HFS

HOT TECH

HFS Hot Tech: Eclypses

Authors:

Akshat Tyagi, Associate Practice Leader

Joel Martin, Executive Research Leader and Chief of Staff

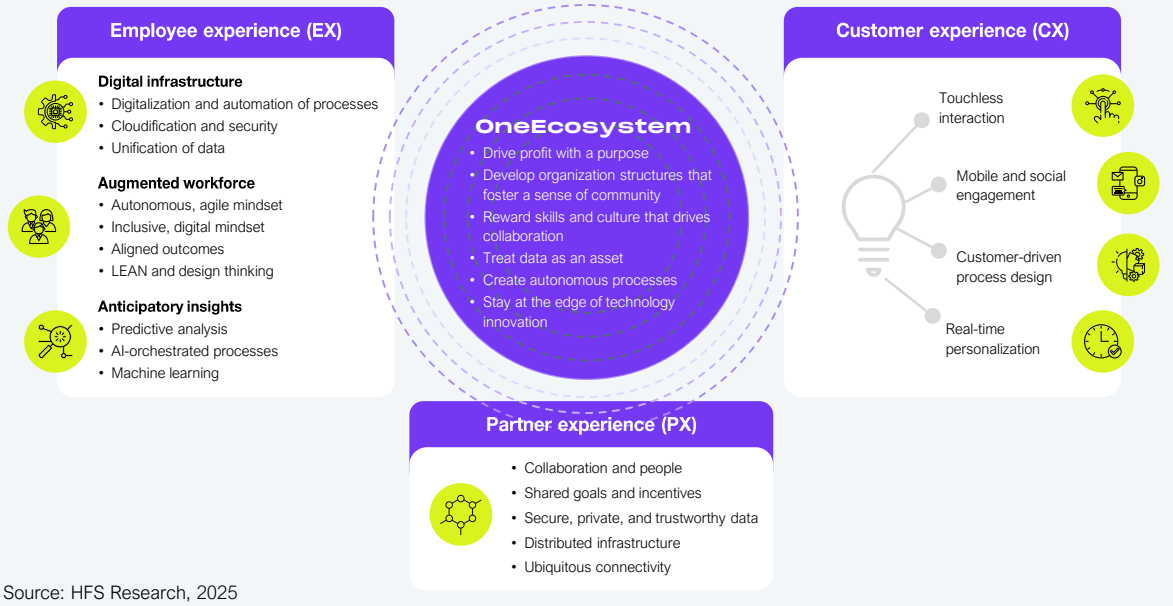
Hot Tech Program Lead:

David Cushman, Hot Tech Editor-in-Chief, Executive Research Leader

Executive summary

HFS Hot Tech are an exclusive group of emerging players, each with a differentiated value proposition for the HFS OneOffice or HFS OneEcosystem. We selected this Hot Tech for its alignment with the HFS OneEcosystem in Exhibit 1.

Exhibit 1: The HFS OneEcosystem adds partner experience to employee and customer experience



Source: HFS Research, 2025

HFS analysts regularly speak with numerous exciting start-ups and emerging players. We designate a select few as HFS Hot Tech based on their offerings' distinctiveness, ecosystem robustness, client impact, financial position, and, in this case, impact in our OneEcosystem framework. HFS Hot Tech may not have the scale and size required to feature them in our Horizons reports, but they have the vision and strategy to impact and disrupt the market.

In the rapidly changing space of digital operations, enterprises realize they cannot be everything to everyone. Enterprises consuming third-party services, service providers, and technology providers need a smart ecosystem to succeed and survive in the future. HFS Hot Tech are service and technology providers hand-picked by our analysts to help you flesh out your smart ecosystem with offerings that solve today's complex business problems and exploit market opportunities.

HFS Hot Tech display truly differentiated offerings and out-of-the-box thinking that can be inspiring and useful. This report profiles one HFS Hot Tech selected through our rigorous five-step assessment. The HFS Hot Tech designation remains in place for one calendar year.

Every Hot Tech joining our program remains listed on our exclusive and searchable database.

HFS © 2025 HFS Research. All Rights Reserved.

