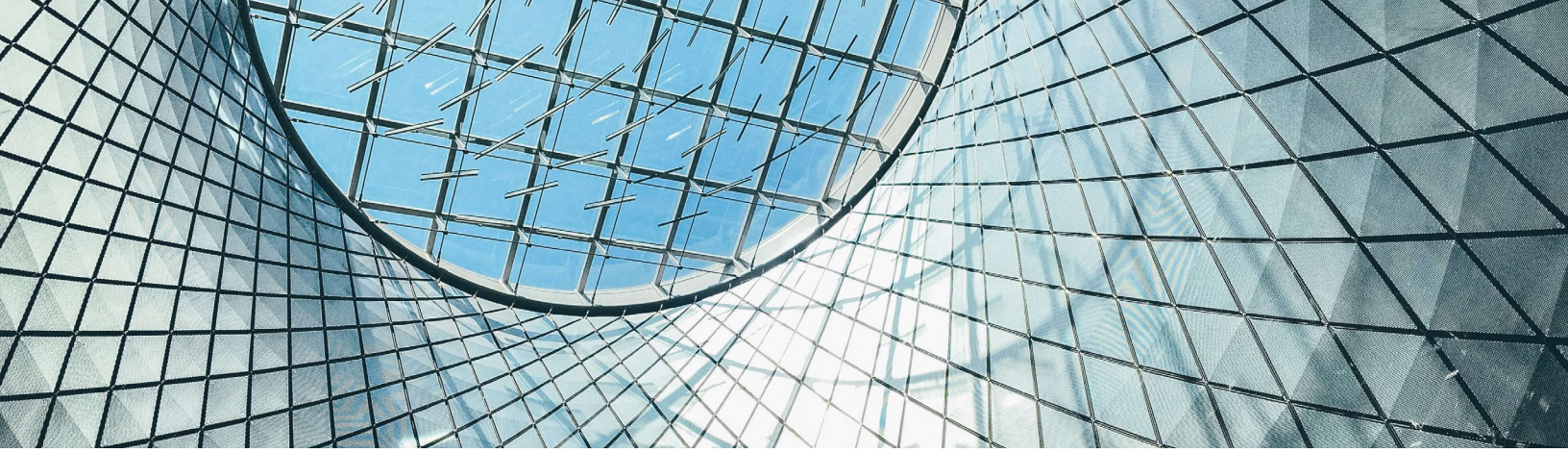


Market Insight Report Reprint

Coverage Initiation: strongDM targets PAM deployment challenges with cloud-native PAM platform

April 29 2022

by Garrett Bekker

Founded to help make privileged access management less onerous, strongDM has an infrastructure access platform that combines remote access, networking, authentication, authorization and auditing functionality into a single platform that can work with legacy on-premises and cloud-native environments.

451 Research

S&P Global
Market Intelligence

Introduction

Traditional privileged access management (PAM) products were mainly designed for controlling access to on-premises infrastructure such as Windows-, Unix- and Linux-based servers. The emergence of cloud-native computing architectures and multicloud operating environments has created new challenges that many existing PAM products are ill-equipped to handle. Beyond standard Linux and Windows servers, most firms now have heterogeneous infrastructure to support, including containers running in Kubernetes clusters, as well as traditional apps that have been "lifted and shifted" to the cloud and are now run in multicloud infrastructure environments.

StrongDM was founded to help make PAM less onerous, for both administrators and users, with an infrastructure access platform that combines remote access, networking, authentication, authorization and auditing functionality into a single platform offering that can work with both legacy on-premises and cloud-native environments.

THE TAKE

The ability to combine connectivity, authentication, authorization and audit capabilities in a single offering puts strongDM on solid footing in an emerging niche in the PAM market that we refer to as "cloud-native PAM." PAM is no longer just for DBAs, developers, engineers and IT administrators, and the company's focus on the user and developer experience should resonate with nontraditional PAM personas such as sales, marketing and customer operations staff. StrongDM also has financial backers with a solid pedigree, although the company is in the early stages and will need to raise market awareness to stand out in a highly crowded and competitive PAM market that includes over 40 different vendors.

