White Paper

The Evolution of Digital Identity

by Vadim Lander, Identity Security CTO and Distinguished Engineer

Perfect Storm for IAM

In today's business landscape driven by the need to grow and differentiate, enterprises launch new applications and services quickly to take the lead in their business domains. Enterprises want to connect to more people to expand reach and build out their brand and they want to maintain mobile presence to securely connect their customers to their services anywhere, anytime, anyplace—gaining competitive advantage and building customer loyalty.

Security is one of the most critical aspects of such initiatives. Enabling end users to securely access authorized resources, preventing accidental data leakage, and guarding against the misuse of credentials and the hijacking of accounts are some of the biggest concerns a business has when trying to move fast to deliver on objectives.

Consider how we were accustomed to securing web applications. A typical approach was to put a web agent in front of a web app and in the process instantly secure the app by providing user authentication and session management capabilities. This enabled application owners to grow business by developing new web apps, and it ensured secure delivery of apps to different end users (B2C, B2B, B2E) without application developers becoming security experts. The end result is enterprises have a significant amount of resources protected by Web Access Management and federated via SAML.

However, the world has moved beyond having a single web perimeter. In today's multi-channel, API-based, mobile-oriented enterprise, no one truly owns the perimeter. Every business, across different verticals and channels, consumes or produces application workloads that could be running anywhere, and no corporate IT organization can control the new perimeter with traditional methods. Enterprises that need to sustain their business or compete for leadership are undergoing digital transformation efforts to adjust to new business realities and must operate in this new world defined by a multitude of infrastructure and application perimeters.

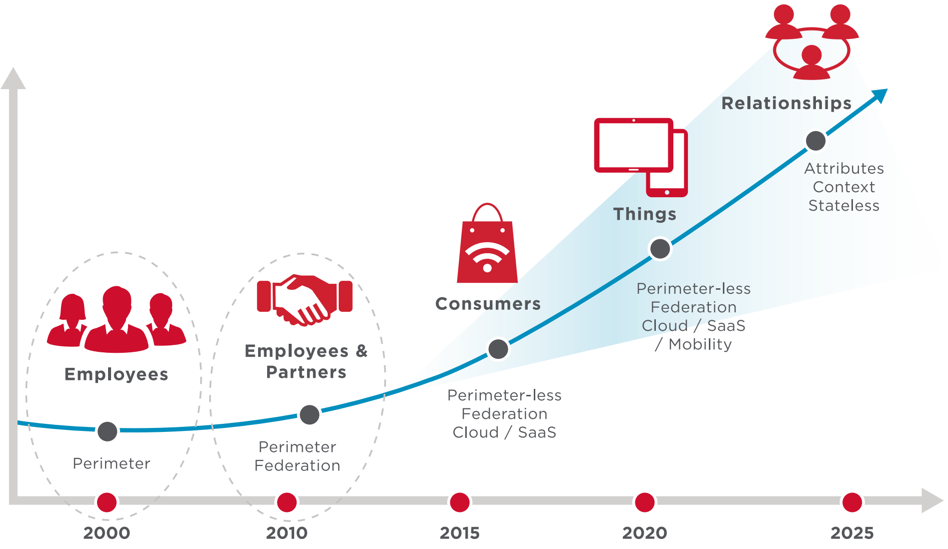
In this world, enterprises have solved the initial authentication use cases using OpenID Connect tokens exchanged for OAuth access tokens, and then rely on each application to validate token claims independently.

This works when everything is working perfectly, but what happens when something goes wrong and there is a security breach? There must be a shared security capability to be able to take action. And there also must be a shared security service platform if users are to get a consistent Single Sign-On/Single Logout experience when accessing resources protected by Web Access Management, federated via SAML in some cases and by OpenID Connect in others. The perimeter-based and multi-perimeter worlds must co-exist for some time with seamless Single Sign-On and Single Sign-Out user experience.

IAM Follows the Apps

The IAM system is responsible for providing omni-channel access to authorized resources, it manages an aggregated view of identities being mapped to applications and systems, and it provides a platform to define and enforce identity

Figure 1: The Evolution of Digital Identity


Employees
Perimeter
Employees & Partners
Perimeter Federation
Consumers
Perimeter-less Federation Cloud / SaaS
Things
Perimeter-less Federation Cloud / SaaS / Mobility
Relationships
Attributes Context Stateless
2000
2010
2015
2020
2025

and access policies to achieve such tasks. A very important consideration an enterprise has is in how to implement a modern IAM for new initiatives, applications, and services.

