wickr

Security Operations and Collaboration Platform

www.wickr.com | support@wickr.com

Copyright © 2019 Wickr Inc

Table of Contents

Introduction

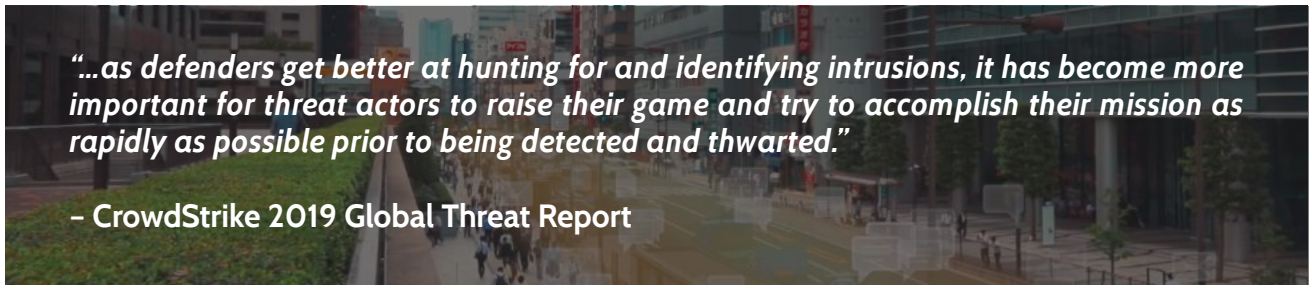
Wickr has been deployed at some of the most security-conscious organizations in the world. For global organizations, information security is not only important, it is paramount to continued business operations. To best protect against dedicated and opportunistic adversaries, organizations must approach security technology as an investment that reduces business risk and enables productivity.

The recent CrowdStrike 2019 Global Threat Report further confirms that sophisticated attackers perform lateral movement quickly once they find a crack in your perimeter. Unless quickly challenged by network defenders, adversaries secure their beachhead by performing the following:

1. **Removing logs and performing anti-forensics;**

2. **Subverting security tooling and enabling long-term access.**

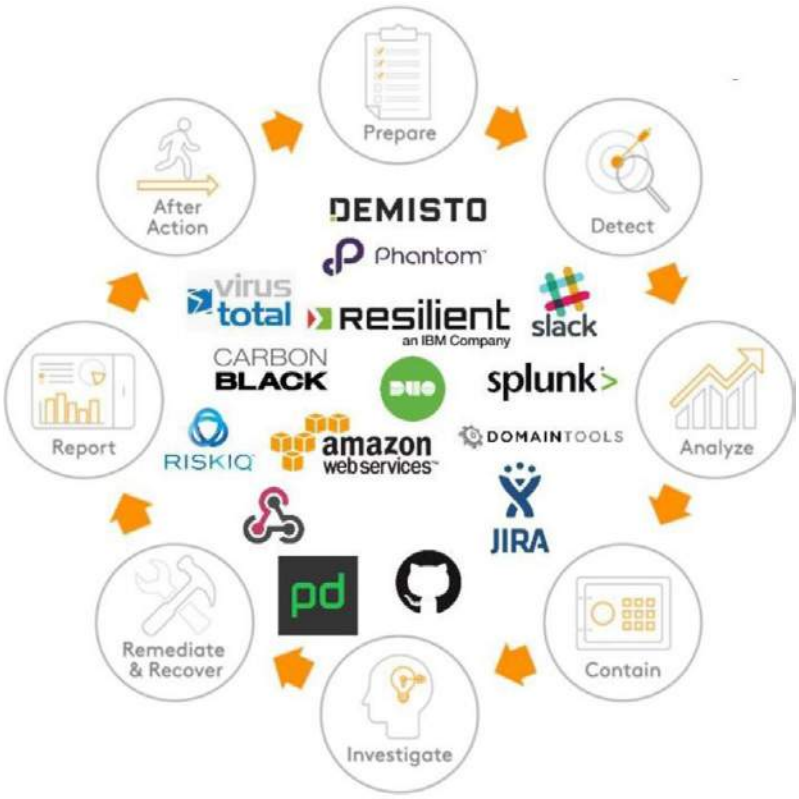
After an initial beachhead is established, adversaries begin to conduct reconnaissance within the environment. To remain undetected until their operational objectives are complete, adversaries will immediately target the security team's communications and incident response tools. When an organization has been breached, only well-coordinated and stealthy response efforts can effectively kick attackers out. Defenders get one opportunity to react before an adversary is aware that they have been burned – don't risk your most critical advantage in an incident for the convenience of commodity communication platforms.



