



Presentation: State and Local Cybersecurity Grant Program (SLCGP) Overview





State and Local Cybersecurity Grant Program (SLCGP) Overview

Agenda

- **Introductory Letter**
- **Notice of Funding Objective and Overview**
- **BeyondTrust Overview**
- **BeyondTrust in Public Sector**
- **Aligning BeyondTrust Driven Outcomes to Grant Initiatives**
- **Meet the BeyondTrust Public Sector Team**
- **Partners in Success**



Introductory Letter

State and Local Grant Program Introductory Letter

You may be aware of a recently issued State and Local Cybersecurity Grant Program (SLCGP). cybersecurity grant program. This grant program, funded by DHS and managed by CISA and FEMA, allows states, local governments, rural areas, and territories (SLT) to request funds from a pool of \$185 million available in 2022. From the overview (linked above), “the program enables DHS to make targeted cybersecurity investments in state, local and territorial government agencies, thus improving the security of critical infrastructure and resilience of the services that STL governments provide to their communities”. The deadline for grant application submission is 11/15/2022 (by 5pm ET).

At BeyondTrust, we have the privilege of working with a significant number of state, local, and territory stakeholders. Our team understands what cyber threats you face and what outcomes you are trying to drive. The grant program stipulates that money must align to one or more of sixteen overarching initiatives. We have attached a presentation that details our alignment to these initiatives, what outcomes can be driven to support your mission, and how to meet the program’s reporting requirements.

Privileged Access Management (PAM) should be a part of any public sector cybersecurity program and our experience makes us confident that we can help improve your security posture. The following presentation will cover:

- Notice of Funding Objective and Overview
- BeyondTrust Overview
- BeyondTrust in Public Sector
- Aligning BeyondTrust Outcomes to Grant Initiatives
- Meet the BeyondTrust Public Sector Team
- Partners in Success

We look forward to discussing your plans and objectives and how this grant can be used to further your cybersecurity stance. If there are partners or integrators that you are working with on existing cybersecurity initiatives, we are happy to share content and work alongside them in your pursuit of grant awards.

Thanks,

BeyondTrust Leadership Team

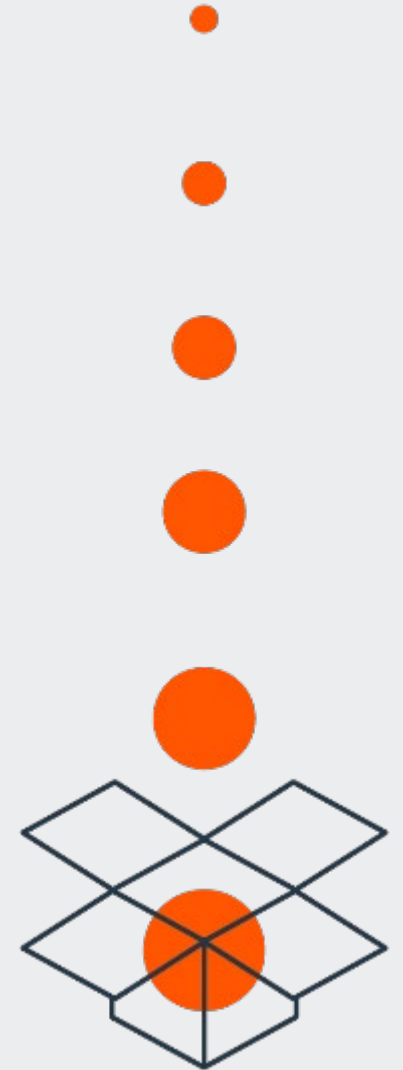


Notice of Funding Objective and Overview

Objective and Overview

Objective - The objective of the SLGCP is to fund State, Local and Territorial (SLT) government efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States.