Enterprises can implement security for each application in a legacy siloed way, or they can leverage a modern platform approach which gives them a shared single identity and policy view across multiple applications and shared services resulting in omni-channel alignment and visibility. The combination of a disappearing network perimeter and an exponential rise of applications being developed using modern application development principles has resulted in enterprises requiring a holistic look at the capabilities of the IAM stack.

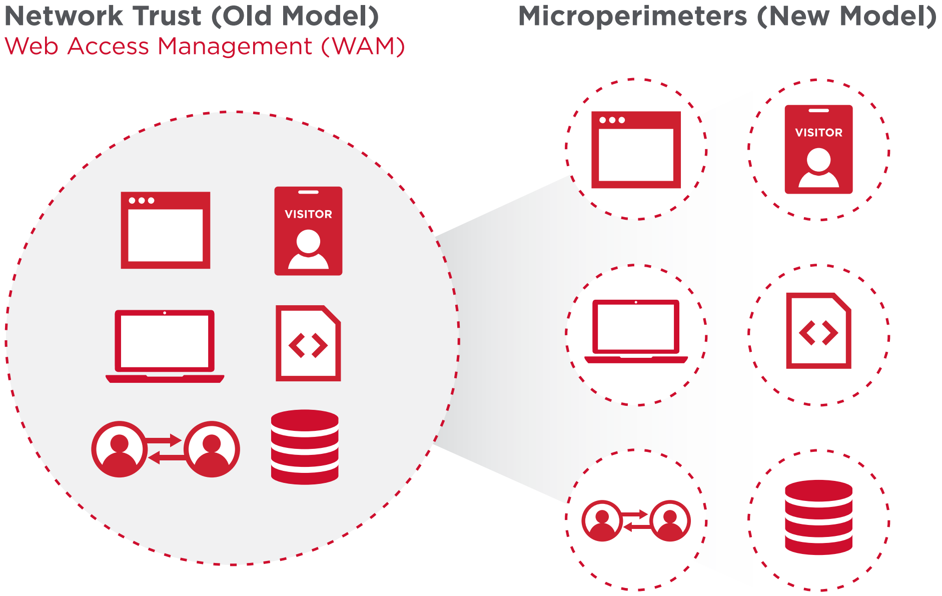
The emergence of federation, cloud, mobile smartphones, and continuous evolution of connected devices are driving a paradigm shift over the enterprise-centric command and control mode of operation.

As shown in the figure below, this results in the single perimeter disappearing around your applications and users, while enabling application workloads to run anywhere, moving away from the central data center—and in the process creating new micro-perimeters.

Securely providing access to applications under such conditions where different micro-perimeters are in play requires enterprises to use dynamic, session-aware, contextual access management that requires as much (or as little) authentication and authorization as necessary to meet the acceptable risk.

The end result is a modern enterprise that must be able to deal with this trend to continue securely delivering applications to end users over any channel, anytime, anyplace —while taking advantage of modern devices to provide excellent user experience. With this trend firmly underway, rooted in enterprise Digital Transformation efforts, application workloads are leaving the central data-center-bound perimeter, and this requires IAM to follow application workloads. The IAM architecture and best practices have to move in that direction as well.

Figure 2: Single Perimeter Gives Way to Microperimeters


Network Trust (Old Model)
Web Access Management (WAM)
Microperimeters (New Model)
VISITOR
VISITOR

With the single perimeter no longer present, a new approach is required to manage the familiar problem of *Who has access to What*. Enterprises must securely connect identities and applications/data across different perimeters using modern protocols and architecture, and this requires a change in how we view IAM.

