EXECUTIVE BRIEF | NOVEMBER 2016

CA and Hewlett Packard Enterprise Joint Solutions

Enable Robust Security in Digitized and Hybrid Environments

94%

of hackers find privileged account information in unprotected files such as spreadsheets[1]

Protecting the enterprise against internal and external security threats has never been more important—or more difficult. In the digital economy, unauthorized access to your network exposes an unimaginable range of data that can damage your business and your reputation in ways from which you might never be able to recover. So, not surprisingly, enterprise security is a top priority for every business from Fortune 500 enterprises to local retailers.

Adding to the challenges IT is facing in keeping the enterprise secure is the rapid movement toward widescale digitization of the enterprise. Your employees, partners and customers now demand unprecedented levels of access to your organization—from anywhere, at any time and on any device. This has led to a dramatic shift in the way users access protected data in the new, open enterprise, creating widely different attack surfaces and increasing risks. According to Gartner, worldwide spending on information security was on a pace to increase by nearly five percent in 2015, to reach an estimated total in excess of $75 Billion.[2] But spending alone can't adequately solve the problem.

Managing Identities in the Age of the Open Enterprise

With most enterprise environments adopting a hybrid approach to delivering digital services, including cloud and SaaS models, security challenges have grown in number and complexity. In the open enterprise, effective identity management and governance must be optimized and automated to address:

- **Employee lifecycle management**—A streamlined process for managing user identities and entitlements from onboarding to termination
- **Privileged access management**—Controlled, auditable access to the most powerful accounts in the enterprise
- **Access requests and approvals**—The ability to provide a convenient, intuitive experience to enable user self-service
- **Certification campaigns**—User access certification
- **Risk analytics**—Detection and prevention of excessive privileges and segregation-of-duties violations

[1] Black Hat, Black Hat Hacker Survey Report. July 2015

[2] Gartner, "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," Sept. 23, 2015

The number one leading cause of data security breaches is non-malicious employee error.[3]

Security measures need to provide a fast, flexible and satisfying user experience. Consumer-facing applications have set the bar high, leading business users to demand comparable convenience, transparency and intuitive usability wherever they are. For instance, users expect customized interfaces that provide a seamless experience based on their unique roles. And increasingly, security must include a self-service component that allows business users to request and obtain access to applications and data. Fulfillment then comes through streamlined processes that often never loop in anyone from IT at all.

Creating a situation where employees play an increased role in managing security is counterintuitive for most IT professionals. But ignoring this new approach carries its own set of risks. Right now, security practices and processes are often so onerous and opaque that they actually create barriers to productivity and worker satisfaction. This, in turn, leads employees to make mistakes, seek workarounds or to shortcut security protocols they deem as too complicated or time-consuming.

The Path Forward to Increased Security Compliance

The ideal goal is ironclad security that is easily navigated by end-users. While that may sound contradictory, it is actually already possible, thanks to a partnership between CA Technologies and Hewlett Packard Enterprise (HPE). Together, CA Technologies and HPE's deep transformational skillsets and run capabilities provide identity and privileged access management solutions that make it easy for employees to get the data and applications they need to do their jobs. And at the same time, maintain tight, real-time security that prevents unnecessary access to other areas of the enterprise.

The prime example is CA Identity Suite, with updated capabilities for an improved, end-user-driven experience that offers secure, application-based access from virtually any device. The process mirrors that of a retail shopping experience with end users selecting the applications they need off the shelf and putting them in a shopping cart. Once they finish "shopping," their cart is sent to a manager with the authority to approve access.

The manager receives a list of the applications that the employee has requested authorization for, along with a risk meter for each that displays the assessed threat of giving that specific user access to that specific application or data set. When the risk seems uncomfortably high, the manager can seek input from a security expert before giving approval. Access can be limited to a predetermined period, and rules can be put in place that trigger reassessment based on changes in job status and responsibilities.

The entire process is quick, seamless and intuitively easy to use for everyone involved. It accelerates access for users, thereby saving time and increasing productivity. CA Identity Suite, with HPE, also drives down costs by automating the process and reducing service desk calls and interventions by system administrators. And it makes life easier for managers who would have previously had to manage such requests through manual spreadsheets.

[3] Ponemon Institute, "Ponemon Institute's Survey on Data Security Breaches," February 2015.