Overview - In September 2022, the Department of Homeland Security (DHS), in conjunction with the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA), announced a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country. The [SLCGP](#) will provide \$1 billion in funding to SLT partners over four years to support efforts to address cyber risk to their information systems. This program appropriated \$185 million for FY22, \$400 million for FY23, \$300 million for FY24 and \$100 million for FY25. [Grant application docs](#) are due 11/15/22 and there is considerable doc prep required. Our SLED GTM team will be assisting CIOs, CISOs, State Cyber Committees, and Partners with document preparation based on the Cybersecurity Plan Elements, as well as for building future cybersecurity plans. This will be an ongoing campaign with ongoing conversations and education.





BeyondTrust Overview



1,400+ Employees

20 Countries

2003 Founded



Market Leader

Ranked as a PAM leader by Gartner, Forrester, and KuppingerCole



Global Presence

~20k customers in 100+ countries and extensive partner network



Integrated Platform

Unified platform with seamless third-party integrations



Broadest Portfolio

Best-in-class identity and privileged access solutions



Customer Driven

90%+ gross retention and exceptional customer support and success



Technology Pioneers

Heritage of innovation with 75+ patents and commitment to R&D

Company Overview

Headquarters **Atlanta, GA | USA**

Global Offices **Americas, EMEIA, APJ**

Privately Held **Francisco Partners & Clearlake Capital**

We are the leader in Intelligent Identity & Access Security



Our Vision

A world where identities and access are protected from cyberthreats



Our Mission

To protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world

Attacks on privileged identities and access are relentless, and the stakes are higher than ever.

What factors are driving the increase in privileged sessions (human or machine) **in your organization?**

36%

Expanded scope of regulatory requirements on what is considered privileged access

37%

Greater reliance **on third parties** (vendors, partners)

48%

Growth in **cloud accounts**

55%

Wider scope of who is considered privileged (developers, finance, HR, etc.)

56%

Increase in the number of machines identities requiring privileged identities

60%

Increased remote access infrastructure requirements

SOURCE: A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020

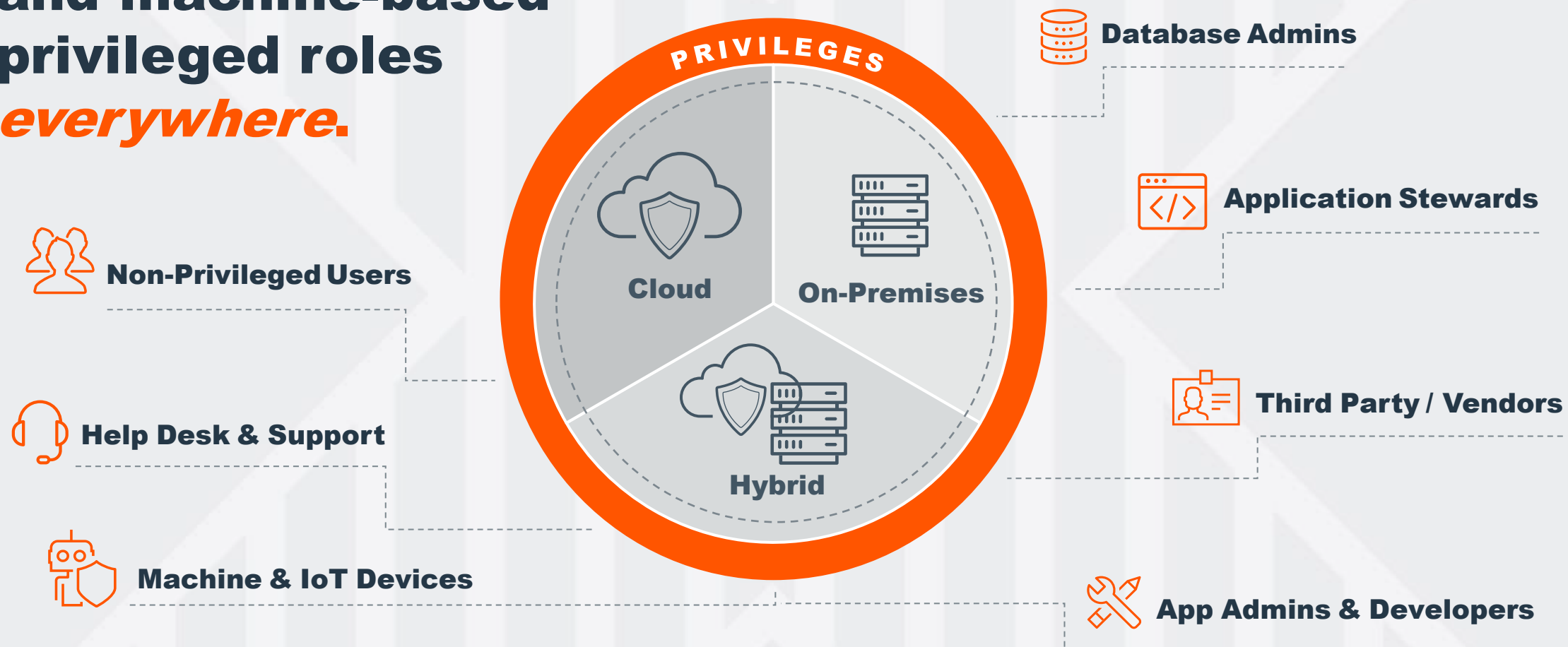
The evolving threat landscape is creating a new urgency to achieving cybersecurity goals

