Palantir

100 Hamilton Avenue
Palo Alto, California 94301

PALANTIR CYBER

An End-to-End Cyber Intelligence Platform

TABLE OF CONTENTS

INTRODUCTION

Every important organization in the world is under attack from sophisticated, persistent cyber threats, from hackers to organized crime networks to state-sponsored attackers.[1] Traditional cyber defense systems rely heavily on rules-based detection methods that focus on blocking attacks in their initial stages. But perimeter defenses based on simple logical rules are only one component of effective cyber defense.

The most dangerous cyber attacks are often perpetrated by advanced persistent threats (APTs) and other highly adaptive adversaries that cleverly evade rules-based detection, linger inside organizational networks, and build intelligence about network vulnerabilities over time. Malicious actors target specific organizations, repeatedly attacking to gain a holistic understanding of an organization's defenses and then patiently waiting to exploit vulnerabilities. In addition to these external threats, organizations face internal threats related to data loss, risky employee behavior, and access abuse.

Combatting such sophisticated threats requires analysis and investigation of data that is both extremely diverse and ultra-large scale. An effective solution must be able not only to ingest large-scale structured and unstructured data from disparate sources but also to expose that data to intuitive analytical tools and enable organizations to build threat intelligence over time.

Palantir Cyber is data fusion and analysis software, capable of rapidly integrating, managing, and securing data of any kind, from any source, at massive scale. Palantir's powerful back end and flexible object model enable both structured and unstructured cyber data to be transformed into meaningful objects and relationships: people, places, things, events, and the connections between them.

Once data is integrated and modeled, Palantir Cyber enables analysts to intuitively interact with cyber data through a suite of powerful analytical applications. Analysts can search across all data sources at once, visualize relationships, explore hypotheses, discover unknown connections, surface previously hidden patterns, and share insights with other teams. All discoveries and analysis are fed back into the system, ensuring that future investigators can build on prior insights.

With all data and analytical applications in one environment, Palantir Cyber leverages advanced detection and alert enrichment technologies, allows analysts to seamlessly pivot from detection to deep-dive investigations to reduce incident response time, and captures analyst insights to enable organizations to harden their defenses, providing a holistic, end-to-end cyber solution.

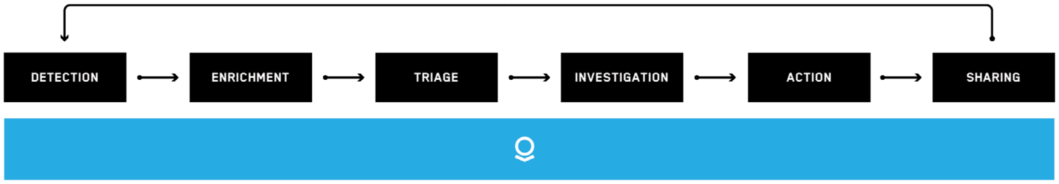
[1] For example, the Justice Department "indicted a group of Chinese hackers who work for the People's Liberation Army Unit 61398, and charged them with stealing corporate secrets." (Chinese Hackers Pursue Key Data on U.S. Workers, *New York Times*, July 9, 2014). Many other severe attacks have been perpetrated against major companies and U.S. government agencies by criminal networks and state-sponsored groups.

OUR SOLUTION

Palantir Cyber is built upon five foundational capabilities:

Data Integration	Fuse petabyte-scale data of any type and format from disparate data sources and third-party systems into a unified environment that is flexible (stores raw data and processes it on the fly) and fast (queries billions of log lines in seconds)
Pattern Detection	Algorithmically search all integrated data to surface events of interest and enrich alerts with relevant context
Analytics & Investigation	Triage alerts by conducting multi-faceted search and analysis across all integrated data, interactively drill down against billions of log lines, and build out investigations to uncover the full extent of a threat
Knowledge Management	Seamlessly capture intelligence, understand what information has been seen before, collaborate to build an institutional knowledge base of threat actors, and incorporate insights into detection algorithms and analyses
Secure Collaboration	Exchange insights, detection methodologies, enriched indicators, and other information about cyber threats in real time, subject to highly granular access controls and automatic redaction of sensitive data

These capabilities reinforce one another to provide a complete cyber solution that enables organizations to monitor activity across systems, enrich and triage alerts, investigate unauthorized activity, and capture insights to harden defenses—all within a unified environment. Palantir integrates with existing defenses and enhances cyber defenses at all stages of the cyber workflow:

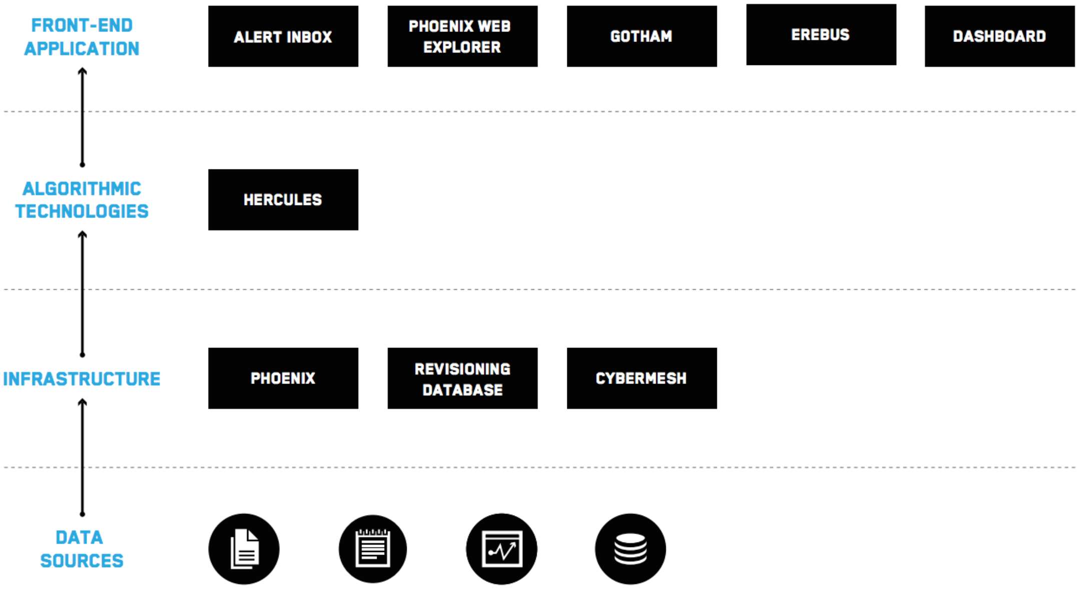


Palantir Cyber was designed from the ground up to protect privacy and civil liberties. Our security model, which includes granular access controls and tamper-evident audit logs of all system and user activity, is an integral component of our platform. By seamlessly integrating multiple security features into Palantir Cyber, we reduce user friction that might otherwise create incentives to circumvent data security measures. In this way, Palantir Cyber safeguards sensitive information while enabling powerful analysis.

TECHNICAL OVERVIEW

Palantir Cyber is built with a powerful back-end infrastructure and flexible front-end interface that optimizes detection and analysis of cyber data at scale. Palantir's comprehensive approach enables organizations to bring all information related to cybersecurity into a unified environment, providing a holistic view of the threats facing an organization. Once all relevant data is integrated, organizations can use Palantir to detect threats, quickly triage and contextualize alerts, perform deep-dive investigations, and automatically incorporate new knowledge into the enterprise repository to harden defenses against future attacks.

Palantir Cyber's technical architecture can be conceptualized as shown in this diagram:



The following sections outline how these key technologies power each of Palantir Cyber's foundational capabilities: namely, data integration, pattern detection, analytics and investigation, knowledge management, and secure collaboration.