Protecting Key Vulnerabilities With Privileged Access Management

Every system needs super users who have expanded access to highly sensitive corners of the network. But the credentials that grant that access are the prize hackers value most. And there's evidence that they aren't as hard to come by as you might think. In a recent survey, 90 percent of hackers believe it's easy, or easier to steal privileged account credentials than in 2013 and 2014.[4]

Why, when security is such a hot-button issue, would high ranking IT professionals take such a risk? Again, the answer is user experience. When existing security protocols take too much time or effort—for instance, changing passwords on each of 200 individual servers every month—time-strapped employees are more likely to seek out a way to sidestep the inconvenience.

With CA Privileged Access Manager, and the deep integration and management offered by HPE, you can reduce the burden on your system administrators while actually enhancing enterprise security to a level that meets federal and military-grade requirements.

CA Privileged Access Manager appliance form factor enables faster deployment to thousands of end points, while offering relatively low TCO. In addition, as a hardened appliance, it is the first, and only security solution for controlling, monitoring and auditing privileged user access to attain Common Criteria certification outlined in the National Information Assurance Partnership (NIAP) Protection profile for Enterprise Security Management–Policy Management. This means that CA meets strict security criteria recognized by more than 27 counties, and addresses the needs of federal and private sector companies

Think of CA Privileged Access Manager as an impenetrable box that holds the access credentials to all of your most sensitive systems and hardware. The CA and HPE integrated service allows privileged users to connect to the box using high-security single sign-on credentials with dual-factor authentication that can include tokens and biometric checks, if desired. Once the user's identity is confirmed, CA Privileged Access Manager applies encrypted credentials that allow her to access the devices and data for which she has authorization. Once the session ends, those credentials are automatically reset.

Authorization can also be limited to preset times. And all activity during the session is recorded to provide a forensic record in case unauthorized activity is detected.

Engaging Employees Enhances Security

An open enterprise requires seamless, two-way, unfettered access to appropriate information and resources between employees, partners and suppliers. So, the focus must be to eliminate the main reasons your employees undermine your identity and access system security. This requires a commitment to open, enterprise-driven security protocols that speed access to job-critical resources, and provide an intuitive, easy-to-use interface.

By offering your employees a responsive, identity management experience, they become allies rather than hurdles in your efforts to keep your enterprise and your sensitive data safe from cyber criminals. In addition to moving closer to a compliant state, you will free them up to become more productive—including help-desk personnel and administrators who no longer need to devote as much time to managing access.

[4] Jeff Edwards, Identity Management News, July 14, 2015

It's time to activate your most powerful weapon against cyber threats—your employees—and give them increased agility with the synergies of CA Identity Suite and CA Privileged Access Manager backed by HPE. Whether on-premise, off-premises, in the cloud, or as a fully managed service, CA and HPE have the depth of experience and technologies to set your business free.

About the CA Technologies-Hewlett Packard Enterprise Partnership

HPE and CA have partnered and worked together for the past 20 years, and have a a successful history of collaboration in helping our clients resolve their unique business and technology challenges. Together with dedicated teams, we deliver a powerful combination of tools and technologies that take advantage of the ability of CA software and HPE to transform enterprise security. Our combined and proven approach allows you to successfully integrate diverse technologies and processes to achieve better results, even for your toughest enterprise challenges. **To learn more about our partnership, connect with a representative.**

CA Technologies:

Philip Kenney
VP, Security Strategic Partnerships
Mobile: +1 571 235-3211
Philip.Kenney@ca.com

Farouk Al-Shorafa
Global Technology Advisor
Mobile: +1 347 489 4189
Farouk.Al-Shorafa@ca.com

Hewlett Packard Enterprise:

Mark Vanston
AMS Enterprise Security Services Sales Lead
mark.vanston@hpe.com

Meurig Jones
EMEA Enterprise Security Services Sales Lead
meurig.jones@hpe.com

David Fox
APJ Enterprise Security Services Sales Lead
david.fox4@hpe.com

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more a **ca.com**.

Find out more at www.hpe.com/services/security

HPE Enterprise Services draws upon decades of IT security, risk and availability management experience to help you predict and disrupt threats, manage risk and compliance, and extend your own security team, so you can focus on what matters most. We bring together the people, technology and expertise to advise, transform and manage security solutions that allow your business to flex to meet the digital challenges in the idea economy.

This document does not contain any warranties and is provided for informational purposes only. Any functionality descriptions may be unique to the customers depicted herein and actual product performance may vary.