The Need for Contextual, Omni-present IAM

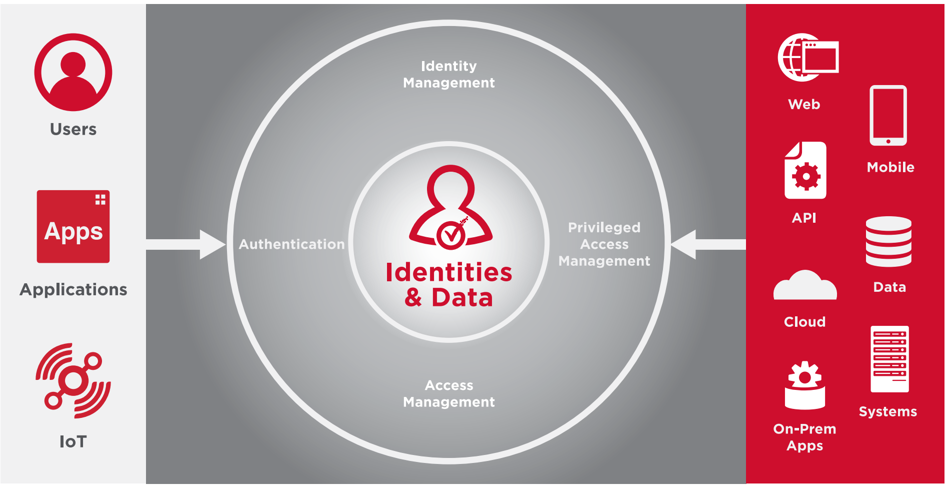
With the Internet being used more and more to transact business via the local data center, SaaS apps, or public cloud, the enterprise no longer owns or controls all the connection points. While enterprises still maintain a perimeter around their data center, the perimeter around the identity and application is no longer in place. Enterprises must be able to securely connect their identities into heterogeneous application infrastructures, and they must be able to securely connect third-party identities into their own application infrastructure.

As mentioned previously, this results in the dramatic increase in the number of perimeters. These new perimeters are no longer around the enterprise data center, but around the User/Session, their Devices, and their Applications.

Let's look at this popular scenario: an employee sometimes works from the office where both the Mac and iPhone are connected to the enterprise's network. During this time the employee is accessing a SaaS-based sales portal to obtain a sales presentation, and he or she is accessing the enterprise's ERP system to submit or approve a purchase order. Occasionally, the employee works from a coffee shop using the local Wi-Fi network and sets up a VPN session to the corporate office.

The risk of exposing sensitive content to malware or some

Figure 3: Identity Is the Perimeter and Must Be Embedded Within These Dynamic Environments



other attacker is greater when the employee is working from the coffee shop and addressing this to adequately mitigate risk requires contextual, risk-based authentication and authorization policy to manage access:

- Where is the user and how is he or she accessing the apps? From the local corporate network, via VPN, or via the Internet?
- How sensitive is the application being accessed? Email, ERP, a company portal, a sensitive SaaS app, and so on.
- How risky is the user's machine/mobile device/network? Does it have known vulnerabilities?

The identity becomes one of the new perimeters, and this identity must be validated at the right level of assurance to access application workloads—and this process must be handled in a way that delivers great user experience. For example, having disparate implementations of authentication systems often results in multiple and annoying authentication challenges causing users to dislike and, in some instances, avoid using such applications.

With the micro-perimeter paradigm now being practically the norm, this means that security and underlying policy should now be based on the context representing the user, their device, their session, and the application with its underlying data.

With users and apps everywhere, access must be provided based on this context including the risk, and access activity must be continuously monitored and adjusted when necessary. IAM must be seamlessly embedded within these dynamic environments as well as protecting micro-perimeters.

What does this mean for the enterprise? As the perimeter continues to disappear, or more correctly morphs into micro-perimeters, enterprises are finding it very difficult to protect corporate data in the presence of micro-perimeters (meaning security silos), and they are struggling to offer a seamless and delightful user experience as users get bombarded with requests for re-authentication.

The end result is that enterprises must ensure that proper risk-based security controls are embedded into the fabric of application perimeters using a range of methodologies such as access proxies, identity federation, native security agents, and direct API calls. The more integrated this architecture is with regard to login flows, central or distributed session management, and consistent risk evaluation across all the micro-perimeters, the better equipped the enterprise is to securely connect users to their applications with the best user experience and least security exposure.