This document outlines how the Wickr Security Operations and Collaboration Platform can be deployed within an organization to enhance network security operations, incident response, and enable secure communications. Wickr will allow incident responders, cybersecurity analysts, and key business stakeholders to take a proactive stance against attackers targeting your organization's most critical assets. This document summarizes our views on the key characteristics of an effective information security program, and how Wickr has developed the capabilities necessary to power security operations teams in their fight against persistent adversaries.

The Wickr Platform

Wickr is designed from the ground up to act as the nexus for security operations. Wickr has taken battle-tested secure communications and collaboration and built deep integrations with productivity and security tooling. The result is a platform which allows network defenders and business stakeholders to spend more time focusing on defense and less on firefighting the very systems they rely on.



The Wickr platform implements the key characteristics of an effective information security program by allowing network defenders to have secure collaboration, enhance their investigation and detection capabilities, and support automation and orchestration workflows. Unlike traditional communications platforms, Wickr has been engineered from the ground up with operational security – and incident response workflows – in mind. As historic incidents have shown, traditional business communications and collaborations systems have been explicitly targeted, degraded, or destroyed by adversaries during an incident – leaving network defenders blind and the business unable to respond. Wickr Pro is the only communication or collaboration product with group-based perfect forward secrecy and explicit integrations that leverage your existing SIEM and security infrastructure. While many collaboration tools function well in peace-time, only Wickr provides the security, stability, and features necessary to survive during war-time against active, sophisticated, and dedicated actors.

Secure Collaboration

Network defenders can leverage best-of-breed secure communication and collaboration technology. With protocols and clients designed to resist targeted adversary activity, Wickr provides reliable, out-of- band, and end-to-end secure messaging, file transfer, voice and video conferencing, and screen sharing. With no complication configuration or IT management required, defenders can response, manage crises, and maintain readiness. Examples of collaborative features and integrations accessible in the Wickr platform include:

Secure instant messaging

- Analysts can discuss ongoing incidents, security issues, and crises with stakeholders without worrying about the confidentiality of messages.
- 1:1 and group messaging provide perfect forward secrecy (PFS) out-of-the-box and without complicated key management or exchange.
- Custom bot integrations, retention settings, and burn-on-read functionality provide security controls configurable for the needs of each organization and incident.

Secure voice and video

- Key business stakeholders, network defenders, and incident responders can collaborate securely in real time via voice or video.
- Screen sharing and secure file transfer enable rapid discussion and collaboration on incidents and alert triage.
- Telecommunication surveillance risks for employees in high-risk countries can be mitigated through usage of the Wickr platform.
- Intelligent smart VPN allows Wickr to bypass restrictive network security controls and filtering in hostile networks.

Native integration with key productivity software

- Analysts working on incidents, alerts, or security operations within Wickr can natively interact with their productivity tooling without context switching.
- Integrations with JIRA, ServiceNow, Trello, GitHub, and Asana allow for creation and tracking of ongoing tasks and projects.
- Integration with PagerDuty easily allows for tracking and responding to incidents. Defenders can manipulate incidents via a chat interface, identify the current on-call, and share updates with other analysts.
- Incoming webhooks allow for teams to dynamically share data from external systems within the Wickr environment.

Advanced API interfaces

- Wickr provides a robust, REST-based API for custom integrations and plugins.
- Native docker images allow teams to quickly spin up new capabilities.
- New plugins and modules can be rapidly deployed to extend the functionality and integration of the Wickr platform.

Enhanced Investigation and Detection Capabilities

Network defenders leverage their day-to-day chat and collaboration capabilities to perform investigation and detection actions. Wickr enables chat-driven and contextual operations for network defenders to investigate, note, and interrogate investigative artifacts. Examples of integrations and features accessible in the Wickr platform include:

Native reporting of IP addresses, hashes, domains, and URLs to investigative services.

- Results are immediately posted back to a given channel for greater transparency and collaboration with other team-members.
- New custom integrations can be easily added through a module-based bot integrated with the Wickr platform.
- Analysts can leverage their existing virustotal, passivetotal, urlvoid, maltego, shodan, maxmind, and domaintools resources.

