OPTIV

IDENTITY DEFINED SECURITY (IDS)

Solution Primer

Heath Nieddu
Senior Research Analyst
Office of the CISO, Optiv

Introduction

The deficiencies of perimeter-based security strategies are obvious and growing. Our infrastructures are moving off-premise, our partners are increasingly offering their applications as a cloud service, and our enterprise machines are progressively not under direct control. **Identity Defined Security**™ (IDS) is a concept that attempts to provide a superior approach to perimeter-based security. Instead of simply bemoaning the strain, IDS empowers next-generation identity and access management (IAM) practices to adapt and overcome current challenges.

What IDS actually implies in terms of transformation ranges in industry literature from a complete overhaul of architecture to the more **basic recognition that identity and access should be more tightly integrated throughout the entire security program.**

For the security leader that is protecting the enterprise's most valuable digital resources, it is crucial to understand what IDS is to create a plan that allows for proactive management of the evolving blueprints, ensure enhanced processes, and pave the way for fully utilizing identity resources.

How enterprises best transition their IAM efforts so that their programs are more identity-centric will depend upon their goals and ambition. The shift to IDS is a fundamental adjustment in posture from *discover* and *react* to *inform* and *adjust*. For most organizations, the principles of IDS will most likely be integrated incrementally and over time. Once integrated, this shift will require socializing within the organization to truly be effective. This shift can be positive if well planned for, but needlessly expensive if attempted without proper preparation.

Traditional Security Processes Becoming Less Effective

There is a growing body of evidence that the combination of off-premise deployments, increasing integration with third-party partners, and increased use of personal and mobile devices is straining assumptions of many security approaches. [1,2,3] The historic assumptions that are increasingly questionable include:

- The most secure architecture is one where controls are applied solely within a domain that is directly managed.
- Various security technologies, such as security information and event management (SIEM), data access governance, and data loss prevention (DLP) can operate in isolation.
- The perimeter defenses are sufficient to reduce the majority of risks.
- The location of a single source of truth for identity and permissions can be managed under direct control in a centralized domain.

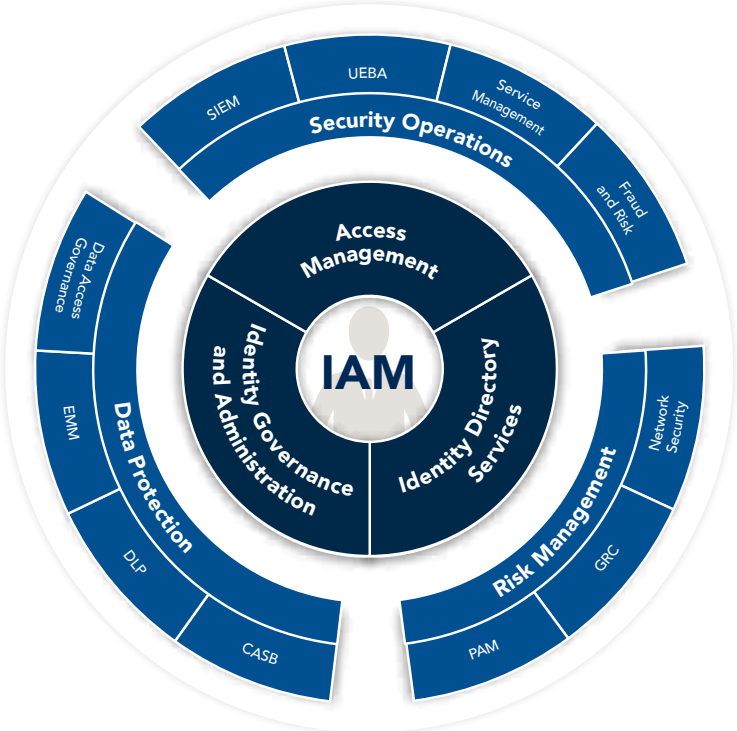
These assumptions are quickly becoming irrelevant and should be re-examined. These forces challenge the above expectations:

- Various stages of off-premise infrastructure deployment, including hybrid deployments, are often conducted in a decentralized manner.
- There is increasing domain integration with suppliers and partners with varied security postures and integration capabilities.
- Security technologies are increasingly interdependent, requiring contextual data to make adaptive decisions about access.
- Personally owned and mobile devices with uneven policy deployment and varied network access paths are increasingly present.
- The Internet of Things (IoT) is becoming more corporate and mainstream, and these newly connected devices are authenticated and granted access in non-standard ways and with limited computing power that can be dedicated to security agents.