New IAM/Security Architecture Required

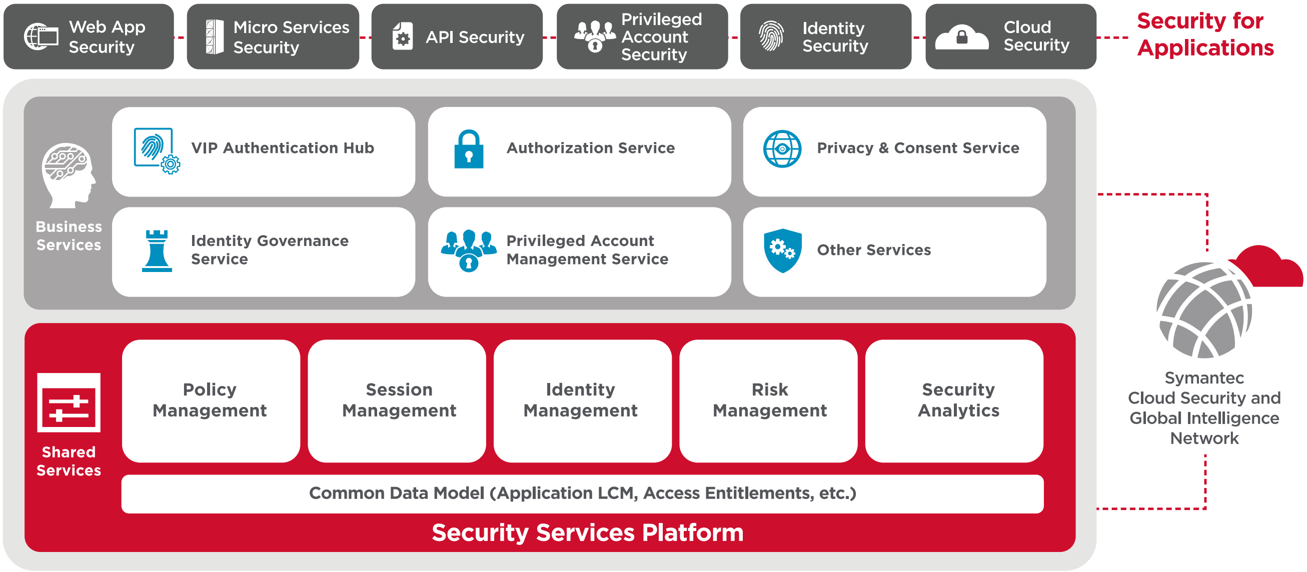
One of the popular industry terms for such security architecture is Zero Trust Computing. Zero Trust is valuable for enterprises because it offers the ability to decouple logical application access from the physical perimeter while still maintaining policy-based control over *Who can do What*. Achieving this requires that identity and security be incorporated into the fabric of applications and application infrastructure, in the process creating a reasonable blanket of protection around the enterprise assets.

Zero Trust requires a new approach to handle the dynamic, fast evolving business environment by enabling enterprise application developers to embed IAM into the fabric of their applications via standards, APIs, or environments-specific agents. Such architecture would give the enterprise an agile way to meet the security needs of their transformation efforts as they convert legacy processes into digitally integrated application ecosystems.

This forces IAM to undergo its own digital transformation by replacing siloed product-centric architecture by the architecture where the IAM business services used to secure, manage, and provision access are underpinned by a common architecture of policy, risk, session, analytics, and so on, giving enterprises a number of substantial benefits:

- Business agility to securely meet emerging business requirements and customer needs.

Figure 4: The New Digital IAM Architecture


Web App Security
Micro Services Security
API Security
Privileged Account Security
Identity Security
Cloud Security
Security for Applications
Business Services
VIP Authentication Hub
Authorization Service
Privacy & Consent Service
Identity Governance Service
Privileged Account Management Service
Other Services
Shared Services
Policy Management
Session Management
Identity Management
Risk Management
Security Analytics
Common Data Model (Application LCM, Access Entitlements, etc.)
Security Services Platform
Symantec Cloud Security and Global Intelligence Network

- Development agility to integrate and interoperate via IAM industry standards and APIs.
- Improved user satisfaction from reduced logins, elimination of password overload, and timely access.
- Reduced costs of operations and administration.