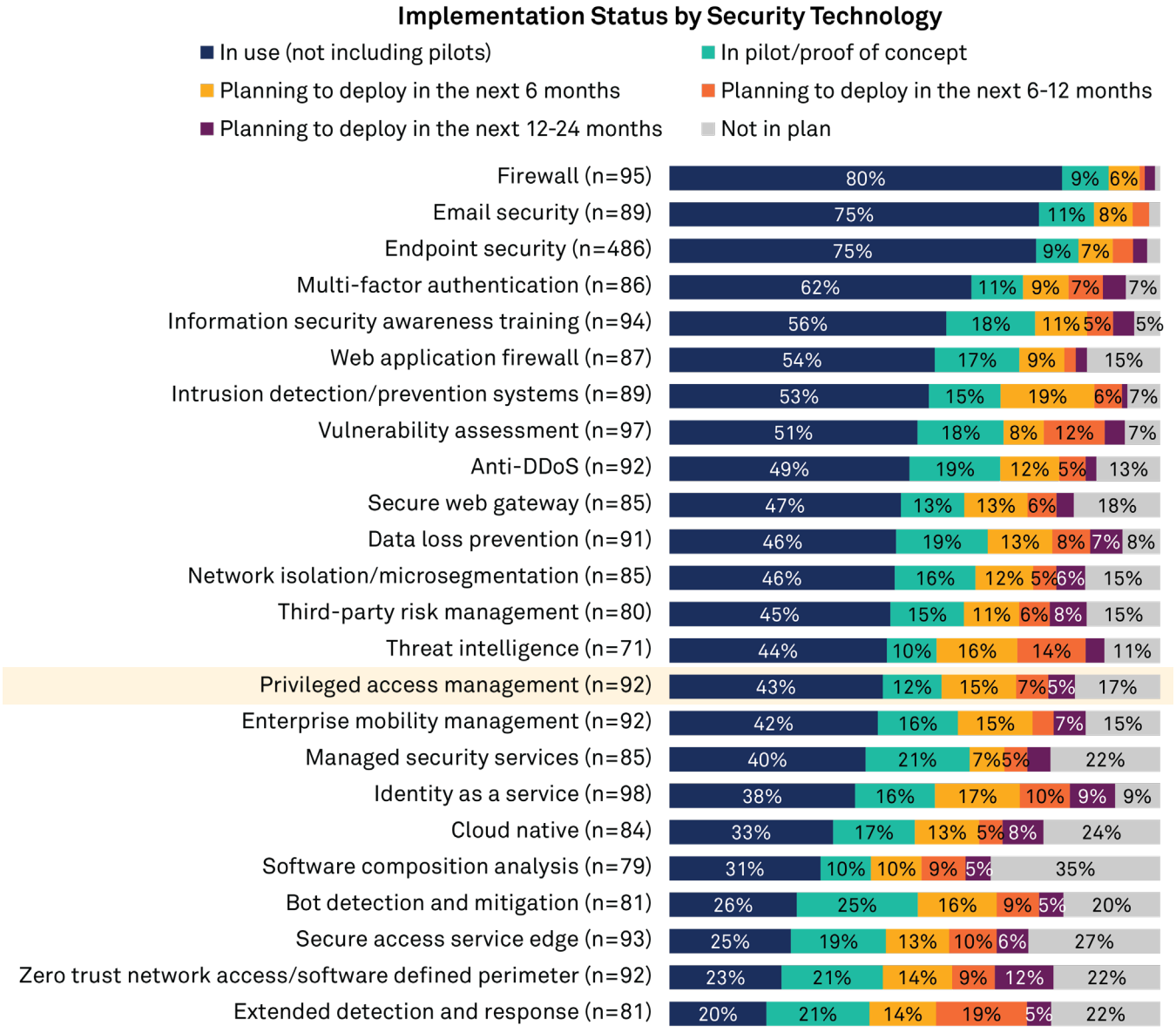
Context

StrongDM was founded in 2015 by CCO Schuyler Brown, CTO Justin McCarthy and former CEO Liz Zalman. Current CEO Tim Prendergast – who previously founded Evident.io (acquired by Palo Alto Networks Inc. for $300m) – joined the company in 2021. StrongDM operates as a fully remote organization, with nominal headquarters in Burlingame, California, and over 150 employees. The company is backed by True Ventures, Sequoia Capital, GV (formerly Google Ventures) and Tiger Global, and has raised a total of $76 million in funding, most recently a $54 million series B round late in 2021.

Products

Many legacy PAM products are complex to install and operate. That may help to explain why enterprise PAM deployments have lagged other security tools, despite the growing role of privilege escalation and lateral movement in many successful attacks on organizations. To illustrate, 451 Research's Voice of the Enterprise (VotE) survey data shows that just 43% of enterprises have deployed a PAM product to date, which is well below other security staples such as network security, endpoint security, email security or SIEM and analytics tools.

PAM Deployments Lag Other Security Technologies



Q. What is your organization's status of implementation for PAM within the next 24 months?

Base: All respondents (n=92)

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

As noted above, strongDM's Infrastructure Access Platform combines authentication, authorization, networking and observability in a single offering. It works with both legacy on-premises and cloud-native (including Kubernetes) environments and connects (via zero-trust networking instead of VPNs or bastion hosts) any user (pen testers, QA teams, developers, engineers, DBAs, data scientists, etc.) to any resource (databases, SSH nodes, Kubernetes clusters, Jenkins, SSH bastions, SQL servers, Windows servers, etc.) regardless of where they are located.