A recent breach at a payroll processing company illustrates how complex computing relationships can create unforeseen vulnerabilities. The vulnerabilities in this case could have been addressed with next generation identity-defined concepts, allowing systems to make risk-based real time authentication decisions with multiple enforcement and notification mechanisms.

- Identity thieves attempting to perpetrate identity and tax fraud gained access to the W2 information of one of the company's customers by assembling a number of credentials from multiple sources. [4]
- The bank uses the payroll processor for various services, including an external portal made available to employees to access their tax information. Multifactor authentication was used to create accounts at this portal, but the factors had weaknesses that created security gaps.
- One set of authenticators was single sign-on (SSN) and birth date, easily attainable in black markets. Account creators also needed to obtain a URL and in some cases a unique identifier, but both were static. The URLs were mistakenly published by the processor's customers in some cases.
- This is an example of the increasingly typical interactions with suppliers, which are necessary to build effective business for good reasons. However, the interactions create effects that are hard to predict by all parties involved.

There is a growing awareness of the weakness of previous security assumptions and the promise of IDS approaches. This is demonstrated by recent whitepapers on the topic, and by the emergence of several industry groups that provide direction on the issue and suggest ways to coordinate efforts among solution providers. The Identity Defined Security Alliance (IDSA) promises to be a venue for technology partners, services organizations and enterprises to illustrate these alternatives along a spectrum of adoption with clarity. [5]



The Identity Defined Security Alliance (IDSA) promises to be a venue for technology partners, services organizations and enterprises to illustrate these alternatives along a spectrum of adoption with clarity.

IDS Defined

While IDS can be defined in many different ways, Optiv defines IDS as:

"Identity Defined Security (IDS) is the next generation of identity and access management, providing real time, intelligence-based access to data and applications by integrating IAM infrastructure with enterprise cyber security technologies. An identity centric approach to enterprise security allows enterprises to optimize their cyber security investment while controlling risk as IT infrastructures converge."

This research addresses how to take a mature IAM program to export it to the rest of the security program. **This program approach will address the key stakeholders, business requirements, people, process and technology needed for an IDS program, and briefly outline a three phase program path to leverage identity functions in the rest of the security program.** Other research at Optiv discusses more deeply both:

a) Program frameworks for next-generation IAM

b) Detailed implementation roadmaps and technology integrations needed to gain an IDS approach.

This research also assumes that IAM programs are changing now, and will continue to change in dramatic ways to meet current security challenges posed by cross domain activities. A next-generation IAM program will be able to handle increasing complexity as it matures, embracing naturally the principles of IDS.

- Clear, standardized and widely used role definitions will help bolster the baselines of user behavior anomaly detection, thereby increasing responsiveness to emerging threats.
- Integrating your application access controls with other information providers along the transaction (network, endpoint, etc.) allows for a defense-in-depth approach.
- Virtualized identity stores that span both off-premise and on-premise infrastructure deployments can increase security and speed integration as hybrid architectures are embraced.
- Having mature IAM process (and an understanding of the data) integrated with other data driven investments (SIEM, user behavior analytics) will provide clarity to security leaders about the overall security posture.

The Stakeholders that Impact an IDS System

The stakeholders involved in creating an effective IDS system are best characterized by starting with those needed for IAM and then broadening the view dramatically.

One of the points of IDS is to find ways to coordinate a vast array of parties that were not viewed previously as integral. As applications and new data types increase prolifically, centralized access management becomes impossible and the algorithms to automate and decentralize access decisions become more important. When our businesses become constellations of partnerships with various firms, our identity information and entitlements must necessarily transcend their normal borders. The stakeholders become a web of identity providers and receivers.

Stakeholders include those directly associated with the IAM program, such as the existing provisioning teams, directory managers, IAM-related application owners and executive sponsors. Stakeholders specifically relevant to an IDS approach are:

- The CISO
- Security leaders in other security technology areas such as SIEM, governance, risk and compliance (GRC), privileged access management (PAM), NetSec, cloud access security brokers (CASB), user behavior analytics (UBA), risk and fraud
- The CFO
- Any business units that own the end-user experience, whether trusted internal user or customer.

Operationalizing IDS

Program Drivers

Program drivers guide the development of the overall IDS approach. These are the elements that propel security programs to the point of taking action on an IDS perspective.