Native reporting of files to investigative, sandboxing, and detonation services.

- Analysts can leverage their existing virustotal and wildfire resources.
- Reporters are immediately posted back to a given channel for greater transparency and collaboration with other team-members.

Support for generic incoming webhooks.

- Use cases include incoming TAXII, STIX, and other structured data into channels.
- Analysts can ingest incoming RSS feeds, alerts, twitter notifications, open-source reporting, and arbitrary HTTP content.

Automatic de-referring, de-fanging, and unfurling of hyperlinks.

- Analysts working with dangerous domains or against adversary resources can specify granular security controls on a per-channel basis.
- De-referring prevents hyperlink activity from leaking the source of the request by hiding the referrer.
- Unfurling automatically resolves short-links to their original hyperlink.
- Ephemeral browsing can be used to securely view potentially harmful resources.
- De-fanging prevents accidental clicks on potentially dangerous hyperlinks.

On-demand visual capture of hyperlinks.

- Analysts can leverage native integrations with ScreenshotMachine and URLVoid to perform a dynamic visual capture of a given hyperlink. The image is posted back to a given channel for greater transparency and collaboration with other team-members.

Support for tagging of messages with a given Traffic Light Protocol (TLP) designation.

- TLP is the standard for information dissemination in trusted communities.
- Messages may be tagged with a WHITE, GREEN, YELLOW, or RED TLP tag.
- Presence of a TLP tag will prevent accidental disclosure, control interactions with integrations, and assist defenders in compartmentalizing incident findings.

Automation and Orchestration

Incident detection and response programs scale through intelligent automation and orchestration. Integrating with leading security orchestration, automation and response (SOAR) technologies, Wickr allows network defenders to detect and respond to security issues faster than conventional platforms. Examples of integrations and features accessible in the Wickr platform include:

Native integration with SOAR platforms.

- Analysts can leverage their existing Splunk Phantom, Demisto, or Resilient platforms through bi-directional native applications.
- Notifications of new alerts, incidents, or issues can be configured to immediately notify team members in a given channel.
- Wickr API functionality can be leveraged through native SOAR apps to automatically distribute messages and send files to verified recipients, process evidence, and spin up war rooms.
- Alerts from Splunk and ELK can be ingested into Wickr to notify defenders of potential security incidents.
- Network defenders are empowered to develop, distribute, and manage effective incident response playbooks without worrying about operational security concerns.

Decentralize alerting through Wickr-based user alerts.

- Security events, alerts, and incidents can have decentralized triage through native user notification and challenge/response functionality.
- Users can be notified of security events via Wickr direct messages or channel notifications to increase security awareness and reporting of unusual activity.
- Users can optionally be given a challenge/response scenario where confirmation of a given alert must be accepted or denied using the Wickr client.
- Native Duo integration can allow for multi-factor authentication on alert notifications.
- Leveraging Wickr for decentralized alert triage decreases the burden and friction for network defenders, decreases mean time to detection, and enables scale of the detection program.

Securely process sensitive data, artifacts, and forensic evidence.

- Native integration with Amazon S3 and end-to-end encryption allows response engineers to quickly and securely acquire, store, and share incident artifacts.
- Disk and memory snapshots, logs, and other forensic artifacts can use the Wickr platform for encryption, access controls, and key management.
- Evidence is encrypted, uploaded to a team-controlled S3 bucket, and can then be retrieved or shared using the Wickr client.
- No longer do teams need to deal with clumsy command-line encryption tools, complex key exchanges, or unencrypted artifacts.

Key Characteristics of an Effective Information Security Program

Fortune favors the prepared. For cyber incident responders and continuity experts, the most critical time to act is before an incident occurs. Increased dependence on electronic communications and IT systems means increased vulnerability to cybersecurity attack. Catastrophic business compromise and breaches have dragged information security into the boardroom and public eye. Wickr has worked with countless security-conscious organizations to identify and analyze the three most important processes in breach mitigation and response. Wickr has focused development efforts to build innovative solutions to inject security and speed to these critical processes:

