Identity Defined Security is a novel term, but not necessarily a new idea. Applications have been moving toward securing data through identity information for some time, now, but the weakness of a simple one-factor password to secure a user’s identity has been proven again and again. While organizations continue to attempt to tie identity to security, the practice often has been limited to traditional mechanisms which simply don’t provide enough assurance that personal or corporate information and data is secure. This document describes the vision, mission and strategy of a combined technology alliance that provides a holistic view of a complete solution which leverages identity for security from the user to the device to the application.

“Whether it’s creation of an authentication ceremony, definition and enforcement of policy, enforcement of those policies at APIs or code samples for mobile app writers, the requirements necessary to perform true IAM encompass numerous software and service entities across numerous domains.”

- Pam Dingle, Senior Technical Architect
  Office of the CTO, Ping Identity
The practice of identity and access management (IAM) has been around for as long as the Internet, but it has become so complex, and the challenges so numerous, that the term has become rather ambiguous.

A new way of thinking about IAM is needed, and defining security through identity from beginning to end provides a clear alternative to denying access by default, which, while still an overriding rule in security, provides little comfort in our present breach-a-week reality.

The Identity Defined Security Alliance is a partnership between leading, best-of-breed technology vendors to provide a complete solution blueprint and best practices for a comprehensive security platform. This platform goes beyond passwords and beyond traditional IAM to ensure that trusted users can seamlessly and securely access the right data using the right applications on trusted devices from anywhere.

“It’s critical for companies to understand where identity fits into their broader strategy to ensure secure access to data across the business. By partnering with the Identity Defined Security Alliance, Optiv will be able to develop and quickly bring to market solutions that more seamlessly integrate identity into our clients’ environments.”

- Robert Block, Vice President of Client Solutions
  IAM for Optiv
At the intersection of web, mobile, cloud and the Internet of Things (IoT), ensuring that trusted employees, partners and customers can access the right data using the right applications on the right devices is the only way to provide complete enterprise security while enabling fluid, efficient interactions.

IAM requires huge amounts of coordination and integration as well as specific expertise in discrete areas of identity security in order to provide the assurances that customers and businesses demand. Identity federation and single sign-on (SSO) are expected, but so are identity security and the protection of private data and personal information. The requirements range from enterprise needs for workforce security and data loss prevention to the protection of credit card and customer information to federally mandated privacy rules such as those required by HIPAA. Securing all of these types of users, assets and data is a massive task and requires a paradigm shift in enterprise security.

IDENTITY DEFINED SECURITY

Identity Defined Security makes it possible to provide a more secure environment by putting identity at the center of the security architecture. This evolution in IAM solves the complex enterprise challenges imposed by cloud mobile, and IoT trends by providing a steel thread across existing and emerging security technologies, allowing users to securely navigate across borders. Is it simple? No. Is a single vendor able to provide a comprehensive solution for securing workforce, partner and customer identities—and the ability for CISOs and admins to sleep well at night? No. The problem is simply too big. However, by combining best-of-breed solutions with best practices and blueprints for integrating these solutions, the alliance provides a clear method for weaving this thread of Identity Defined Security into any organization’s infrastructure.

The six design principles of Identity Defined Security are:

- All identities: designed for employee, customer, and partner use cases
- Federated architecture: assume resources are outside your network perimeter
- Built on standards: improve interoperability, speed integration and prevent vendor lock-in
- Web, mobile and APIs: secure all resource types, including future IoT resources
- Internet scale: build for millions of identities by focusing on automation
- Flexible deployment: deploy where necessary, in the cloud, data center or both
TODAY’S SECURITY CHALLENGE

THE MISSION OF THE ALLIANCE

The mission of the Identity Defined Security Alliance is to accelerate the vision of the digitally transformed enterprise, where secure access from anywhere is possible for workforce, partners and customers. Additionally, the alliance aims to reduce the pain and confusion inherent in creating a best-of-breed Identity Defined Security platform by defining blueprints and best practices that streamline the implementation patterns. The alliance helps customers secure their assets while enabling the correct access for the right people and applications, and further to determine when the wrong authorization or access has occurred—and quickly provide resolution. The alliance is a collaborative coalition that aspires to accomplish this mission with the ultimate goal of achieving a more secure, connected world.