- Controlling **access** for vendors and remote workers
- Securing **expanding cloud** infrastructure
- Mitigating **ransomware** attacks
- Supporting **digital transformation** initiatives
- Enabling a **zero trust** posture
- Driving **IT efficiency** and automation
- Maintaining **compliance** and **cyber insurance** policies

**How are you managing
and controlling privileged
identities and access
to protect your
organization?**



You have user and machine-based privileged roles *everywhere.*



**Threat actors
are targeting
broader
identity attack
vectors due to
inadequate
protection**

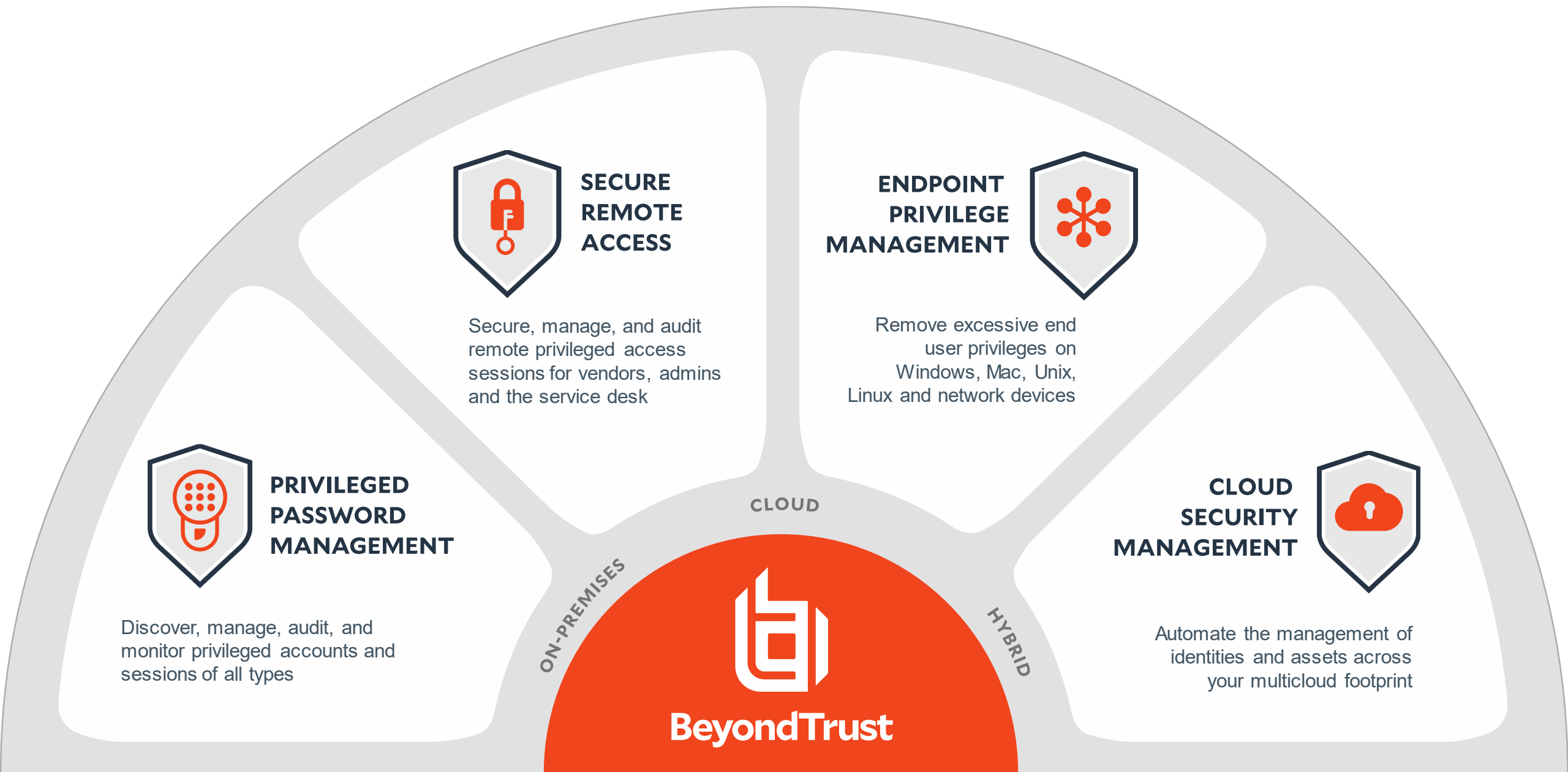


**How are you shrinking
the windows of
exposure across a
widening attack
surface?**



Our integrated platform and solutions **protect all identities, access, and endpoints** across your entire environment.

We've got you covered.



BEYONDINSIGHT

Discovery













Reporting

Threat Analytics

Connectors

Central Policy & Management

Innovative Product Portfolio

Category	 PRIVILEGED PASSWORD MANAGEMENT		 SECURE REMOTE ACCESS		 ENDPOINT PRIVILEGE MANAGEMENT			 CLOUD SECURITY MANAGEMENT
Products	 Password Safe	 DevOps Secrets Safe	 Privileged Remote Access	 Remote Support	 Privilege Management for Windows & Mac	 Privilege Management for Unix & Linux	 AD Bridge	 Cloud Privilege Broker
User	Security / IAM Ops IT Admins Compliance	Security / IAM Ops DevSecOps Engineers	IT Operations OT Admins MSPs	Service Desk Support Centers	Endpoint Security Mgrs IT Operations Desktop/Server Admins	Auditing / Compliance Security Admins	Auditing / Compliance Security Admins	Cloud / IT Operations Site Reliability Engineers Developers