- **Hardened Communications:** Secure communications are vital to a business, especially for information security, response, and executive teams. Information shared during a security incident – including vulnerabilities, countermeasures, or investigation summaries – are extremely valuable to attackers. Wickr Pro is the only communication or collaboration product with group-based perfect forward secrecy, allowing us to provide transparent key management and guaranteed security of all communications and data.
- **Detection and Response:** Breaches are an inevitability and network defenders must be armed with the ability to detect and respond to adversaries. Incident responders need to have greater provenance and faster response times to potential security incidents, as well as deep integration with tooling to multiply their effectiveness during incidents. Wickr Pro is built atop a fast and secure data transport layer that eliminates unnecessary latency while embracing best in class encryption.
- **Automation and Orchestration:** Automation and orchestration are the key to scaling security operations and reducing the mean time to detection for incidents. Deep integration with productivity and security orchestration, automation and response (SOAR) is crucial to the maturity, scale, and effectiveness of a security team. Wickr Pro integrations enable secure data transfer between security and orchestration tools to empower network defenders.

In the absence of these principles, organizations quickly find themselves vulnerable to ongoing cybersecurity incidents and breaches. When these processes are inefficient and insecure, alert fatigue plagues members of the security operations center (SOC). Communications cannot be trusted against tampering or interception, and adversaries are able to operate within the network with impunity. Wickr has been designed from the ground up to empower businesses with highly reliable, out-of-band, end-to- end secure collaboration and deep integration with existing security technologies. With Wickr, information security teams can effectively manage crisis, maintain readiness, and ultimately mitigate risk to critical business operations.

Common Challenges Faced by Incident Response Teams

Industry giants like Sony, Maersk, and Merck, have joined an exclusive fraternity of which the only requirement is to have business operations taken offline through cybersecurity attack. Analysis of incident post-mortems have routinely identified deficiencies in detection and response programs. Without adequate investment in automation and orchestration, detection and response, and secure communications, the timeline and impact of a given incident grows dramatically in size.

The Sony Breach of 2014 is a prime example where attackers were able to exist within the network without detection and compromise critical business information. In this attack, the adversaries gained access to Sony's internal communications channels and were able to monitor the incident response communications and react to remediation efforts. Enabling effective incident detection and response and maximizing security automation have been the primary focus of security teams, but any advantages gained through automation can be neutralized by an attacker who knows your process and sees your communications. Advanced teams are optimizing for data and communications security to ensure security incidents are contained and orchestration and automation is sustainable.

Secure Collaboration is Impossible

Incident responders rely on having collaboration tools that are suitable for conducting investigations and defensive operations with. This work not only must enable responders to communicate with one- another but with critical business stakeholders as well. Members of the executive, legal, communications, and infrastructure teams need to be able to operate seamlessly with defenders during an incident. Teams need highly secure, out-of-band communication channels that can allow for 1:1 and group messaging, audio/video conferencing, and file transfer workflows. Instead, response teams must rely on organization-managed chat clients which provide no end-to-end security guarantees, file transfers over potentially compromised infrastructure, and rely on the availability of corporate resources. As identified numerous incident post-mortems, the lack of secure communication ultimately erodes trust in the integrity and confidentiality of collaboration and greatly weakens the effectiveness of security response operations.

Too Many Panes of Glass Exist

Each security tool has touted itself as the next 'pane of glass' to unify all the complex workflows and analysis work for security engineers. In doing so, the focus, attention, and energy of defenders is stretched and fragmented. Engineers waste precious cycles hopping between chat clients, sending files via e-mail, opening browser tabs, accessing other tools, and manually copying data into ephemeral documents for tracking. Deep focus is required for defenders to perform at their best during investigations and, without building workflows to enable this focus, they will be at the mercy of their tooling. Teams need to reduce the number of discrete systems they need to access during an incident. Collaboration tooling should work to bring the knowledge and information they need into a centralized location, give them the tools to effectively handle a crisis, and then get out of the way. In the incident response world, focus is the currency of defenders.