Digital IAM is about meeting such requirements with a holistic, yet loosely-coupled and distributed architecture delivering the following six key capabilities:

- **Risk-based business services to address the needs of the business when the business needs it.** The Zero Trust approach allows for visibility into users' activities to enable analytics to determine the risk to applications and data.
  - Authentication Microservice: Policy-based orchestration of asserting one's identity using a variety of factors including password-less, across different types of devices.
  - Authorization Microservice: Policy-based validation of one's rights to resources or data whether you are a business user or a privileged user.
  - Privacy and Consent Microservice: Policy-based controls over one's personal information.
  - Identity Governance Microservice: Policy-based validation and confirmation of one's privileges complying with corporate policies.
  - Privileged Account Management Microservice: Policy-based authorization over access to sensitive accounts, application secrets, and mission critical servers.
- **Shared platform services to ensure consistency and interoperability across business services:**
  - Policy management: Scalable, dynamic, multi-context policy language and engine.
  - Session Management: Policy-based orchestration and partitioning of one's activities into seamless application experiences.
  - Identity Management: User and group lifecycle management for administrative and end user personnel.
  - Risk management: Policy-based detection of "risk" based on one's behavioral patterns and health of systems and devices.
  - Security Analytics: AI/ ML-based detection and remediation of anomalies and visibility into business in terms of what is going on.
- **More configuration and less customization to enable productivity:**
  - Bring your own applications: Build applications rapidly and secure with Identity Services in hours using open standards for fast uptake.
  - Enable multi-channel access by leveraging REST enabled context-aware APIs that can be consumed by any platform or language. It's fully context aware so that a policy decision can be made depending on where and when an application is being accessed.
- **Built on modern cloud-native principles of Scalability, Elasticity, Resilience, Ease of Deployment, Functional Agility, and Technical Adoption:**
  - Using multi-tenancy to enable operational teams as providers of Identity Capabilities

  - Using microservices architecture to deploy in any public cloud, private cloud, or on-premise environment via the Kubernetes platform. Security teams need fewer specific technical skills and resources to manage the solution
  - Using industry standard stacks for Runtime (Kubernetes), for Logging/Auditing/Tracing (Fluent, Prometheus, Elastic) with config-time extensibility to other stacks, for Security Analytics (Siddhi)

- **Leveraging Open Standards to maximize productivity and reduce interoperability challenges:**
  - OpenID Connect for browser-based user authentication
  - OAuth2 for securing REST API calls
  - FIDO for modern password-less authentication
  - SAML for providing Single Sign on for Cross Domain applications using Federation
  - SCIM for simplified user management by defining a schema for representing users and groups
  - RESTful APIs for all identity functions for customization and headless operations
  - Standards-based JWT ecosystem to model and represent trust among distributed systems and applications

- **Embracing and extending existing IAM infrastructure to maximize reuse and ensure business continuity:**
  - Extending existing IAM solutions (for example, SiteMinder, API Gateway, VIP, and Advanced Authentication) to deliver modern authentication best practices such as password-less to existing applications with existing user communities without having difficult application changes
  - Integrating with existing session and audit management infrastructure (for example, SiteMinder) for comprehensive view of the session and audit trail across existing and new application ecosystems
  - Leveraging existing LDAP identity stores already containing user and group populations

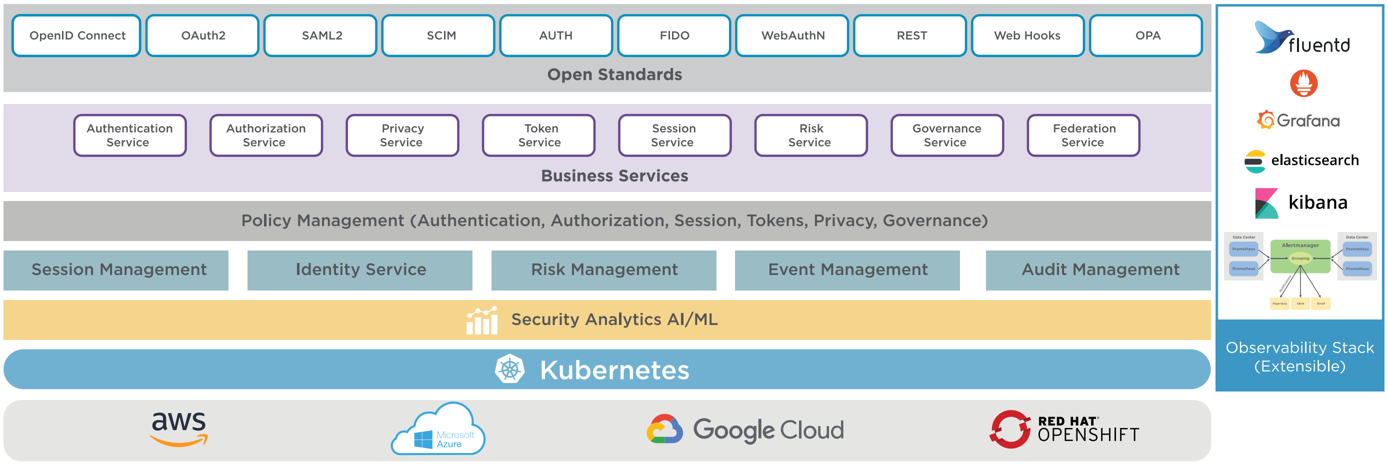
The architecture of Digital IAM also enables the enterprise's security practitioners to not only meet the business needs of the enterprise going forward, but at the same time extend the value of their existing identity stack already securing enterprise applications and processes. This architecture allows enterprises to embed standards-based identity services into the fabric of their applications resulting in a much improved user experience and elimination of security and governance siloes.