Key Benefits	Password Vaulting Privileged Account & Session Mgmt Auditing	Secrets Management & Security	Session Mgmt Vault & Auditing for Remote and Vendor Access	Remote Support Screen Sharing Chat Support ITSM Integration Unattended Support Mobile Support	Least Privilege & Advanced Application Control	Root Access Control Auditing Governance for Unix & Linux	Extension of AD Authentication SSO to Unix & Linux	Cloud Infrastructure Entitlements Management Least Privilege in Cloud Footprint
Cloud and On-Premises Deployments								

 Highlights particular grant element alignment



BeyondTrust in Public Sector

Public Sector Reference Customers



Bureau of Workers' Compensation



Department of Finance & Administration

Fulton
County Schools
Where Students Come First




LOUDON
COUNTY
PUBLIC SCHOOLS



Thought Leadership Content

- [Zero-trust architecture demands a new view on data security](#) (GCN)
- [Achieving zero trust requires changing data security views](#) (Federal News Network)
- [3 best practices to manage cyber insurance](#) (eCampusNews)
- [Threats Against Critical Infrastructure Are Looming, Agencies Must Safely Modernize OT Systems](#) (Cyber Defense Magazine)
- [NASCIO 2022 Key Takeaways](#) (BeyondTrust Blog)
- [New National Cybersecurity Strategy: A Much-Needed Overhaul for Digital Ecosystems](#) (NextGov)
- [Amid Digitization of Public Infrastructure, Cybersecurity is Increasingly a Challenge](#) (American City & County)
- [Addressing Urgent Security Needs for Operational Technology](#) (FedInsider)

Mapping BeyondTrust Capabilities to NIST SP 800-207

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.