- High profile incidents, incidents at peer organizations and internal incidents all raise awareness about the potential impact of lapses in cyber security.
- A tide of technological change rising from supply chains, customer demands and internal IT teams shift organizations into hybrid infrastructure deployments and require credentials and access information that transcends traditional boundaries.

- An active state of integrations driven by M&A activity.
- The long-established inability of perimeter defenses to be sufficient in thwarting attacks, although they remain necessary.

As high impact insider threat-based incidents and unforeseen vulnerabilities in cloud architectures make mainstream news, business leaders are asking more questions about the state of their security programs and demanding higher levels of accountability. Effective security leaders need to demonstrate that they can define the broader IAM problem and explain to what extent it is an internal issue.

Business Requirements

While the program drivers help guide the development of the overall program, business requirements help define the initial deliverables. Operating a successful program means effectively meeting the demands from the business stakeholders in a timely manner.

The above program drivers cause security teams and business leaders to ask:

- Can identity data do more for our security and our customers?
- Can an IDS strategy protect key business functions at an acceptable cost?
- Can IDS minimize the burden of administration within the other investments we have made in cyber security?
- Can IDS enable more real time and risk-based decision making, especially in the authentication process?
- Can IDS provide the flexibility required to manage access with an unlimited amount of touch points and device types?

For business leaders, there is usually a significant function, process or initiative that needs to be protected above all others. This could be the key revenue generating process, or comprised of specific risks generated by an enterprise risk management program. The need to support this function should be easily understood and agreed upon by a large portion of management, thereby creating an objective topic to rally around. Communication can be centered on how a holistic IDS system benefits this initiative in particular.

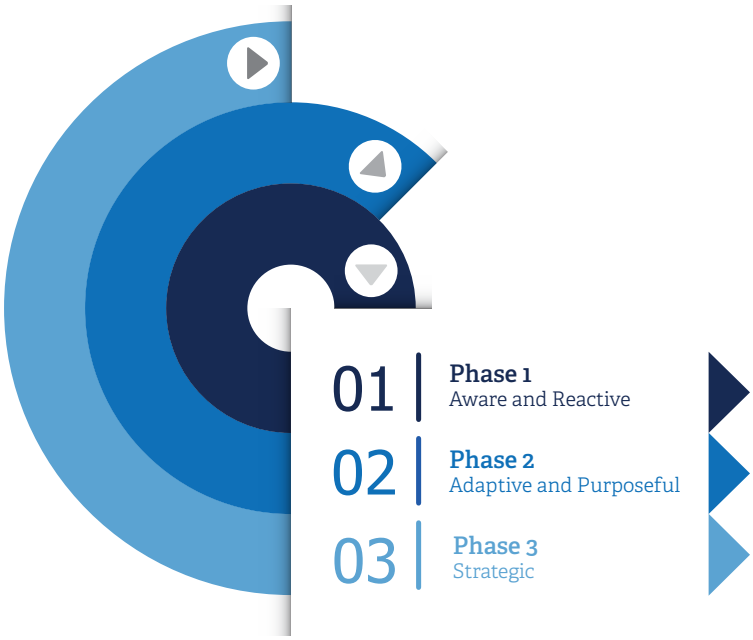
Developing a Strategy Approach

The foundation of any well-orchestrated security program or strategy is rooted in business alignment and supported by an appropriate balance of personnel, processes and tools. Without an appropriate alignment to business objectives and available resources, the program will be unbalanced, may not keep up with the momentum of the organization and could produce irrelevant results.

Linchpin Assumption: This paper assumes that previous IAM investments have been made and implemented at least to some degree (even if basic), and that an organization is now ready to formulate a next-generation IAM program and initiate IDS. To determine if this assumption is appropriate for you, ask yourself:

- Have I begun to treat my IAM investment programmatically and do I have a diverse set of advocates such that next generation IAM is achievable?
- Have my IAM investments been measured to be successful enough so that I can focus on the next generation of IAM?
- Does my organization understand the overall migration path toward intelligence-driven management of risk and decision making?

The foundation of any well-orchestrated security program or strategy is rooted in business alignment and supported by an appropriate balance of personnel, processes and tools.