THE BENEFITS OF THE ALLIANCE

The Identity Defined Security Alliance is made up of vendors that provide proven products that have been integrated to solve real-world problems. Beyond technology, the alliance provides a set of blueprints, best practices and detailed use cases that describe and help implement a comprehensive platform.

The integration points detailed by the alliance give customers and prospects a jump start on determining how solutions from the alliance members can fit into existing infrastructures, allowing the blueprints and the vendor solutions to be leveraged in both greenfield projects as well as legacy environments.

By ensuring that members provide real value to their customers as part of an integrated platform, the alliance makes it easy for customers and prospects to determine what gaps might exist in their existing security practice, quickly determine and evaluate the vendors that can fill them and implement solutions that provide the fastest time to value.
The framework for the alliance is driven by the current needs of customers and by evaluating the most pressing issues in identity security today. This framework incorporates solutions for the following high-level categories:

ACCESS MANAGEMENT

Identity federation and SSO provide standards-based access to every application through trusted relationships using a single password, multi-factor authentication uses contextual data to determine and enforce the correct level of user identity validation for mobile and token-based authentication (MFA) and web and API access security enables group and attribute-based, policy-driven access management for web applications and APIs, on-premises and in the cloud.

ENTERPRISE MOBILITY MANAGEMENT (EMM)

Container management providing complete separation of corporate and personal data, mobile device management for simplified control of devices, mobile application management for acquiring, distributing, securing and tracking mobile apps, and mobile content management for secure mobile access to content.

CLOUD ACCESS SECURITY BROKERS (CASB)

On-premises or cloud-based security policy enforcement points between users and service providers that build and enforce enterprise security policies as resources are accessed.

FRAUD, RISK AND THREAT ANALYTICS

Predictive analytics to find and prevent fraud, correlate security incidents from disparate sources and ensure compliance with corporate and industry regulations.

PRIVILEGED ACCOUNT MANAGEMENT (PAM)

Centralized management and deployment of credential updates to systems and applications across the enterprise, time-limited, privileged credential control and account policy compliance and audit.
USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

Security intelligence that leverages machine learning to quickly discover actors and systems that exhibit uncommon behavior, detect advanced attacks, prioritize incidents and guide effective response.

ALLIANCE CATEGORIES AND MEMBERS

ACCESS MANAGEMENT

ALLIANCE MEMBER AND FOUNDER: PING IDENTITY

Contextual MFA is becoming a requirement in the modern enterprise. Utilizing the right level of authentication for given users, groups or applications and driving the decision by evaluating contextual user data provides the highest levels of security and the least amount of friction for users, regardless if they're workforce, partners or customers. Combining MFA with identity federation and SSO is also a requirement for enterprises today in order to increase security and productivity as well as provide audit and compliance. Web and API access security that leverages attribute-based access control completes this user interaction process and provides Identity Defined Security from beginning to end.

Ping Identity is the leader in Identity Defined Security for the borderless enterprise, allowing employees, customers and partners access to the applications they need. Protecting over one billion identities worldwide, Ping Identity ensures the right people access the right things, securely and seamlessly. More than half of the Fortune 100 trust Ping Identity to solve modern enterprise security challenges created by their use of cloud, mobile, APIs and the IoT.
ALLIANCE CATEGORIES AND MEMBERS