Read this whitepaper to learn how BeyondTrust Privileged Access Management (PAM) solutions map into guidelines set forth in the NIST Special Publication (SP) 800-207 on Zero Trust Architecture.

[Read the Whitepaper >](#)



[Explore More BeyondTrust Thought Leadership Here](#)



Aligning BeyondTrust Driven Outcomes to Grant Initiatives

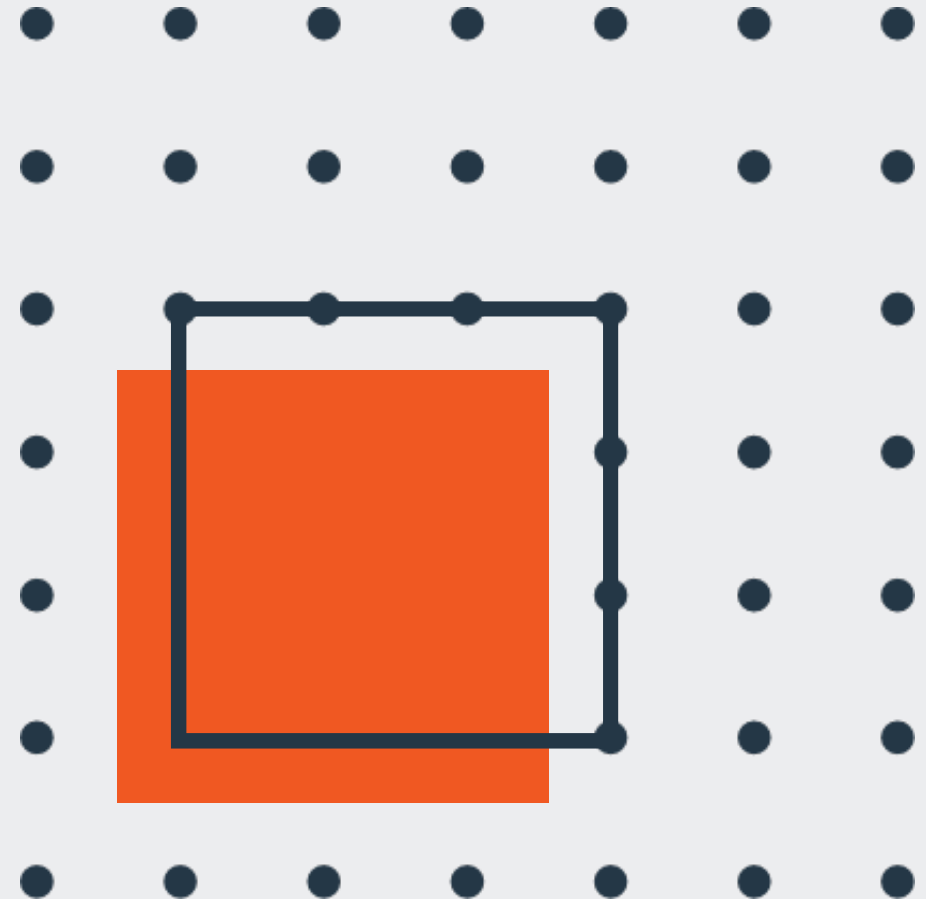
Required Plan Elements

There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities.

They also include specific **cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats.**

While each of the 16 required elements must be addressed in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized.

Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.



