Endpoint Privileges Management and More

Data and intellectual property are some of the most important assets an organization owns, but their fluidity makes them difficult to quantify. As a result, business needs are often pitted against risk mitigation. Privileged access management (PAM) is a core piece of the equation, one that can effectively insulate against most data breaches and drives a quick and visible return on investment for organizations.

As a cybersecurity leader, Optiv provides an effective array of service offerings for clients, including strategies for handling privileged access and assistance with the complete roll out of industry-proven PAM programs.

Optiv Solutions

Optiv’s methodology includes planning for your business outcomes and designing, developing and implementing your technology based on best practices. Our industry-leading position in the field drives a holistic perspective and we incorporate organizational change management as part of the process.

Password and Secrets Management
Provides credentials management within an organization’s privileged access infrastructure, including privileged user access, OS level access, database level access and any other human-specific privileged access accounts within the environment.

Endpoint Least Privileged Management
Focuses on the device level least privilege principle, which restricts users or processes from being granted access rights in excess of those specifically required for the performance of their defined tasks. They are elevated to those privileges in real-time only when necessary. Other functionalities include ransomware protection, threat detection/prevention and just-in-time access, which allows access for specific times and tasks.

Application to Application Integrations
An extension of privileged access management, strictly focused on interactions between applications and their services/deps.

Secure Remote and Vendor Access
Provides external access to an organization’s environment without using VPN for access. These solutions may also provide session management and isolation to prevent internal credentials from being externally viewed.

Identity Solutions
Focuses on identity and access management (IAM) tools and account lifecycle management. These solutions look at the entire life of a privilege credential and provide provisioning, attestation and certification.

How Do We Do It?

Phase 1: Discovery
- Optiv’s experts identify the client’s current concerns
- Experts provide policy and governance assistance to better align outcomes with client expectations
- Identify target use cases

Phase 2: Design
- Experts build a technical and/or business architecture that best addresses the use cases defined in the discovery process

Phase 3: Installation
- If necessary, components will be installed in system
- Configuration with third-party services as part of process

Phase 4: Implementation
- Experts collaborate with stakeholder teams to onboard credentials, users or other necessary configuration details to address use cases
- Architecture testing with stakeholder teams

Phase 5: Go-Live
- Assist clients with any needed documentation (SOP, job aids, operations guides) to ensure a smooth transition process into production
- Provide any required technical assistance to ensure a successful transition to production
Why Clients Choose Optiv

**Industry Awards**
CyberArk North America 2019 Partner of the Year (four consecutive years)
Okta 2019 Partner of the Year
BeyondTrust Americas Partner of the Year 2019 (three consecutive years)
Continuous vendor exploration of new and emerging PAM products

**12+ Years**
The average experience of Optiv’s IDM team

**100,000+ Hours**
Identity services delivered annually

**Certified Solution Architects & Engineers**
CyberArk
BeyondTrust

Case Study
Large medical device company

**Desired Outcomes**
The client was seeking assistance with their global expansion of its current PAM implementation.

**Solution**
Optiv conducted a 240-hour in-depth architecture, design and use case analysis to ensure the purchase of appropriate software licenses, infrastructure setup and long-term global growth with the current PAM solution.

**Client Benefits**

- **Additional services**
  - PAM – More than 1,000 hours to support their global deployment
  - Architectures, design and use case analysis
  - Infrastructure global solution buildout (Dev, UAT and Prod)
  - Data migration from version 7.x to 9.x (17k+ accounts)
  - Multiple phased use case configuration (EPV, PSM, PSMP, etc.)
  - More than 100k privileged accounts to be integrated on a variety of end points with automated password rotation and policy configuration

Statistics

**15 Years Average Experience:**
Former Big 4 IAM leaders, IAM directors, enterprise architects, risk/compliance auditors

**Team-Based Delivery:**
Multiple consultants on most engagements, providing depth of knowledge and acceleration of outcomes

**Strategy into Action:**
Deliver quality and executable ‘Day 2’ actions

**Accelerated Value Realization:**
IAM paired with OCM to maximize stakeholder buy-in, drive user adoption, measure value

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2022 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.