For authentication, customers can use a variety of identity providers (Active Directory, Okta Inc., etc.) and secrets managers (HashiCorp Vault, AWS Secrets Manager, GCP Secret Manager, etc.); customers can also use strongDM's secrets manager if they don't already have one. For authorization, strongDM uses both attributed-based access controls (ABAC) and role-based access controls (RBAC) and does just-in-time (JIT) least privilege access. Users and roles can also be managed via an IdP like Okta or Azure AD, making it possible to onboard and offboard employees with a single click or automation.

The platform performs auto-discovery of all resources in the environment, and users can connect without having to know keys, passwords, credentials, etc. or where resources are or who owns them. StrongDM can also capture and record every single query and command in every session across the entire stack, and logs permission changes and access requests. Session replays are available for SSH, RDP or Kubernetes sessions for auditing purposes.

Technically, strongDM is a proxy that interprets network protocols, and has a local client on Mac, Linux or Windows workstations that creates a TLS tunnel from the endpoint to the proxy gateway. The gateway sits on the internal network and provides access to target resources directly for flat networks, or via a reverse tunnel, and forms a mesh with other proxies in the environment. Users can log into the client directly or single sign-on (SSO) from an identity provider such as Azure AD or Okta. StrongDM also provides a SaaS app that serves as a configuration layer that can manage user roles, permissions, etc. that are pushed to the client and used to control real-time authorization and access to resources.

Strategy

StrongDM is targeting companies that are building their businesses on top of modern IT stacks and adopting cloud-native services such as IaaS, PaaS, containers, etc. to run as efficiently as possible, as well as large incumbent enterprises that are running both on-premises and with multiple clouds and need help stitching it all together. StrongDM is also looking to address a broader set of user personas than traditional PAM deployments, which were typically designed for IT administrators with a more narrowly defined set of objectives. In modern corporations, a wide variety of employees can be considered "technical professionals," including sales ops, customer ops and marketing ops – all of whom must manage and use technical infrastructure as part of their jobs.

Competition

Given its focus on providing secure access to heterogeneous infrastructure, strongDM's most direct competitors are likely part of the traditional PAM market, which includes over 35 vendors like BeyondTrust, Broadcom Inc. (CA/Xceedium), Centrify, CyberArk Software Ltd., One Identity and Delinea (previously Thycotic), as well as Manage Engine and Wallix. Newer PAM vendors with a greater focus on JIT privileged access include Remediant, Stealthbits Technologies (acquired by Netwrix) and Xton (acquired by Imprivata).

However, strongDM may be most directly competitive with vendors that offer PAM capabilities with a focus on DevOps, including HashiCorp Inc., Akeyless, Iraje, Senhasagura and particularly Teleport, with which it shares a similar proxy-based architecture and similar go-to-market messaging, as well as HashiCorp's Boundary offering. HashiCorp's Vault is capable of doing "traditional" secrets management, while Consul also provides a distributed key store in contrast to Teleport's reliance on short-lived certificates.

Although strongDM has zero-trust networking functionality, the company is not competing directly with ZTNA vendors looking to provide remote network access for entire workforces. The list of ZTNA vendors is nearly as crowded as the PAM market, and includes Appgate, Banyan Ops, Netskope, Palo Alto Networks, Perimeter 81, Check Point Software Technologies Ltd. (via the acquisition of Odo Security), Fortinet Inc. (OPAQ Networks), Cisco Systems Inc., Juniper Networks Inc., VMware Inc., Google, Microsoft Corp., Proofpoint (Meta Networks), Zscaler Inc., Forcepoint, Ivanti (Pulse Secure), Akamai Technologies Inc. (Soha Systems), Cloudflare Inc., Broadcom (Luminate Security), Verizon Communications Inc. (Vidder) and Barracuda.

SWOT Analysis

STRENGTHS

The strongDM platform combines connectivity, authentication, authorization and audit capabilities in a single "cloud-native PAM" offering. Protocol-aware proxy, commitment to user experience, breadth of resources supported and strong financial backers are other strengths.

WEAKNESSES

StrongDM is still in the early stages and will need to raise market awareness to stand out in a highly crowded and competitive PAM market that includes over 40 different vendors.

OPPORTUNITIES

Companies looking to do "modern" PAM in a cloud-native, DevOps-centric world are likely targets for strongDM. PAM is no longer just for DBAs, developers, engineers and IT administrators; nearly everyone who needs to work with technology is a potential customer.

THREATS

StrongDM's challenge will be to convert customers to a new way of thinking about PAM, as well as fend off inevitable responses from legacy PAM vendors retooling or expanding their offerings.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence