Just a few of the companies embracing WFH or hybrid operations include Fujitsu, Google, Facebook, Amazon, Microsoft, and Twitter.

With employees no longer able to collaborate in person, the shift to remote work has accelerated the adoption of cloud-based collaboration platforms and mobile-chat channels, such as Slack, Zoom, Microsoft Teams, WhatsApp, LinkedIn, and We Chat. For example, Microsoft reported that over the first months of the pandemic, Teams usage grew from 44 million to more than 75 million daily active users. Organizations are using these technologies for remote meetings and to make online collaboration more seamless and cohesive.
Organizations have traditionally employed VPNs to secure access for remote workers to corporate data/apps located on-premises or in online collaboration apps. Yet, VPNs may not be available for everyone, leaving some employees to use their home networks for corporate access. If they do have a VPN, it might not be set up properly. Or, employees may forget to use it every time due to the stress of working from home with kids under foot.

The work space has also shifted, with working norms in flux. Employees may respond to requests away from home or while connected to public wifi networks.

These remote workers often rely on personal devices, home networks with legacy routers, and IoT devices to obtain corporate resources. These devices and networks simply don’t have the same security as company-owned devices inside the firewall. Yet most organizations’ security architectures are designed for on-premises users and data centers.

At the same time, while cloud-based collaboration tools were once relatively safe environments, criminals are paying more attention to these channels now that employees are flocking to them. Because these channels are outside the corporate firewall, they are easier to compromise and the attacks are virtually invisible to security teams. For example: a hacker recently took control of the Twitter accounts of political, corporate, and cultural elites after gaining access to credentials from within Twitter; and a Singaporean PhD student used LinkedIn to lure in Americans to provide insider knowledge to Chinese intelligence agents.

This transformation of the way work is done creates a large attack surface with huge cyber risk exposure for the enterprise.
These vulnerabilities have not gone unnoticed by cybercriminals and nation state actors. Remote workers are highly susceptible to attacks such as spear phishing, account compromise, cyber espionage, and zero-day exploits.

Hackers use these attacks to steal legitimate credentials so they can access the corporate network through the front door. Or they download malware onto the end users’ machines or devices. Either way, cybercriminals then penetrate the enterprise network and move laterally across it, often remaining undetected for long periods. Such attacks can exfiltrate data, infect networks with Ransomware, or provide an avenue for extortion, where attackers threaten to release sensitive exfiltrated data as a backup to ransomware. According to the Global Threat Report 2020, ransomware represented 26% of all eCrime threats reported in 2019. That percentage climbs to 37% of threats when ransomware reports were combined with malware operated by big game hunting adversaries.

As more employees collaborate online, insider threats have become a growing issue as well. A 2020 report by Ponemon Institute found that the frequency of insider incidents spiked 47% since 2018. Insider attacks include malicious threats as well as deliberate or unintended data leakage. For example, employees might send data to their home network or to unsecured printers.

Employee Conduct Can Increase Enterprise Risks
Internal threats can also include employee conduct which results in regulatory compliance and business conduct violations. Employees might make sexist or racist remarks or irresponsible comments on these channels. Unlike in-person meetings where it can be difficult to prove inappropriate behavior, collaboration tools capture these interactions in texts where they can be verified. Companies need to catch these incidents in real-time. This task is daunting due to the volume and velocity of digital communications. One Fortune500 insurance customer with 5,000 employees is producing over 150,000 Slack messages per day since migrating to remote work.

Risks Magnified by Lack of Visibility
Security teams now suffer from a massive visibility problem, exacerbated by the rapid adoption of cloud-based SaaS applications and the physical distribution of physical endpoints. Without a line of sight into these apps and the business communications they contain, it becomes increasingly difficult to respond to threats in real time. Every second counts. Once a malicious attachment or link is opened, security teams are playing catch up. Enhanced visibility enables proactive security and more rapid response times.
WHAT'S NECESSARY IN A SECURITY SOLUTION?

The paradigm shift in the way employees work necessitates changes in the way security is deployed. To secure a remote, distributed workforce that uses cloud apps, organizations must shift from securing on-premises network systems to securing employees where they are physically (distributed around the world) and where they communicate (in the cloud).

Organizations need a cloud native approach to secure the technologies that empower the workforce and allow them to be productive from anywhere. A cloud native approach delivers a number of benefits. It can:

- **Be deployed on any network (on-prem, VPN, WiFi).**
- **Support every workload everywhere—even if they are outside the firewall or offline.**
- **Provide enhanced visibility across an enterprise’s entire digital footprint.**
- **Protect apps on any device (laptop, smartphone, tablet).** For example, if a user is sent a phishing link in LinkedIn, she must be protected whether she accesses the message on the LinkedIn app on her mobile device or in a browser on her laptop.
- **Stop attacks in the cloud or in the app before they can transit to corporate networks with the help of machine learning and risk analytics.**
- **Provide scalability to support the volume and velocity of communications in the cloud, enabling organizations to provision resources as needed to flex up or down with user demand.**
- **Add business value by opening up new channels to business users in a secure and compliant manner.**

HOW CLOUD-NATIVE DEFENSE WORKS

1. **Detect/quarantine IOCs on accounts**
2. **Detect/contain IOCs on endpoints**
3. **Share IOC detections to manage risks from app to endpoint**
4. **Post account and endpoint IOCs to SOC/SIEM**

SOC CORRELATES ACCOUNT/ENDPOINT IOCs

CLOUD-NATIVE CYBER DEFENSE: SECURING THE FUTURE OF WORK | 05
SafeGuard Cyber’s digital risk protection is purpose-built to operate in the cloud as the first line of defense for the remote workforce. SafeGuard Cyber offers:

- **API-based integration directly with digital collaboration, mobile chat and social network apps.**
- **Ability to detect spear-phishing, malware attachments and links (including ransomware), and compliance violations directly in the messaging stream as they are received or posted.**
- **Ability to remediate many cyber threats before they can propagate to managed endpoints.**
- **Ability to provide early visibility to cloud-based attacks that may be targeting corporate networks.**

When users employ cloud-based applications, the SafeGuard Cyber platform monitors these communication sessions in the cloud, no matter what device the user is using. During these sessions, the platform scans for code patterns and behavior indicative of malware, malicious content, high-risk social connections, account impersonations and takeovers, or compliance violations.

Upon identification of suspicious content, it will run it through a static analyzer and then a sandbox as necessary to determine whether it’s malware, and if so, get a threat signature or put zero-day attacks into a sandbox. This stops malicious files before they can transmit from digital accounts to endpoint devices.

CrowdStrike protects all your endpoints in the cloud by detecting malware when it is activated on the endpoint. If someone downloads a malicious macro in a Word Doc, the CrowdStrike Falcon® platform will detect and prevent the macro from running when the user clicks on it.

The CrowdStrike Falcon® architecture is built from the ground up to protect managed endpoints wherever they reside. That means:

- **Employees are protected regardless of what device they’re connecting from or whether that device is located on-premises, in a remote office, or at home.**
- **Workloads can be safeguarded everywhere, even outside the firewall or offline.**
- **Protection scales up and down according to the needs of the customers.**
- **IT has comprehensive visibility into who and what is on the network, regardless of where they’re connected.**
- **Implementation is through a lightweight agent on each device that has minimal impact on device performance and continuously monitors without additional reboots or downtime.**
- **CrowdStrike’s team of security experts performs implementation, management and incident response as a turnkey endpoint security service, including proactive 24/7 managed hunting for adversary activity so that you can detect and block attacks before they wreak havoc on your environment. The result is an instantly optimized security posture without the burden, overhead, and cost of managing a comprehensive endpoint security program.**

SafeGuard Cyber extends the Falcon® platform’s visibility to the messaging level in over 50 social, mobile, and collaboration applications — areas that have traditionally been blind spots for security teams. These include platforms such as Facebook, Twitter, Microsoft Teams, LinkedIn, Slack, and even mobile apps like WhatsApp and WeChat.

CrowdStrike and SafeGuard Cyber work together to help coordinate your response to threats across managed endpoints as they occur.
Increased remote work and online collaboration has forced organizations of all types to contend with growing cybersecurity vulnerabilities and breaches. CrowdStrike and SafeGuard Cyber work together to give you visibility into cyber threats on both your endpoint devices and your cloud-based SaaS applications. Because these solutions are built from the ground up for the cloud, IT has complete visibility into employee endpoints and workloads and can protect any device from any location—on-premises, remote or in the cloud. And you benefit from the cloud advantages of scalability, simplified implementation, and as a service delivery.
CLOUD-NATIVE CYBER DEFENSE: SECURING THE FUTURE OF WORK

Your organization may be using cloud-native apps without your knowledge or may request your assistance in evaluating the security and compliance of communication and collaboration apps outside your network. Either way, your security team’s ability to defend against today’s increasingly sophisticated targeted attacks depends on your visibility and defense strategy. Asking key stakeholders the following questions and working with your CrowdStrike and SafeGuard Cyber Team will help you be ready for secure and compliant growth in any circumstance and on any device.

**ASSESS YOUR ENTERPRISE**

**Ask your CFO, CMO:**
If rules and policies could provide security, compliance & visibility on social, collaboration, & chat applications would you be able to increase productivity without increasing headcount?

**Ask your Chief Compliance Officer or General Counsel:**
Do you want to ensure that data/IP being transmitted in cloud applications not in our control are safe and secure and compliant?

**Ask your CMO & CEO:**
Would the organization benefit from securely enabling the executive team and recruiters to communicate effectively on channels like LinkedIn?

**Ask Marketing & Sales:**
Are your products & services accurately represented on social media and the web? Do you have visibility of malicious intent on the dark web?

**Ask your R&D or CPO:**
How long would it take us to discover IP data leakage was distributed over a private chat or collaboration channel?
SafeGuard Cyber is a Charlottesville, Virginia-based company with a cloud-based platform that empowers organizations to use social media and digital channels securely, compliantly, and at the scale of global business. With coverage across more than 50 channels and its award-winning machine-learning risk analytics engine, SafeGuard Cyber helps security, compliance, and marketing teams work better together to drive business forward. The company’s customers include Global100 enterprises, small businesses, municipalities, and national governments.

Learn more at www.safeguardcyber.com

CrowdStrike® Inc. (Nasdaq: CRWD), 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 over 3 trillion endpoint-related events per week 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.