Plan Elements and Corresponding Case Studies (Outcomes)

Plan Element 1- Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

Much like plan element 1 lays out, the IL DOIT used [Password Safe](#) and [Endpoint Privilege Management](#) to gain operational control over application permissions, user account permissions, and associated credentials as a part of their BeyondTrust roll out. As is required by the SLCGP grant, auditing was a major benefit of the implementation of these BeyondTrust solutions, as the before and after state (as well as the interim impact) can be generated in reporting.



Plan Element 5e- Prohibit use of known, fixed, default passwords and credentials.

Prohibiting the use of known/fixed/default passwords and credentials is a good goal, but organizations need a solution that will help achieve that mission, or productivity will grind to a halt. [Password Safe](#) allows static credentials to be replaced with dynamic, vaulted credentials... credentials (extending to service accounts and application passwords as well) that will be rotated upon use and that never need to be known by a person. This shift in dynamic not only improves the workflow for users, but it also dramatically shrinks the attack surface.

[Link to the IL DOIT Case Study on Our Website](#)

Plan Elements and Corresponding Case Studies (Outcomes)

Plan Element 7- Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.



Plan Element 9- Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

Continuity of operations and communication are necessary components of a cybersecurity plan both during normal operations and in times of crisis (like the IL DOIT experienced in the aftermath of ransomware).

BeyondTrust [Privileged Remote Access](#) is leveraged across our Public Sector customers and is the gold standard of session management for internal IT teams, developers, contractors, and vendors. Connect to any device, anywhere, with no VPN required, while also gaining an unimpeachable audit trail. This audit trail is not only good for audit/compliance purposes, but also to meet the reporting requirements of the cybersecurity grant.

[Link to the IL DOIT Case Study on Our Website](#)



INDUSTRY

State of IL DOIT

PRODUCTS

Password Safe

Privilege Management for Windows
Desktops,

Privileged Remote Access

All Cloud Deployments

Extended Remote Access Security While Saving Time & Money

CLIENT

- Relationship began in 2020, in which they utilized our Remote Support product to quickly enable remote work for all state employees.

PROBLEM

- Then, in 2021, the IL Attorney General was hit with a ransomware attack, so Adam Ford (CISO) and his team came to us to help secure their organization and prevent cyber-attacks from occurring in the future.

OUTCOME

- Reduced risk of a future cybersecurity breach.
- Achievement of security goals and compliance requirements (audits).
- Comprehensive visibility across network.
- Easier management of IT infrastructure through a common platform.



Additional Public Sector Case Studies



INDUSTRY

Higher Education

PRODUCTS

Privileged Remote Access

Password Safe

“BeyondTrust gives us a level of control and capability that we never had before... I would have started on this project much sooner had I know how painless BeyondTrust has made it.”

Chris Stucker
Associate IAM Director

Leveraging **Just-in-Time PAM** to **Mitigate Risk & Achieve Full Visibility**

PROBLEM

- Secure a diverse user population with a wide variety of roles and access requirements, including students, faculty, university hospitals and healthcare systems, some of which overlap
- Protect this complex group of users with complete Privileged Access Management (PAM) solution that manages and controls the many different types of privileged accounts
- Meeting the compliance requirements of instruction's hospital status

OUTCOME

- Implemented a Just-in-Time Privileged Access Management (JIT PAM) model to enforce true “least privilege”, in conjunction with Password Safe
- Gained a true understanding of privileged access at the university to mitigate internal and external threats, with the ability to quickly provision accounts
- Achieved full visibility and security of their robust environment of users



SOCOM

INDUSTRY

Department of Defense

PRODUCTS

Password Safe

Remote Support

Unified combatant command charged with overseeing various special operations component deploys BeyondTrust universal privilege management to support zero trust objectives

ABOUT

USSOCOM develops and employs fully capable Special Operations Forces to conduct global special operations and activities as part of the Joint Force to support persistent, networked and distributed Combatant Command operations and campaigns against state and non-state actors to protect and advance U.S. policies and objectives

PROBLEM

Manually rotating passwords on 3,000 service accounts spread across 3 separate enclaves