Data Integration

Defending against sophisticated cyber adversaries requires analysis of data that is both extremely diverse and extremely large scale. **Palantir Phoenix**, a horizontally scalable, distributed data store, enables integration and sub-second querying of trillions of records at petabyte scale. Unlike traditional warehousing that can take years to clean up and process data into a unified format that is ready to consume, Phoenix stores data in its raw format and transforms it on the fly into Palantir's structured object model. Phoenix can integrate new data sets extremely quickly and easily evolve formats to fit changing business needs.

Out of the box, Palantir can integrate the full spectrum of common cyber data sources into a unified environment for rapid analysis, including but not limited to:

- **Network Appliance Data:** Proxy, firewall, IDS, VPN, DNS queries
- **Communications Data:** Email, internal chat logs, phone records
- **Physical Data:** Facility access logs, print logs
- **Host-based Data:** Antivirus, endpoint protection
- **Contextual Data:** HR data, Active Directory, asset inventory
- **Third-party Data:** RSS feeds, databases of cyber threat actors, indicators of compromise (IOC) intelligence reports, IP and domain reputation feeds

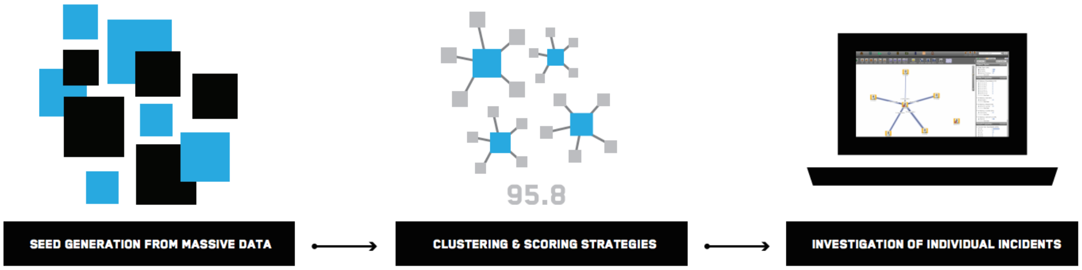
Palantir also ships with a suite of applications to enhance your enterprise's security posture, enable secure information sharing, and facilitate data reliability. Palantir provides access to collaborative and external cyber resources, including the Palantir Cybermesh (discussed below).

Pattern Detection

Traditional cyber defenses generate thousands of alerts that drown investigators in noise and false positives. Moreover, these alerts depict only one slice of attacker activity during a limited timeframe. An effective cybersecurity strategy relies on both rapid alert triage and identification of activity patterns across alerts.

Palantir Hercules allows enterprises to build and iterate on strategic search algorithms that prioritize and enrich existing alerts as well as detect new cyber threats. Unlike traditional systems that trigger alerts based on activity during a narrow time window, Palantir's data integration and knowledge management capabilities enable Hercules to flag activity based on intelligence received months ago.

To produce alerts, Hercules combs through all data integrated into Palantir (including existing alert feeds), clusters related alerts, enriches them with information from across the enterprise, and prioritizes them for analyst triage. These capabilities allow analysts to quickly discard false positives, immediately contextualize events of interest, and accelerate investigations.


95.8
SEED GENERATION FROM MASSIVE DATA
CLUSTERING & SCORING STRATEGIES
INVESTIGATION OF INDIVIDUAL INCIDENTS

Palantir Hercules lifts signal out of noise by building context around each alert using other data sets integrated into Palantir.

For example, if an alert is generated on outbound proxy traffic indicating a potential malware callback, Hercules will search data stored in Palantir to determine whether there are other alerts related to that particular callback and form an alert cluster. The alerts are then enriched with additional information, like the computer's owner, DHCP lease, and additional proxy traffic around the time of the alert. These clustered, enriched alerts are then prioritized for analyst triage and review.