Eclypses redefines data protection for the AI era

Enterprise services are now hybridized and borderless, connecting remote users to digital services through APIs stretching across unmanaged networks, multiple clouds, SaaS platforms, and increasingly AI-based systems. Traditional security tools, built for centralized heritage systems, are challenged to manage data protection in this fragmented reality.

Today's CIO needs solutions built for the modern context of AI and cloud services. They shouldn't be limited to using tools retrofitted from a different era. Today's CISOs are battling their budgetary constraints alongside adversarial actors, and costly credential management and key rotation are avoidable expenses. Tomorrow's CXOs will also need solutions to defend data against Quantum-enabled threats without the legacy tools' operational burden and complexity.

Dealing with a large attack surface in the age of AI

For decades, businesses have relied on sprawling digital ecosystems to deliver real-time, data-driven services powered by interconnected apps and intelligent automation. From a CISO's point of view, the scale of the attack surface has grown exponentially while adding complexity; thus, legacy security models are not optimized for the challenge.

Yet, many organizations still depend on standard security controls such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), virtual private networks (VPNs), key management and rotation, and firewalls. These tools were built to defend a network boundary that no longer exists. Once a bad actor breaches a network session, the data can be exposed, harvested, and compromised. Even with legacy network session-based encryption, skilled hackers can discover the weak links they need to decrypt and expose company and user secrets.

As the growth of AI is driving the usage, distribution, and creation of more data, security leaders must confront a hard truth: they're not adequately protecting the data. They're only protecting the pipes, not the payloads. To change the nature of security, CISOs must find new solutions. HFS has seen how data protection can be embedded within the data rather than the network, in a cloud-native, quantum-safe, and tokenized solution available from Eclypses.

Introducing Eclypses and its MicroToken Exchange (MTE) solutions

HFS previously covered Eclypses [HFS OneEcosystem Hot Vendor: Eclypses] and how we see it challenging the status quo with its MicroToken Exchange (MTE) technology. Eclypses focuses on a critical problem: *How can CIOs ensure their organization's most valuable data is never exposed, even when systems are breached?*

Their MTE solution is a cloud-native, FIPS validated and NIST quantum safe technology that encrypts data in transit at the application layer before it moves across any networked connection.

HFS © 2025 HFS Research. All Rights Reserved.

The value proposition of MTE is its innovative approach to encryption. Rather than statically encrypting data through key-based cryptography, each piece of a message is individually masked, rotated, and then encrypted using constantly rotating, self-managing keys. This approach creates a stream of randomized, unintelligible data packets. Whether data is transmitted over the internet, through APIs, or in a private data stream, the packet's data cannot be read.

HFS believes that MTE can fundamentally elevate an organization's defensive posture. When a network session is compromised, the attacker gains nothing. There's no key to steal, no credentials to replay, and no data to decrypt. It's just a stream of characters that appears as 'digital white noise.'

Legacy controls are failing in a borderless enterprise

Why does that matter if your firm has invested significantly in traditional data and application security? With the advent of cloud, AI, and API-enabled connectivity, the attack surfaces are growing too fast to be economically defended successfully with heritage tools and processes. Technologists, partners, and third parties dynamically create connections across unknowable or unmanaged networks that may inadvertently expose valuable or private data.

Traditional governance and policy frameworks can't keep up with the pace of change in the digital enterprise's interplay of people, architectures, apps, and data. Regulated industries and critical national services cannot abdicate their accountability to deliver safe and secure services for their citizens, consumers, and stakeholders.

As breach reports continue, a compromise in a distant part of a complex supply chain of services rapidly translates into an attack on the data at the enterprise's core.

One organization HFS spoke with described how Eclypses' MTE is helping them improve protection across internal and client-facing systems. The firm processes large volumes of sensitive consumer data and needs to reduce exposure across environments it can't directly control.

> "Removing static credentials and dynamically encrypting every payload helped us solve problems that traditional encryption just couldn't," the company shared.

The team emphasizes that securing data from the point of collection to final delivery was a decisive factor in choosing the Eclypses MTE solution.

