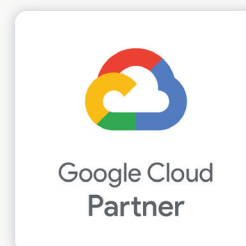


Partnerships and Integrations

Our partners integrate with or leverage Ionic to deliver scalable data security and access control to organizations. Ionic's portfolio of integrations with leading technology partners, system integrators and consultants will help you win more customers to drive revenue.

Deep, Unmatched Integration Across Major Cloud Platforms



ISVS AND TECHNOLOGY ALLIANCE PARTNERS



AWS

Ionic Machina provides unified data security and access controls at enterprise-scale, delivering dynamic authorization to control the security of your data stored in Amazon S3 from an external system. Centralized RBAC/ABAC policies coupled with encryption key management are leveraged to deliver just-in-time authorization decisions in cloud or hybrid environments. Machina can be procured from the AWS Marketplace, which includes our GovCloud option.



BigID

BigID leverages data intelligence to provide organizations the ability to discover and manage personal and sensitive data across the entire data ecosystem for privacy, protection, and perspective. BigID's approach enables enterprises to better understand and classify their data, while Ionic leverages the BigID Data Intelligence to automatically assign and apply data security controls driven by Data Residency, Data Sensitivity, and Personal Data Attributes findings for consistent policy enforcement across multiple deployment architectures. The partnership delivers a consolidated approach for sensitive data protection and security enforcement and an automated model to mitigate compliance, privacy, and security risks throughout the entirety of the data lifecycle.



Google Cloud External Key Manager (EKM)

Machina for Google Cloud EKM enables you to create, store and manage your own encryption keys outside of GCP's infrastructure. You can now control the security of and access to your data in BigQuery and resources in Compute Engine, such that you can even deny Google the ability to decrypt your data for any reason. Machina consistently enforces access control policies across hybrid or cloud environments. From a single interface you can implement external encryption key management, attribute-based access controls, real-time policy enforcement, and auditable visibility across your organization.

Google Cloud Storage

Google Cloud Storage provides best in class performance and reliability through unified object storage for developers and enterprises, from live data serving to data analytics/ML to data archiving. Google Customer-Supplied Encryption Keys, or CSEK, is an offering for customers with stricter regulatory needs, or a need to provide their own key. Machina for Google Cloud Storage allows you to easily manage these keys in a scalable way and apply consistent access policies across any environment.



HyTrust

HyTrust provides solutions that automate security controls for software-defined computing, networking and storage workloads to achieve the highest levels of visibility, granular policy control and data security. HyTrust and Ionic work together to allow customers to accelerate cloud and virtualization cost savings, while improving their security posture by automating and enforcing real-time security policies, adapting quickly to compliance requirements, and preventing unplanned outages.



IBM Cloud

Red Hat is the world's leading provider of open source solutions. Red Hat helps more than 90% of Fortune 500 companies solve business challenges, align their IT and business strategies, and prepare for the future of technology. Red Hat does this by providing enterprise-grade solutions through an open business model and an affordable, predictable subscription model. Ionic has certified Red Hat Enterprise Linux (RHEL) 7 as a commercially supported operating environment for Ionic Machina. We are proud to work with Red Hat to deliver data security, access control, and data handling visibility on the world's leading open source operating system for the enterprise.



Intel SGX

Ionic Secure Files™ with Intel® Data Guard extends Ionic Secure Files and Folders technology by using the Ionic Machina and Ionic SDK to directly integrate with Intel® Data Guard technology. This provides hardened crypto functionality using Intel® Software Guard Extensions (Intel® SGX) at the endpoint, ensuring that the keys remain protected both at rest and in use. Using Ionic Secure Files™ with Intel® Data Guard, employee files, including Microsoft® Office & Adobe® PDF documents, are automatically encrypted and remain protected on IT-managed PCs when stored locally, in the cloud, or on a USB drive.



Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 225,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts.



Kudelski Group

The Kudelski Group is a world leader in digital security and convergent media solutions for the delivery of digital and interactive content. Their expertise in digital device and chip technology support your embedded security assessment needs and protect your bottom line throughout your video content device deployment. Leveraging the Ionic Machina, you can now continuously control video and IoT data streams with greater flexibility and persistent security in real-time.



McAfee Skyhigh

McAfee Skyhigh Security Cloud™ helps the world's largest organizations unleash the power of the cloud by providing real-time security for enterprise data and users across all cloud services. Together, Ionic Security and McAfee Skyhigh deliver a solution that enables enterprises to not only secure their data, but trust in its privacy, wherever that data may go.