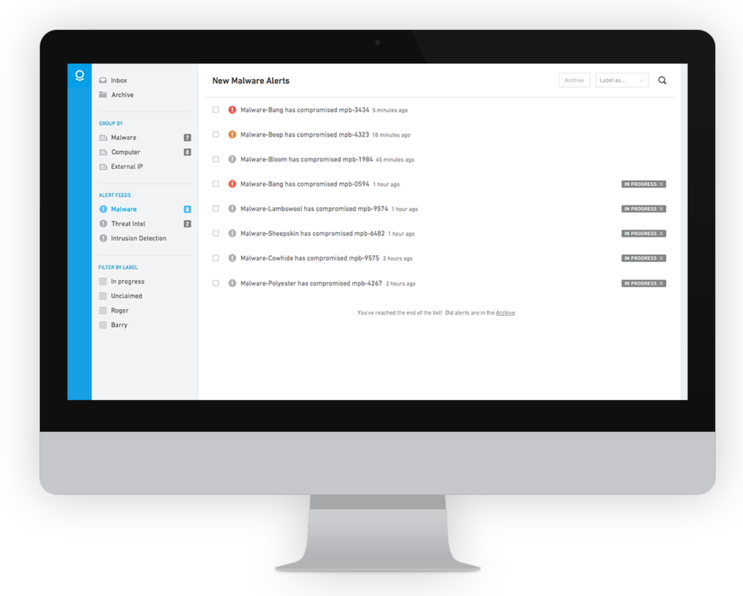
Analytics & Investigation

No matter how robust a network's defenses, breaches are bound to happen. Consequently, the time immediately following detection is critical to preventing additional damage—analysts must be able to rapidly understand the nature of the threat and identify the breadth of exposure.

Analysts can leverage a robust suite of analytical applications that enable organizations to triage alerts, drill down on the most critical ones, and quickly assess the extent of exposure. Out of the box, Palantir Cyber provides the following technologies to support rapid alert triage and investigation:

Alert Inbox	Presents and contextualizes enriched alerts in an intuitive web application
Phoenix Web Explorer	Allows search and top-down analysis of massive-scale data stored in Palantir Phoenix
Gotham	Enables relational, link, geospatial, temporal, and statistical deep-dive analysis

Alert Inbox is a web-based case management and alert processing application that presents analysts with alerts generated directly by Hercules as well as by third-party systems. Alert Inbox enables analysts to track, visualize, and drill down to view additional detail on alerts, as well as label and assign alerts. All context around a potential threat is displayed, including the triggering event and source log lines, allowing analysts to quickly determine whether the threat is a false positive or needs to be escalated for more in-depth review.



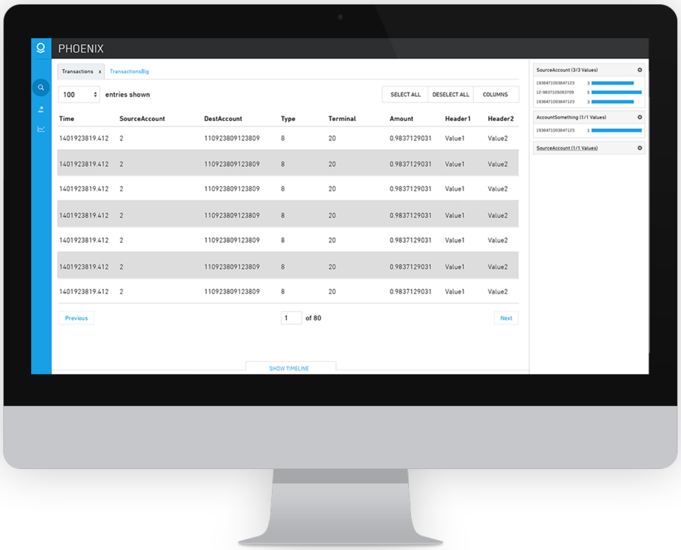
New Malware Alerts

- □ Malware-Bang has compromised mpb-3434 5 minutes ago
- □ Malware-Beep has compromised mpb-4323 18 minutes ago
- □ Malware-Bloom has compromised mpb-1984 45 minutes ago
- □ Malware-Bang has compromised mpb-0594 1 hour ago IN PROGRESS ×
- □ Malware-Lambswool has compromised mpb-9574 1 hour ago IN PROGRESS ×
- □ Malware-Sheepskin has compromised mpb-6482 1 hour ago IN PROGRESS ×
- □ Malware-Cowhide has compromised mpb-9575 2 hours ago IN PROGRESS ×
- □ Malware-Polyester has compromised mpb-4267 2 hours ago IN PROGRESS ×