HFS © 2025 HFS Research. All Rights Reserved.

Traditional encryption is losing the cyber arms race

Classical cryptography models could not have anticipated the hyper-scale demands of contemporary enterprise architectures, which continue to evolve rapidly:

- APIs have become the architectural standard to connect services and share sensitive data across Tech, applications, and countries.
- Multi-cloud and containerized systems are increasing complexity and reducing the visibility of security control effectiveness.
- Network connectivity has become a commodity service, with unknown or unmanaged levels of security from end to end.
- AI-powered tools such as Claude and GPT-based agents are now acting as agents on behalf of users.
- Quantum computing is approaching the point where legacy encryption will be rendered obsolete.

Enterprises continue to grapple with the operational fragility of certificate-based encryption schemes, where minor lapses in administrative hygiene can block users from accessing critical services. Eclypses offers a solution built for hyperscale systems and modern architectures. MTE removes the need for certificate lifecycle management, key distribution, and secrets rotation by operating at the application layer. Instead, it protects data by default, before it ever moves across a network, eliminating complexity while improving resilience.

The growing failures of certificate-based schemes in enterprise cryptography fail to protect company assets. As emerging AI, agentics, and quantum factors are part of an organization's technology systems, you must refresh how you safeguard your IP and data assets. This means that security must be operable at the application layer, transparent to users, and avoid adding latency to data and communications. With a MicroToken Exchange model, companies may have just what they need.

Eclypses MTE protects data by design—a key to adapting to current and future technology and business changes

MTE embeds protection into the data, transforming it into quantum-safe microtokens generated through a synchronized logic between sender and receiver. Even if intercepted, these tokens appear as meaningless white noise. This ensures the original data remains irretrievable. MTE eliminates the need for traditional key management, reducing both operational overhead and risk exposure.

It is also resilient in real-world conditions. The token stream can recover from disruptions such as dropped packets or message delays, maintaining secure data flow without manual intervention or session restarts.

HFS © 2025 HFS Research. All Rights Reserved.

Deployment models and integration pathways

Eclypses has engineered its platform for real-world use. Its offerings are modular, cloud-ready, and designed to be integrated without requiring an overhaul of existing systems. The core components include:

- **MTE relay server and API relay:** Enable real-time data tokenization in flight across public clouds (AWS, Azure, GCP) and on-prem environments. They can be deployed quickly via cloud marketplaces, including AWS, Azure, and Oracle, and plugged into existing infrastructure with minimal friction.
- **SDKs for mobile and web:** Developer toolkits for iOS, Android, and browser-based apps allow enterprises to embed MTE directly into customer-facing and internal apps.
- **Encryption-as-a-Service (EaaS):** A fully containerized deployment which removes the burden of key management and ensures that each piece of data is encrypted with unique and ephemeral keys, further reducing risk.
- **Eclypses Cryptographic Library (ECL):** A FIPS 140-3 validated module powering MTE's post-quantum capabilities, built with NIST-approved CRYSTALS-Kyber algorithms. This provides forward compatibility with upcoming government and industry compliance requirements.

Where it's working: Real use cases in production

MTE is already being applied in critical environments across industries such as:

- **Financial services:** Protecting sensitive customer data without requiring system re-architecture, while helping institutions align with privacy and regulatory mandates.
- **Healthcare:** Supporting Health Insurance Portability and Accountability Act (HIPAA)-compliant mobile applications where personal health data never exists in readable form on devices or in cloud storage.
- **IoT and smart cities:** Tokenizing sensor data from distributed environments to prevent tampering or spoofing, even over untrusted networks.
- **Blockchain and Web3:** Protecting high-value transactions in decentralized environments where trust is hard to establish and easy to lose.
- **Election technology:** Ensuring mobile voting data is secured from source to destination, including against future decryption by quantum attackers.

In all of these examples, Eclypses' appeal lies in its ability to let enterprises adopt next-gen architectures such as AI, edge, and multi-cloud, without relying on legacy encryption models.

HFS © 2025 HFS Research. All Rights Reserved.