SOLUTIONS PROVIDER
ALLIANCE MEMBER AND CO-FOUNDER: OPTIV SECURITY

With Optiv as the premier solutions provider partner, the alliance takes a formidable step. Optiv is a leading provider of cyber security services and integrated solutions that help organizations address their full range of cyber risk and security needs in a customized and integrated fashion through a holistic, lifecycle and strategic approach. For the alliance, Optiv plans to build out in the company’s client lab a reference architecture focused on demonstrating the value of identity data across other areas of cyber security, create packaged integration solutions and service bundles, and educate the industry on identity-related issues.
ENTERPRISE MOBILITY MANAGEMENT

ALLIANCE MEMBER: VMWARE®

The definition of EMM, continues to evolve. In 2014, Gartner changed their mobility Magic Quadrant from mobile device management, or MDM, to EMM, essentially expanding the functionality that mobility management vendors are expected to provide and defining a baseline for the capabilities of a complete EMM solution.

In the mobile cloud era, users are accessing corporate resources increasingly from corporate and personally owned laptops, tablets and smartphones, and are more likely than ever to be outside the firewall. Meanwhile, the form factor, sensor integration and simplicity of modern mobile devices represents new opportunities for transforming business processes, putting crucial information in employees’ hands when they need it and creating new ways to interact with customers. Successful adoption of this new, mobile-cloud digital workspace requires a simple user experience with application provisioning and one-touch access to apps, but the threats to data loss are also only a touch away. Creating a secure chain of trust between the user, their device, the OS vendor and the enterprise is enabled by registering a device with EMM. This chain of trust exposes device attributes and compliance rules to conditional access policies while automating out-of-compliance escalations.

VMware offers market-leading digital workspace solutions for business mobility including AirWatch Enterprise Mobility Management, Horizon virtual desktop and application management and the integrated VMware Identity Manager for mobile-cloud and virtual apps that is fully interoperable with existing identity management solutions. AirWatch is the global leader in enterprise-grade mobility solutions across every device, every operating system and every mobile deployment, and has been named a leader in Gartner’s mobility management Magic Quadrant five years running.
The explosion of software as a service (SaaS) over the past few years has created the need for a central control point that offers a wide range of security capabilities specific to these cloud-based applications. These capabilities include application discovery, granular access control for sanctioned and unsanctioned applications, data loss prevention (DLP), anomaly detection and application auditing.

This combination of requirements has given rise to the CASB, an on-premises or cloud-based security policy enforcement point that operates between users and cloud service providers to provide visibility and control for cloud-based applications. Netskope is the leading CASB available today. With surgical, or fine-grained, visibility and control for both sanctioned and unsanctioned apps, advanced “noise-cancelling” DLP that reduces false positives and increases detection accuracy and a variety of deployment options, Netskope mitigates risk and enforces cloud access policies in a holistic way, with or without an agent. Netskope is a Gartner Cool Vendor, a top 10 CIO Magazine cloud security company and has been featured in key media outlets including CBS News, the Wall Street Journal and Forbes.
IDENTITY, BEHAVIOR AND THREAT ANALYTICS

ALLIANCE MEMBER: THREATMETRIX®

Another benefit of taking an identity-centric approach to security is that contextual identity data can provide simpler access to critical applications and data, freeing users from strict, static rules but still providing a high level of assurance of the user’s authenticity.

In order to provide this kind of contextual authentication and dynamic access control, however, strong identity, behavior and threat analytics are required.

Applying behavioral analytics and machine learning to find and prevent fraud and the ability to correlate security incidents from disparate sources as well as ensure compliance with corporate and industry regulations are key capabilities of a complete Identity Defined Security solution. Providing a rich profile of device behavior and the associated users’ behavior without any downloads, containers, or other end-user restraints ensures a frictionless experience for workforce, partners and customers.