You've reached the end of the list! Old alerts are in the Archive.

Alert Inbox provides analysts with a holistic view of alerts and contextualizes them with relevant information, dramatically accelerating alert triage.

To quickly gain additional context on indicators of interest, analysts use **Phoenix Web Explorer** to search across and conduct top-down analysis of all integrated data. Explorer's flexible web-based search empowers analysts to define and test hypotheses on an ad-hoc basis. This lightweight access against billions of records provides situational awareness and enables analysts to understand their data in ways that were previously unachievable.



Time	SourceAccount	DestAccount	Type	Terminal	Amount	Header1	Header2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2
1401923819.412	2	110923809123809	8	20	0.9837129031	Value1	Value2

Phoenix Web Explorer enables sub-second querying and top-down analysis of massive-scale data.

To perform comprehensive, deep-dive investigation, analysts can pivot to the **Palantir Gotham** investigative platform with a single click. Gotham is Palantir's intuitive investigative and analytical workspace and is used to drive investigative insights for organizations across the commercial, intelligence, and military sectors. Unlike traditional cyber defenses that require analysts to switch tools, Palantir's end-to-end solution allows analysts to investigate alerts in Gotham without leaving the workspace. This time saving is crucial in cybersecurity investigations where incoming information goes stale in hours.

Palantir Gotham includes dozens of applications and helpers that analysts can use to perform link, relational, geospatial, temporal, statistical, and other kinds of analysis. Armed with powerful analytical tools, analysts can see high level information about large sets of enriched alerts, discover and visualize connections between seemingly unrelated events and entities, map hostile activity based on origin, and identify critical vulnerabilities across enterprise systems and networks.

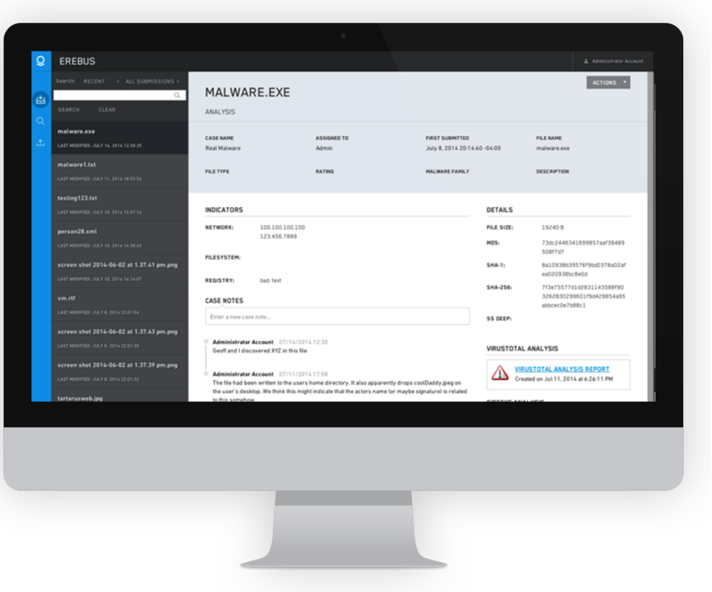
Gotham also allows analysts to perform forensic investigations. Analysts search and analyze enormous volumes of data in a variety of formats and from a variety of sources, such as hard drive images, firewall logs, and sensitive customer databases. Analysts independently research case elements and input discoveries back into Palantir, allowing for real-time collaboration between team members. This collaboration enables teams to piece together a coherent story on an expedited time frame.

Knowledge Management

Sophisticated attackers are highly adaptive and quickly learn to evade static defenses. Without a way to capture insights generated in recent investigations and harden defenses based on the most recent information, organizations cannot keep pace with novel attacker tactics.

Palantir's **Revisioning Database** captures every insight produced at every stage of the cyber workflow and transforms those insights into actionable intelligence. For example, if an IP address flagged in an alert is dispositioned as a true positive, Palantir records that as threat intelligence about that IP address. If the IP address comes up in a future investigation or Hercules search, Palantir will flag the prior knowledge so that investigators can incorporate it into their analysis. These knowledge management capabilities enable analysts to fully leverage previous analysis, decipher patterns of attacks over time, and connect old and new tactics to common threat actors.

Palantir also features **Erebus**, a malware repository that allows analysts to upload potentially malicious files, automatically extracts relevant information (e.g., file size, associated IP addresses), and records analyst conclusions about the file.



malware.exe
LAST MODIFIED: JULY 14, 2014 12:30:35

malware1.txt
LAST MODIFIED: JULY 11, 2014 18:55:54

testing123.txt
LAST MODIFIED: JULY 10, 2014 15:37:16

person28.xml
LAST MODIFIED: JULY 10, 2014 14:38:43

screen shot 2014-06-02 at 1.37.41 pm.png
LAST MODIFIED: JULY 10, 2014 14:14:07

vm.rtf
LAST MODIFIED: JULY 8, 2014 22:01:54

screen shot 2014-06-02 at 1.37.43 pm.png
LAST MODIFIED: JULY 8, 2014 22:01:35

screen shot 2014-06-02 at 1.37.39 pm.png
LAST MODIFIED: JULY 8, 2014 22:01:32

tartarusweb.jpg

MALWARE.EXE

ANALYSIS

CASE NAME	ASSIGNED TO	FIRST SUBMITTED	FILE NAME
Real Malware	Admin	July 8, 2014 20:14:40 -04:00	malware.exe
FILE TYPE	**RATING**	**MALWARE FAMILY**	**DESCRIPTION**

INDICATORS

NETWORK: 100.100.100.100
123.456.7889

FILESYSTEM:

REGISTRY: bad: text

CASE NOTES

Enter a new case note...

Administrator Account 07/14/2014 12:30
Geoff and I discovered XYZ in this file

Administrator Account 07/11/2014 17:58
The file had been written to the users home directory. It also apparently drops coolDaddy.jpeg on the user's desktop. We think this might indicate that the actors name (or maybe signature) is related to this somehow

DETAILS

FILE SIZE: 19240 B
MD5: 73dc2446341699857aaf39489508f7d7
SHA-1: 8a10938b39576f9bd0378a02afea020938bc8e0d
SHA-256: 7f3e75577d1d2831143588f903262830299601f9d429854a95abbcec0e7b88c1
SS DEEP:

VIRUSTOTAL ANALYSIS

VIRUSTOTAL ANALYSIS REPORT
Created on Jul 11, 2014 at 6:26:11 PM

Erebus automatically enriches malware samples with third-party intelligence.

Erebus automatically submits uploaded files to third-party malware sandbox tools like VirusTotal and pulls in associated malware intelligence without any additional analyst action. This information is then fed back into Hercules detection and clustering algorithms, providing a dynamic threat intelligence and detection feedback loop. For instance, an alert will be triggered if an unrecognized file makes a call to a URL that is associated with another file in the malware repository.

Palantir also enables organizations to incorporate the most recent third-party information into their knowledge base. Palantir can integrate any structured or unstructured threat intelligence source and automatically extracts indicators of compromise from threat intelligence documents, allowing organizations to monitor for these indicators on their network.

Palantir's central repository allows multiple analysts to work on the same data while engaging in independent lines of inquiry. This allows for a richly collaborative environment in which each analyst can pursue their own hypotheses and analyses while benefitting from the shared cyber intelligence of others. All investigations performed in Palantir become a source of high-signal investigative intelligence that can be used for correlation, enrichment, and search in the same way as third-party threat intelligence.

Palantir also enables managers and executives to easily view key organization-level statistics and trends to understand the state of their cybersecurity environment via scalable web-based **Dashboards**. Dashboards visually represent network activity, anomalies, and threat trends over time. For example, dashboards can show the volume of IDS alerts over time or highlight a deviation from the mean in the number of malware alerts received in a given month. In addition to the full series of dashboards available out of the box, Palantir provides an HTML5-based framework for rapid dashboard customization.

All knowledge management activities in Palantir are governed by fine-grained access controls. This allows organizations to define granular access controls to secure every piece of information stored in Palantir.

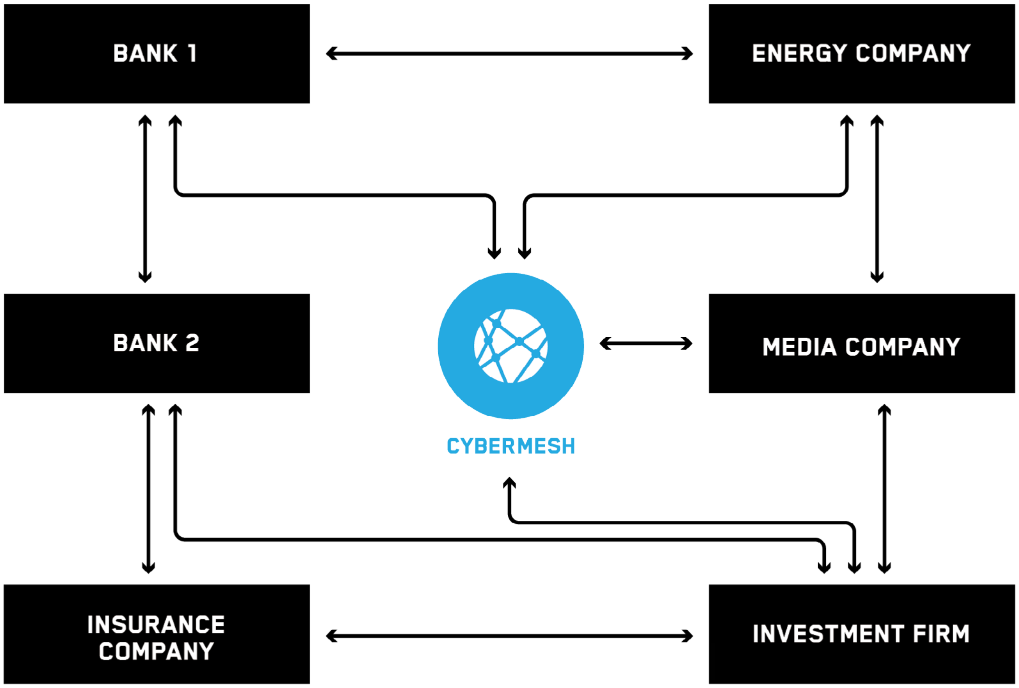
Secure Collaboration

Recognizing that commercial institutions face a shared set of cyber threats, we created the **Cybermesh**, a platform for secure information sharing among peers. The Cybermesh is built on information-sharing technology that we developed for the defense and intelligence communities and has been deployed and battle tested in some of the world's strictest security environments.

Peers are often the only sources of information about targeted attacks. The Cybermesh enables secure peer-to-peer sharing between enterprises with automatic redaction of sensitive data. By enabling organizations to leverage insights from peer institutions, the Cybermesh provides immense analytic value over automated black box solutions.