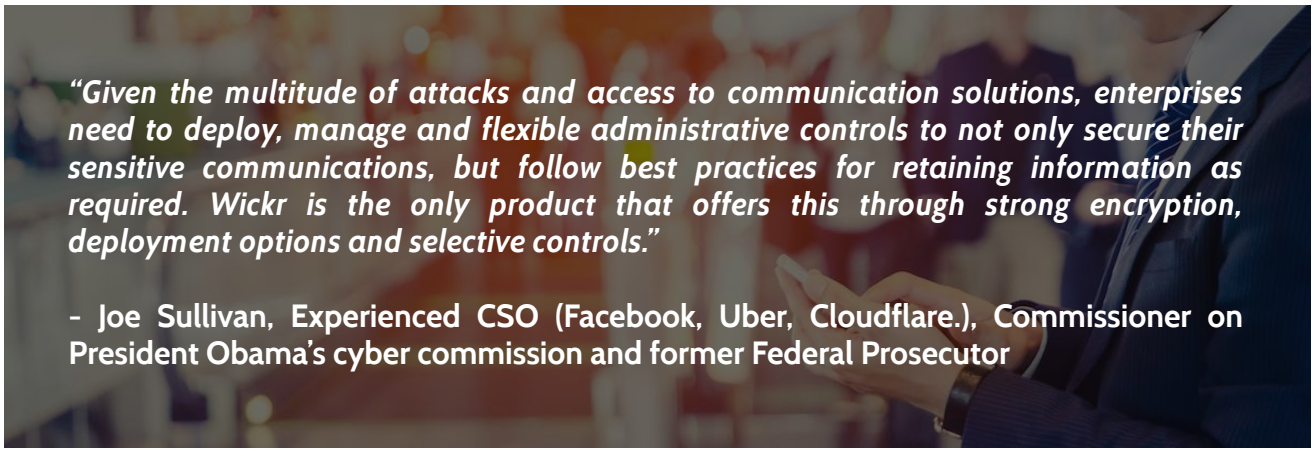
Automation Is Lacking

There is a draught of highly talented information security professionals worldwide and doubly so for incident response specialists. Scaling a security team to match the growth and needs of the business, while adapting and responding to ever-changing adversaries, is not a linear proposition that can be solved through hiring. Security teams are already strapped for time, which prevents investment into automation and other time-saving technologies that could provide uplift to their operations.

Integrations that are developed need to be developed with robustness, handle changes to established application programming interfaces (API) and be updated to fit new tooling. The burden introduced by managing and maintain rudimentary automation can further tax defenders. Wickr Pro integrations are reliable, robust, and secure – leaving little opportunity for adversaries to compromise content or impact availability. Most importantly, automation should be a force multiplier for defensive operations. Wickr Pro gives network defenders the flexibility to decentralize alerting to responsible parties, spin up incident war rooms with ease, and effortlessly utilize their existing tooling.

Summary

Our adversaries are adaptive. As the enterprise has invested heavily in security tooling, highly-trained personnel, and automation, adversaries have responded in kind. Any momentary weakness in the security posture of an organization can be exploited through offensive automation. As improved logging and end-point security technologies have decreased the mean time to detection of an adversary in a network, adversaries have invested in lateral movement, stealth, and exfiltration capabilities – increasing the speed, scope, and breadth of a given compromise. With the arms race of offensive and defensive capability, time to response become more important than ever.



"Given the multitude of attacks and access to communication solutions, enterprises need to deploy, manage and flexible administrative controls to not only secure their sensitive communications, but follow best practices for retaining information as required. Wickr is the only product that offers this through strong encryption, deployment options and selective controls."

- Joe Sullivan, Experienced CSO (Facebook, Uber, Cloudflare.), Commissioner on President Obama's cyber commission and former Federal Prosecutor

As traditional anti-virus products have been supplanted by more sophisticated endpoint detection and response (EDR) and protection (EPP) products, communication and collaboration tools must undergo the same shift. Breaches, such as Sony, Maersk, and OPM have continually reinforced a very important point: any defensive advantage can be neutralized by an attacker who is able to intercept, modify, or deny your communications and response.

Wickr is the only communications or collaboration platform that has been designed from the ground up to provide perfect forward secrecy, integrate deeply with existing security tooling, and enable faster defensive operations. While many collaboration tools function well in peace-time, only Wickr provides the security, stability, and features necessary to survive during war-time against active, sophisticated, and dedicated actors. When the business is at stake, don't rely on traditional cloud communication platforms with weak security, plaintext logs, and minimal tooling integration. Empower your defenders, utilize your existing security technologies, and ultimately maintain the most important home-field advantage you have: the element of surprise. Choose Wickr Enterprise-class Solutions.

Copyright © 2019 Wickr Inc