ThreatMetrix is the market-leading cloud solution for authenticating digital personas and transactions on the Internet. Verifying more than 15 billion annual transactions supporting 15,000 websites and 4,000 customers globally through the ThreatMetrix Digital Identity Network, ThreatMetrix secures businesses and end users against account takeover, payment fraud and fraudulent account registrations resulting from malware and data breaches. The ThreatMetrix solution is deployed across a variety of industries, including financial services, e-commerce, payments and lending, media, government and insurance.
PRIVILEGED ACCOUNT MANAGEMENT

ALLIANCE MEMBER: LIEBERMAN SOFTWARE™

In today’s modern enterprise, administrators, developers and other high-risk users need access to systems from anywhere at anytime. Managing the credentials of these users and ensuring that an attacker hasn’t compromised these “keys to the kingdom” is a required capability for enabling Identity Defined Security.

Lieberman Software simplifies the management of privileged credentials, delivering automated protection against attacks that penetrate the network perimeter. By providing continuous credential rotation and real-time automated response, organizations can protect their environments against the most sophisticated threats. Lieberman Software’s Adaptive Privilege Management Platform provides the right access to the right users without introducing risk and protects access to sensitive systems and data regardless of where those systems live and where users are accessing them from.

In addition to automatically deploying credential updates to systems and applications across the enterprise, Lieberman’s solution also provides time-limited access to privileged credentials, enforces corporate policies with centralized management of credentials and provides full audit capabilities across the enterprise.
ALLIANCE CATEGORIES AND MEMBERS

PRIVILEGED ACCOUNT MANAGEMENT - ALLIANCE MEMBER: LIEBERMAN SOFTWARE

In today’s modern enterprise, administrators, developers and other high-risk users need access to systems from anywhere at anytime. Managing the credentials of these users and ensuring that an attacker hasn’t compromised these “keys to the kingdom” is a required capability for enabling Identity Defined Security. Lieberman Software simplifies the management of privileged credentials, delivering automated protection against attacks that penetrate the network perimeter. By providing continuous credential rotation and real-time automated response, organizations can protect their environments against the most sophisticated threats. Lieberman Software's Adaptive Privilege Management Platform provides the right access to the right users without introducing risk and protects access to sensitive systems and data regardless of where those systems live and where users are accessing them.

In addition to automatically deploying credential updates to systems and applications across the enterprise, Lieberman’s solution also provides time-limited access to privileged credentials, enforces corporate policies with centralized management of credentials and provides full audit capabilities across the enterprise.

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA) - ALLIANCE MEMBER: EXABEAM

UEBA is a rather recent addition to the arsenal of tools available to security professionals, but it’s proving to be more and more valuable as traditional security perimeters continue to erode. Instead of relying on static and manually configured rules to detect anomalies in user and endpoint behavior, UEBA systems leverage machine learning to quickly discover actors and systems that exhibit uncommon behavior, which often indicates that an account or endpoint has been compromised.

In a 2015 market guide on UEBA, Gartner predicted that “over the next three years, leading UEBA platforms will become preferred systems for security operations and investigations at some of the organizations they serve.”

Exabeam is a leading provider of UEBA, enabling customers to detect and prevent attacks that historically would have taken intense, manual inspection of rules, logs and events. Exabeam’s behavior-based security intelligence connects user activities across multiple accounts, devices and locations, highlighting risky user profiles so that security teams can respond to incidents quickly—with full visibility into the event and the systems that were affected.
CONCLUSION

The vision of the Identity Defined Security Alliance is to empower organizations with best-of-breed solutions that enable secure interactions without relying on traditional, rigid, enterprise boundaries.

By providing documented use cases and examples of logical integrations that span every aspect of identity and access security, the alliance provides a holistic view of a complete Identity Defined Security solution for the modern enterprise. The framework provided here describes the components of the solution, and additional use cases and documented integrations will continue to be developed and shared by the alliance. The categories defined by the alliance may also be expanded as additional requirements and capabilities are combined with the solution.

By weaving this steel thread of Identity Defined Security from best-of-breed solutions and tightly integrated components, the alliance allows users to securely navigate across borders and allows CISOs to have complete control and visibility for all of their assets—and a better night’s sleep.