As members of the Cybermesh, organizations also receive a weighted data feed of indicators of compromise (IOCs) drawn from open source and other Cybermesh participants. Palantir automatically correlates the feed against customer–owned data sets and presents algorithmic-based alerts for investigation. While the automatic correlation rules are deployed broadly, they are run specific to each customer and run against only the data sets in their environment.

Organizations participating in the Cybermesh can also opt to share analytical insights with trusted partners. Organizations decide what information (if any) they want to share and receive and who their partners are.



Cybermesh enables secure information sharing among peers.

PALANTIR CYBER USE CASES

From data exfiltration and other internal threats to external threats like malware or phishing schemes, Palantir Cyber addresses the most critical threats from both inside and outside the enterprise. The following sets forth a non-exhaustive list of use cases where Palantir Cyber drives successful cybersecurity outcomes.

Internal Threat Use Cases

Data Exfiltration	Analysts can deploy custom algorithms to detect high-risk employee behavior, such as sending emails to vulnerable accounts (including personal email addresses) or writing data to thumb drives. These algorithms can also identify unusual employee activity, such as a spike in printing activity or uncharacteristic access to critical or sensitive internal resources.
Access Abuse	Palantir Cyber reconciles application and privileged access across the enterprise. By integrating and correlating application access logs, Active Directory records, HR files, VPN activity, authorization systems, and other data sources, Palantir enables analysis of access rights across sensitive internal data repositories. With entitlements from across the enterprise integrated in a unified environment, CISOs and other executives can pursue data-driven access reduction strategies to reduce both internal and external risk.

External Threat Use Cases

Phishing	Palantir Cyber streamlines the detection, triage, and investigation of phishing incidents by running automated searches to detect emails with similar subjects, senders, or attachment names and discover all recipients of the attachment.

Phishing (Cont.)

Hercules contextualizes high-risk emails with referential data and prioritizes them for analyst review based on “clicks,” the potential malicious nature of the URL contained in the email, and proxy traffic to the URL.

Palantir Cyber also allows analysts to correlate email metadata with other integrated network logs to identify recipients who clicked on malicious links and create lists of high-risk employees who have been repeatedly targeted to prioritize them for remediation or social engineering training.

Automated Threat Intelligence

Palantir Cyber integrates all structured and unstructured threat intelligence available to the enterprise, including third-party sources and internal material generated by threat intelligence analysts.

Palantir extracts indicators of compromise from unstructured intelligence (e.g., domains, IP addresses, and hashes) and automatically correlates all such indicators against network controls (e.g., proxy and endpoint logs). If a match is found, an alert is generated and enriched with contextual information including all available threat intelligence about the indicators involved.

When enriching alerts not originally generated by threat intelligence correlation, Palantir checks for available threat intelligence on the indicators involved and automatically presents relevant intelligence to the analyst. For example, if an analyst is working on a malware infection alert, Palantir will check for available structured or unstructured threat intelligence (e.g., the malware’s hash, the C2 servers involved).

Automated Threat Intelligence (Cont.)

In addition to automatically correlating and enriching with this threat intelligence, Palantir also makes the entire corpus of intelligence searchable to all analysts for any arbitrary queries necessary during investigation. For example, analysts find answers to questions such as, “Do we have any threat intelligence about this family of malware and if so, what threat actors are associated with it?”

Malware Response

Palantir Cyber provides a central repository of human and machine-generated knowledge about malware to detect new infections and identify trends.

A custom application optimizes reverse engineering workflows by enabling malware analysts to upload collected malware file samples, record observations, and automatically annotate samples with third-party analysis (e.g., FireEye, VirusTotal). This application can be extended to include other custom tools allowing analysts to derive metadata from malware samples.

Analysts can continuously run indicators derived from file sample analysis against network logs to identify new infections. They can also analyze temporal patterns and cluster malware samples based on shared infrastructure or toolsets to identify sustained campaigns against the enterprise.

These capabilities institutionalize malware expertise across the enterprise, automate malware detection based on the latest intelligence, and significantly raise attacker overhead by detecting instances of code and infrastructure reuse.