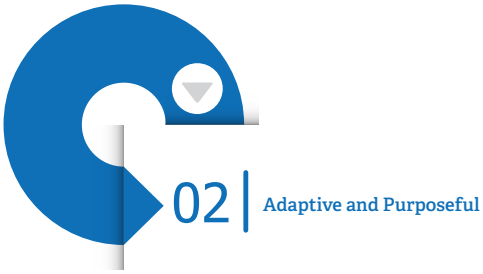
Phase 1 – Assess

The first critical step to enhancing IAM is to assess current efforts within the organization as well as other security technology areas so that the team designs appropriate enhancements that integrate with the whole security program. This is done by evaluating user life-cycle management, provisioning, reviewing relevant risk assessments and audit findings, reaching out to HR teams, assessing DLP capability, reviewing SIEM capabilities and evaluating business goals.

Operational Advice

- Listen to technical leads. Concerns here are often symptoms of larger problems.
- Ensure a strong IAM foundation before attempting to export IDS to the rest of the security functions.
- Review crucial business level strategies and speak with key business stakeholders to ensure strategy development will be relevant to current priorities.

Phase 2 – Formulate IDS Strategy



Initial interest in IAM maturity must be leveraged into commitments and involvement by all stakeholders so that an IDS approach can effectively leverage current IAM resources within the rest of the security program. This continued interest-building will require leadership and strong program management.

The effort to shape the specifics of this strategy require a group of stakeholders beyond the traditional IAM roles, such as the CISO, if not already involved, and the security technology leaders from other parts of the security program, such as SIEM, GRC, PAM, NetSec, CASB, UBA, risk and fraud. The IDS strategy development effort will also require a new set of process owners in areas such as security operations and enterprise risk management.

Make sure to create vivid examples in the plan that describe some of the ways an IDS approach will enhance the entire security program. For example, demonstrate under the assumption of a hybrid IT infrastructure how users and systems can safely access resources across various domains whose perimeters are not directly controlled, with a consistent set of identity-based access controls. Accomplish this by taking advantage of improved authentication services, automated provisioning and dynamic monitoring and enforcement

based on the risk of the context in real time. Finally, describe how this benefits and integrates the rest of the security program in terms of identity intelligence and shifting of the risk posture from the perimeter to the identity.

The IDS strategy should be based on a set of guiding IDS principles that represent the desired approach, and those principles should be used to not only shape the strategy initially, but help it maintain momentum as new challenges arise. The hallmark of this phase should be to think broadly about how to apply IDS to a variety of security problems.

Operational Advice

- Think broadly about the people, processes and technology that should be involved.
- Understand that properly managing tools is necessary – but not sufficient – for developing an integrated IDS.
- Tout successes to get over the initial implementation hurdles.
- Ensure that anomaly detection tools are identity-centric. This will make investigations easier to pursue and the tool easier to use.