HFS' take

Eclypses challenges traditional enterprise security approaches by shifting protection to the application layer and replacing sensitive data with instantly obsolete microtokens. This model moves beyond outdated reliance on TLS, VPNs, and perimeter defenses. It offers a modern, cloud-native approach that aligns well with API-driven, containerized, and zero-trust environments.

Where most encryption solutions introduce operational complexity, Eclypses simplifies implementation. Its lightweight, cloud-native architecture provides fast integration and self-contained cryptographic libraries that reduce the friction associated with transformation. For CISOs managing expensive credential systems and frequent key rotations, Eclypses enables a move toward zero key and credential management. This helps streamline policies and lower operational costs while maintaining strong security. Elcypses offers **risk elimination, not just mitigation**—moving beyond 'reducing' threats to entirely removing entire risk classes.

This is not just about preparing for a quantum future. Eclypses provides a tangible advantage today. Organizations looking to scale AI and data protection, accelerate cloud-native adoption, and minimize dependence on brittle infrastructure can benefit from its practical and deployable solution.

HFS believes Eclypses presents a highly differentiated offering that addresses long-standing challenges in enterprise data security. Its model can potentially support digital-native businesses and large enterprises facing complex legacy environments. The company's path forward is helping the market see that a more secure and simplified option is already available and effective in live environments.

Vendor fact sheet

- **Founded:** 2017
- **Headquarters:** Boston, US
- **Key executives:** David Gomes (CEO), Larry Murray (CRO),Jeff Dance (CIO), Tim Reynolds (CDO), Dan Lemoine (VP of Operations), Adam McElroy(Principal Architect)
- **Number of employees:** <50
- **Funding source:** Private high-net-worth individual investors, amount not disclosed.
- **Number of clients:** Approximately 50
- **Key clients:** WILLPORTtrust, WholesalePayroll, global social platform provider, large insurance and financial services firm, US Federal Gov't agencies
- **Domain:** Security Software, Cybersecurity, Cloud-Native Applications
- **Solutions portfolio:** Eclypses Cryptographic Library (ECL), MicroToken Exchange (MTE), Managed Key Encryption (MKE), Secure Data Replacement (SDR), Eclypses MTE Relay Server, Eclypses API Relay, RST
- **Industry Application:** Available across all industries

HFS © 2025 HFS Research. All Rights Reserved.

The HFS Hot Tech report team

Authors



Akshat Tyagi
Associate Practice Leader

Akshat Tyagi is an associate practice leader at HFS Research, specializing in cybersecurity and emerging technologies such as Web3, blockchain, quantum computing, and XR.

He brings more than eight years of experience as a research analyst at Protiviti, Gartner, and EY, advising C-suite leaders on cybersecurity strategies.



Joel Martin
Executive Research Leader and Chief of Staff

Joel Martin is the executive research leader and chief of staff for enabling tech research on software development and the TMT industry practice for HFS Research.

He has nearly three decades of experience as an analyst, consultant, software product manager, and marketing professional.

Hot Tech Program Lead:



David Cushman
Hot Tech Editor-in-Chief, Executive Research Leader

David is an Executive Research Leader at HFS and Editor-in-Chief of the HFS Hot Tech program. He also leads our OneOffice™ Emerging Technology Practice, is our strategic lead on Generative AI, Web3, and metaverse, and covers automation and employee experience. He is a published author (*The 10 Principles of Open Business*, Palgrave-Macmillan), a former tier-1 consulting director, and a digital strategy and innovation expert with leadership experience in start-up, scale-up, and enterprise digital transformation.

HFS © 2025 HFS Research. All Rights Reserved.

HFS

About HFS

- **INNOVATIVE**
- **INTREPID**
- **BOLD**

HFS Research is a leading global research and advisory firm helping Fortune 500 companies through IT and business transformation with bold insights and actionable strategies.

With an unmatched platform to reach, advise, and influence Global 2000 executives, we empower organizations to make decisive technology and service choices. Backed by fearless research and an impartial outside perspective, our insights give you the edge to stay ahead.


www.hfsresearch.com


hfsresearch


www.horsesforsources.com


www.horsesmouthpodcast.com