The Path Forward

Broadcom is in the process of redefining and developing a new Digital IAM architecture to address the needs of its customers undergoing digital transformation. Digital IAM, supporting Zero Trust principles, enables the business and drives new opportunities through a functional, secure, and scalable architecture designed to address the business agility enterprises must have to evolve their businesses.

This comprehensive IAM platform built to cloud-native specifications is meant to be an integral part of the enterprise security fabric. Fully based on open standards, it enables rapid integration of applications using a 100% open and standards-based solution, while extending the value proposition of the existing solutions enterprises have already in place. The combination of capable IAM services and ease of operations reduces development costs and prevents vendor lock-in

Figure 5: The new Digital IAM architecture embeds standards-based identity services into the fabric of applications



by using proven industry standards to integrate IAM business logic into custom applications using open APIs.

The platform's scalable and secure back-end infrastructure is capable of being deployed anywhere the organization chooses, including on-premise data centers, cloud-data centers, or a hybrid combination. The platform securely connects identities to applications - it needs to be everywhere and it needs to be easily consumed by developers who are not security experts. The platform becomes the glue that enables enterprise's digital transformation:

- Common data model for modeling "Access" to unify and simplify the lifecycle of IAM relationships currently requiring presence of multiple, siloed solutions
- Based on Zero Trust principles with built-in risk-based policy infrastructure
- IAM as Big Data to provide built-in Security Analytics for anomaly detection and remediation
- Omni-channel authentication for Identity Assurance across native and federated application workloads
- Web and Web Services authorization to manage transactional risk and meet regulatory compliance
- Common session management infrastructure for continuous monitoring and partitioning of identity activities with seamless SSO across different application ecosystems
- Cyber protection for overall security and enhanced risk assurance via optional integration with Symantec's CASB, Proxy, VIP, and SAC solutions

Conclusion

The shift to modern architectures based on multiple perimeters such as Cloud, Mobile, API, and so on, requires a modern, integrated, and open Digital IAM architecture to enable the enterprise to securely achieve its business initiatives while managing the business risk and complying with regulations.

The Digital IAM architecture lets enterprises embed standards-based identity capabilities into the fabric of their applications—driving enterprise agility, maintaining adequate risk controls, and leveraging Zero Trust principles into all user activities. It delivers a shared, risk-based security service platform for identities to get a consistent SSO/SLO experience across existing and new application paradigms. It enables the business to gain necessary governance capabilities required for a multi-cloud, multi-perimeter world. It integrates with Symantec's security solutions to both harden network security by providing deeper identity context and leverages additional insight provided by security controls to make IAM decisions more meaningful.

In the ever fragmented world, Digital IAM, made up of IAM Business Services underpinned by shared security services, allows enterprises to gain visibility into the user's activities, uses smart analytics to determine the risk imposed by the user, and allows/restricts/manages user activities accordingly while enabling user satisfaction across different channels.

It enables the enterprise to securely connect any user, from any device, to any application while offering a seamless user experience and keeping enterprise assets secure.

Disclaimer

Certain information in this paper may outline Broadcom's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product. The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.

THIS PAPER IS FOR YOUR INFORMATIONAL PURPOSES ONLY. Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this paper, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com