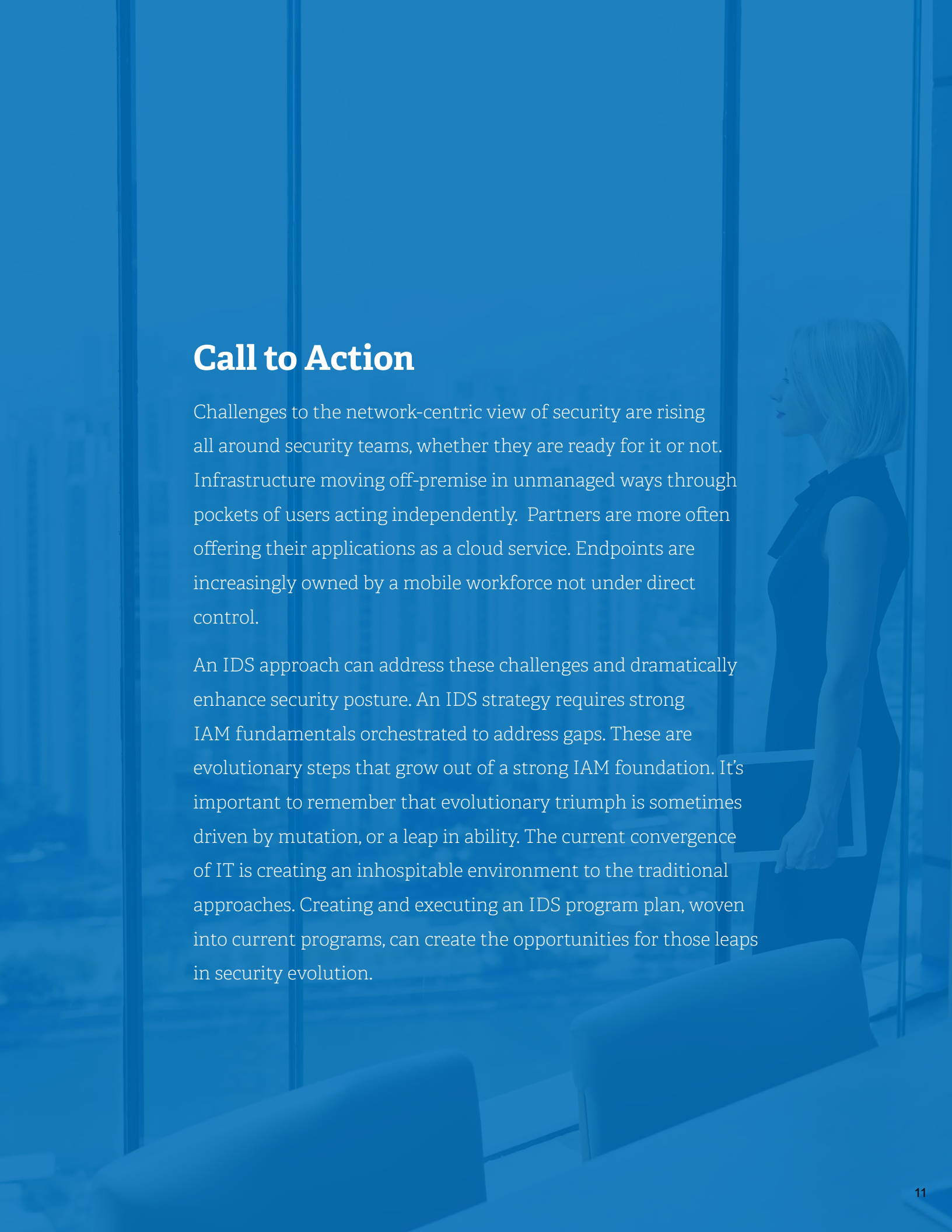
Phase 3 – Initiate an IDS Program

Measure progress towards goals and do the groundwork to ensure implementation follows principles of strategy and program objectives. This stage will require driving the details of strategy to completion.

As IDS-based objectives are completed over time, challenges will arise and the environment will change. Visionary leadership will need to remind stakeholders of guiding principles and how identity has helped and will help with security. Simultaneously, those executing change will need to maintain a practice of managing the orchestration of various activities. Michael Porter has said that managing how things are done in concert is as important as deciding what to do. Never was this more true than with shifting the security program to an IDS approach.

Operational Advice

- Utilize a set of guiding IDS program principles to quickly react to unforeseen events.
- Advertise quick wins even before the completion of the IDS integration.
- Have short and concise goals to maintain momentum across various parties.



Call to Action

Challenges to the network-centric view of security are rising all around security teams, whether they are ready for it or not. Infrastructure moving off-premise in unmanaged ways through pockets of users acting independently. Partners are more often offering their applications as a cloud service. Endpoints are increasingly owned by a mobile workforce not under direct control.

An IDS approach can address these challenges and dramatically enhance security posture. An IDS strategy requires strong IAM fundamentals orchestrated to address gaps. These are evolutionary steps that grow out of a strong IAM foundation. It's important to remember that evolutionary triumph is sometimes driven by mutation, or a leap in ability. The current convergence of IT is creating an inhospitable environment to the traditional approaches. Creating and executing an IDS program plan, woven into current programs, can create the opportunities for those leaps in security evolution.

References

1 "Identity-Centric Security," CA, Retrieved from: http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/identity-centric-security-enabling-protecting-business-pdf-1-w-1085.pdf

2 Cameron, Kim, Reinhard, Posch, and Rannenberg, Kai, "A User-Centric Identity Metasystem," October 5, 2008. www.identityblog.com. Retrieved from: http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/identity-centric-security-enabling-protecting-business-pdf-1-w-1085.pdf

3 Ward, Rory and Beyer, Betsy. "BeyondCorp: A New Approach to Enterprise Security," Login: December 2014, vol.39, no. 6.

4 Krebs, Brian. "Krebs on Security Blog," Retrieved from: https://krebsonsecurity.com/2016/05/fraudsters-steal-tax-salary-data-from-adp/#more-34704

5 Dingle, Pam and Block, Robert, "The Identity Defined Security Alliance" Ping, retrieved from: https://www.pingidentity.com/content/dam/pic/downloads/resources/white-papers/en/ids-alliance-white-paper.pdf

6 Porter, Michael E. "What is Strategy?" Harvard Business Review, 1996. Pp. 1-3

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

6.16 | F1