Microfocus

Ionic's Machina provides a wide range of control for logging events related to data security and access control activities. The Smart Connector integration enables enterprises to consume and process those events with Micro Focus ArcSight.



Microsoft

Ionic Machina enables external authorization management for Azure Blob Storage and AIP services—with unified access controls, access policy and encryption key management—to deliver consistent access decisions in cloud and hybrid environments. Organizations can implement consistent RBAC/ABAC data handling policies with full visibility of data activities and authorization transactions.



Palo Alto Networks

Ionic and Palo Alto Networks have integrated our platforms to provide recognition and rule-based response to Ionic-secured data in the Palo Alto Networks Next Generation Firewall. With this integration, customers will be able to quickly and easily enforce policies for sensitive data handling when passing through the firewall.



Privitar

Privitar empowers organizations to use sensitive data to gain valuable insights, and to support data-driven decisions. By delivering comprehensive data privacy techniques and streamlining data provisioning, Privitar enables enterprises to extract the maximum value from the data they collect, manage and use, while minimizing risk.



ReversingLabs

ReversingLabs delivers game changing threat detection and analysis solutions. The integration of ReversingLabs' TitaniumScale File Analysis with Ionic Machina improves the management of file analysis results as part of an organization's malware security profile. TitaniumScale customers building file lakes in the cloud or on-premises can now use Ionic's automated and scalable key management technology and granular access control policies to securely store and manage file content based on classification and risk level.



Sentris

Ionic Machina allows Mantech's Sentris product to deliver the highest levels of security, enabling DevSecOps to remove barriers and cut across silos when developing cloud- and web-enabled software for entities in the public sector. The integration supports Microsoft Office Suite and provides an endpoint O365 files/document solution that is powered by the data encryption, policy enforcement and dynamic authorization capabilities of Machina.



Splunk

Splunk's market-leading platform powers Operational Intelligence and has pioneered innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 10,000 customers in over 100 countries use Splunk software and cloud services. Ionic's integration with Splunk Enterprise allows Splunk customers to capture detailed Ionic data access telemetry, and manage it through their powerful Splunk searching and reporting capabilities. It leverages the Splunk "REST TA" Module, and is fast and easy to set up and use.



TITUS

TITUS enables organizations to classify, protect, and confidently share information. Classification is foundational for data security, as it helps both technology and people make decisions on how to handle data appropriately. TITUS integrates with Ionic Machina to combine data classification with data security from Machina for Outlook email, Microsoft Office documents and sensitive files stored in cloud and on-premise data repositories. Flexible policy rules define access to sensitive data, based on attributes using TITUS Data Classification and TITUS Data Discovery, ensuring that only the right users have access to data, from the right devices and at the right time.



Virtru

More than 8000 organizations trust the Virtru Data Protection Platform to easily protect and control sensitive information regardless of where it's been created, shared, or stored. The Ionic Security and Virtru partnership builds on an increasing market demand to secure email communications for enterprises, their vendors, and 3rd party customers and collaborators. The solution extends Ionic Machina, the only dynamic authorization engine, to Virtru, enabling organizations to encrypt emails and email attachments end-to-end, from any platform, with customer-hosted keys managed centrally in Machina.



Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services.



Alpharetta Consulting

Alpharetta Consulting provides expert technology advisors to Fortune 500 companies in the United States, specializing in helping clients prepare for, implement, and remediate complex application development projects, that enable clients to realize the expected benefits of their technology investments.



Cloud Rush

Cloud Rush is a cloud services company dedicated to helping organizations navigate their digital transformation journey. Because the cloud is more than a new technology — it’s a total paradigm shift. To create outstanding results for clients, Cloud Rush reinvents business models, innovates new customer experiences, and digitizes processes, to enable enterprises process oceans of data, develop predictive apps by integrating machine learning recommendations, and learning how to operate it all using industry best practices.



Norseman Defense Technologies

Norseman Defense Technologies has over 23 years of success as an Information Technology provider and Systems Integrator delivering best of breed solutions that solve our Federal customers IT problems. Based in Elkrige, MD, Norseman prides itself in solving real customer problems in the areas of DevOps, Cloud Migration, Cyber Security, Enterprise Data Management, and Data Analytics.



Sagence

Sagence is a premier advisory services firm specializing in data management and analytics. Sagence works with clients to extract value from their data assets by implementing innovative techniques that complement traditional data management methodologies. Together Sagence and Ionic provide a data-centric security framework that enables enterprises to share data in a secure and controlled manner.