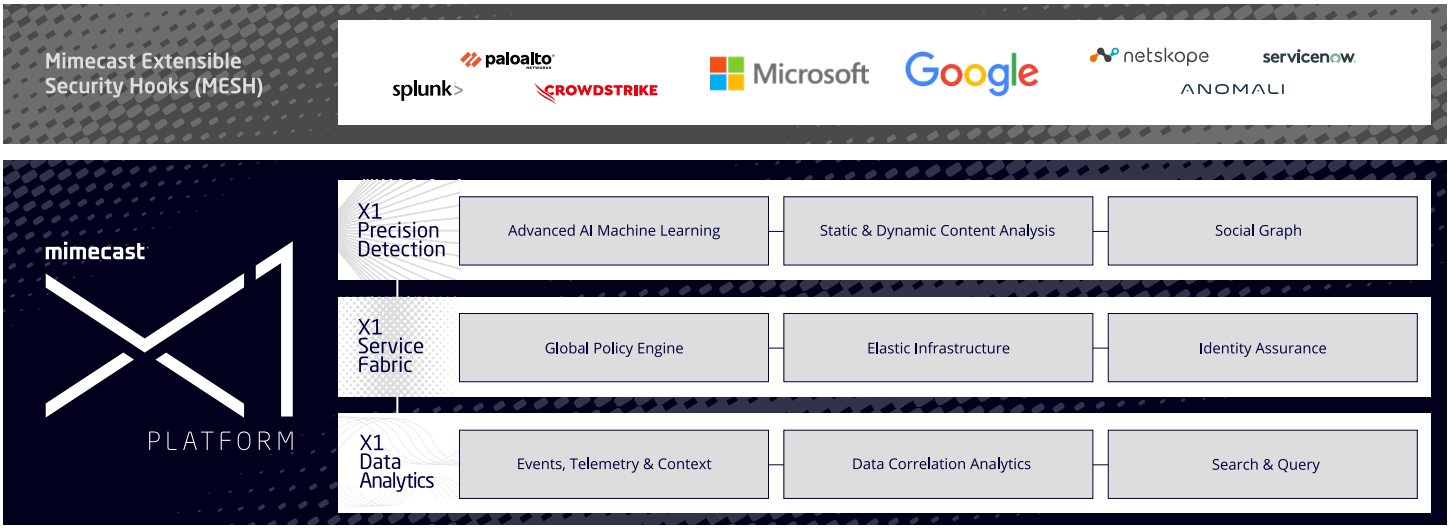
Solution Brief

mimecast

The Mimecast X1 Platform

Protection, Insights, Scale

Mimecast X1 is the foundation of the Mimecast Solution Suite — powering fully integrated services that deliver industry-leading protection for communications, people, and data; making information actionable at scale; supporting rapid innovation; and providing the resilience and scalability that the modern threat landscape demands. The result is the ability to tame complexity, control risk, and work protected.



X1 Precision Detection

Unparalled protection from threats

Mimecast X1 Precision Detection provides the industry's most advanced defense for the top attack vector, email, and protects organizations at their most vulnerable point — the intersection of communications, people, and data. By applying the right detection capabilities at the right time, X1 Precision Detection surrounds your communications with continuous protections, letting end users work protected — not interrupted. The industry's most robust view of the email threat landscape — derived from Mimecast's inspection of 1.3 billion emails daily — powers instantaneous blocking of the vast majority of email-based threats, while the latest in AI and Machine Learning provides intelligent detection of both emerging and unknown threat types. With continuous learning built in – backed by the human intelligence that only 20 years of experience can provide — X1 Precision Detection delivers continuous protection, proactive defense, and world-class efficacy.

X1 Precision Detection includes the following key components:

AI and Machine Learning

Mimecast uses AI and Machine Learning across the X1 Precision Detection layer, with analysis and models based on Mimecast's analysis of more than 1.3 billion emails daily. By filtering out malicious emails at scale and driving intelligent analysis of the "unknown", AI and Machine Learning optimize efficacy and help Mimecast's experts make smart decisions about communications that fall into the gray area between safe or malicious. These learnings are continuously fed back into our detection engines to optimize our inspection models with up-to-the minute intelligence, blocking emerging attack types and protecting our customers from the most dangerous threats while also minimizing false positives.

Mimecast's philosophy is that AI and Machine Learning are only as effective as the data and cybersecurity expertise that power them. They are not a panacea but rather a critical augmentation layer for the detection capabilities that we have developed, invested in, and continuously improved for 20 years. We apply these technologies whenever they are the right choice to help us maximize our customers' defenses and back them with the most critical ingredient of all — the visibility, human intelligence, and deep expertise that only Mimecast can provide.

Social Graphing

Powered by Machine Learning, Social Graphing is technology that can be used to link properties (e.g., M365 or Google Workspace) with identifiers (e.g., end-user name, physical location, etc.) to create a consistent, unified view of communications. Mimecast uses this technology to map an organization's communications patterns and create a social graph that stores information about relationships and connections between all senders and recipients, including the strength or proximity of those relationships.

The Social Graph learns about behaviors with respect to what's normal and what is not and can then detect anomalous behaviors that may indicate a malicious email or the potential exposure of data, whether accidental or intentional. Mimecast uses Social Graphing as an added layer of protection against data leaks and to bolster defenses against highly sophisticated, targeted email attacks that rely on tactics like social engineering and file-less malware.

Static and Dynamic Content Analysis

X1 Precision Detection uses static and dynamic content/metadata analysis to identify and instantly block the vast majority of email-based threats. By applying the right detection capabilities at the right time and continuously optimizing them through AI, machine learning, and the expertise of the Mimecast Security Operations Center (SOC), X1 Precision Detection blocks the most sophisticated email attacks. From inspections that check for disqualifying factors, such as DNS authentication and spam, to in-depth analyses that detect tactics like impersonation, malicious URLs, and weaponized attachments, X1 Precision Detection applies inspections in real time to keep communications protected without impacting productivity. The visibility that Mimecast gains by applying these inspections to nearly 1.3 billion emails daily gives us the industry's most robust view of the email threat landscape.

X1 Service Fabric

Cloud-delivered security at scale

The Mimecast X1 Service Fabric is the cloud-native infrastructure that powers the Mimecast Product Suite. Providing a reusable set of platform capabilities, it allows Mimecast to deliver an integrated product suite at scale, accelerates the development and deployment of new capabilities, and provides the resilience and reliability that today's threat landscape demands. By enabling the consistent application of protections across users and applications and allowing customers to grow securely and seamlessly, X1 Service Fabric provides the foundation for cloud-delivered security at scale.

X1 Service Fabric includes the following key components:

Global Policy Engine

As organizations continue to increase the number of communications and collaborations tools their employees use, standardizing security policies across these systems is becoming increasingly critical. In fact, doing so is essential — for creating a cohesive security strategy, for reducing manual effort, for supporting compliance efforts, and for reducing risk. The X1 Global Policy Engine dramatically simplifies the process of establishing policies that can follow end users, keeping them protected however they may communicate or wherever they may collaborate. With a "create once apply everywhere" approach, the X1 Global Policy Engine takes the complexity out of policy creation, giving organizations the ability to consistently protect end-users anytime, anywhere and providing the customization and flexibility to meet their organization's unique needs.

Elastic Infrastructure

The X1 Platform's Elastic Infrastructure powers a cloud-native platform that provides secure multi-tenancy, scalability, and resilience. By allowing Mimecast to provision efficiently and securely across our customer base, it delivers high performance at the lowest possible cost for our customers, while supporting continuous optimization of our detection capabilities and rapid innovation.

Software components are built to be flexible and extendable, allowing them to be repurposed and reimagined as customer needs and the threat landscape changes, reducing time-to-market for new development initiatives and accelerating time to value. Customers can also rapidly scale their businesses as needed, knowing that Mimecast will provide the reliability and resilience that today's threat landscape demands.

Identity Assurance

A key component of managing risk while also protecting productivity is understanding and controlling who and what is accessing communications tools — when, from where, and how. The X1 Platform centralizes and simplifies identity assurance across the Mimecast Product Suite, providing consistent application of permissions across products based on identity, role, and authorization for individuals, organizations, and systems. By associating events with identities and capturing information that can be ingested and analyzed using the Data Analytics component of the X1 platform, Identity Assurance can help create an early warning system, allowing IT and security teams to act quickly to shut down attacks not just within email or collaboration tools but across their entire network.

X1 Data Analytics

Actionable information, distributed intelligence

X1 Data Analytics provides a platform for ingesting, correlating, and querying the mass volumes of data that Mimecast generates from the process of protecting every organization's most vulnerable point — the intersection of communications, people, and data. Providing the foundation for a wide array of services and capabilities — from the discovery/analysis of new threats and accelerated product innovation to rich context for threat researchers and support for cross-correlation of data with systems beyond email — X1 Data Analytics is built with one primary goal in mind: making information actionable.

X1 Data Analytics includes the following key components:

Events, Telemetry, & Context

Securing communications, people, and data is a complex process that generates massive volumes of data that most often sits in silos, making it difficult or impossible to connect the dots and leverage this treasure trove of information. X1 Data Analytics provides the foundation for automating the capture of data from an unlimited number of sources and making that data easily accessible in near real-time from a single platform. From threat information and logs to communications-related events like emails sent and received, files accessed, and URLs clicked, X1 Data Analytics can ingest data at scale — efficiently and reliably — to feed data correlation, support queries, enable automated response, and ultimately, to serve as the foundation of the X1 Service Fabric.

Data Correlation Analytics

Capturing data is one thing, but making it valuable is another matter entirely. That's why X1 Data Analytics incorporates unlimited, simultaneous, and sequential data processing that allows ingested data to be connected in near real-time and enables systems to respond to and share data sets with each other. The result is connective tissue within Mimecast's own solution suite and with other technologies that allows us to see the whole picture, communicate findings across the whole security ecosystem, and power data-driven decisions that deliver faster, better protection.

Search & Query

As organizations deploy more applications and services — from collaboration tools to data sharing and meeting applications — the amount of data generated continues to grow exponentially. The ability to get the right data for a particular use case or application has become complex and time-consuming as a result — so much so that the vast majority of data sits unused. X1 Data Analytics is purpose-built to change that dynamic. By organizing mass volumes of data into granular streams with powerful aggregation and query capabilities, it allows an infinite number of consumers (e.g., Mimecast products, other security products, services, SOC teams) to simultaneously access data for an infinite number of uses cases. Whether the data required is broadly historical or tightly time-bound; granular or holistic; cross product; cross tenant, cross geo, or all of the above, X1 Data Analytics can deliver back the specific information each consumer needs in near real-time, opening up unlimited possibilities for innovation, insights, and automated response/remediation.

MESH

Mimecast Extensible Security Hooks

Mimecast Extensible Security Hooks (MESH) provide a well-documented, consistent API gateway that enables third-party integrations of all kinds, allowing threat data, policies, and practices to be applied or shared programmatically with other security and data solutions. Integration of Mimecast with other systems is fast and easy, opening up endless opportunities for organizations to leverage threat intelligence from email (the top attack vector), automate tasks, improve visibility, and accelerate detection and response.