Significant number of man hours being spent on a task that can be automated and audited

SOLUTION

SOCOM quickly narrowed their PAM alternatives to the top providers as ranked by industry analyst – BeyondTrust and CyberArk. An in-depth assessment resulted in the selection of BeyondTrust based on the following distinctives:

- ✓ Most comprehensive suite of integrated PAM capabilities
- ✓ Unified platform for ease of deployment, management, and sustainment
- ✓ Open Architecture for quick deployment and interoperability with the larger Zero Trust construct



Defense Manpower Data Center

INDUSTRY

Department of Defense

PRODUCTS

Password Safe

DevOps Secrets Safe

Endpoint Privilege Management
(Windows, Unix, Linux)

Remote Support

AD Bridge

One of World's largest identity organizations deploys BeyondTrust Universal Privilege Management to support Zero Trust Objectives

ABOUT

Serves under the Office of the Secretary of Defense. DMDC maintains information on Department of Defense (DoD) entitlements, benefits, and medical readiness for uniformed Service Members, Veterans and their families.

PROBLEM

As one of the world's largest identity organizations, securing sensitive data is a top priority. DODCAR compliance considerations led to the decision to implement Zero Trust principles. Core to the initiative was to evaluate leading PAM solutions that would discover, onboard and place under management privileged accounts, secure DevOps secrets, and to enforce least privilege across their Window, Unix, and Linux environments to stop unauthorized lateral movement across the network.

SOLUTION

DMDC quickly narrowed their PAM alternatives to the top providers as ranked by industry analyst – BeyondTrust and CyberArk. An in-depth assessment resulted in the selection of BeyondTrust based on the following distinctives:

- ✓ Most comprehensive suite of integrated PAM capabilities
- ✓ Unified platform for ease of deployment, management, and sustainment
- ✓ Open Architecture for quick deployment and interoperability with the larger Zero Trust construct



INDUSTRY

Department of Defense

PRODUCTS

Password Safe

ABOUT

PCTE is a training platform supporting standardized Joint Cyberspace Operations Forces individual sustainment training, team certification, mission rehearsal and provides the foundation for collective training exercises.

PROBLEM

PCTE has no password management solution. A lot of administrators and vendors are required to maintain the application. A solution is needed to add security, tracking and reporting.

POSITIVE BUSINESS OUTCOMES

- Admins & users have right privileges to do their jobs
- Eliminate unmanaged credentials & reduce attack surface
- Frictionless user experience
- Improve productivity & scale as the organization changes

SOLUTION

PCTE quickly narrowed their PAM alternatives to the top providers as ranked by industry analyst – BeyondTrust and CyberArk. An in-depth assessment resulted in the selection of BeyondTrust based on the following distinctives:

- ✓ Most comprehensive suite of integrated PAM capabilities
- ✓ Unified platform for ease of deployment, management, and sustainment
- ✓ Open Architecture for quick deployment and interoperation with the larger Zero Trust construct



Meet the BeyondTrust Public Sector Team

Meet the BeyondTrust Public Sector Team



[Blaine Segal](#)
RVP, Federal Sales
bsegal@beyondtrust.com
704-663-3178



[Sophie Brown](#)
Director, SLED Sales
sbrown@beyondtrust.com
770-238-9703



[Joe Durante](#)
Director, SLED Sales
jdurante@beyondtrust.com



Partners in Success

Cybersecurity Grant Partners

We look forward to discussing your plans and objectives and how this grant can be used to further your cybersecurity stance.

Below are a few partners we are teaming up with on this grant. However, if there are partners or integrators that you are working with on existing cybersecurity initiatives, we are happy to share content and work alongside them in your pursuit of grant awards.

- Insert Partner logo/contact info



Thank You



Thank you for downloading this BeyondTrust Presentation! Carahsoft is the distributor for BeyondTrust solutions available via CMAS, NJEdge, OHS STS 0119Y, and other contract vehicles.

To learn how to take the next step toward acquiring BeyondTrust's solutions, please check out the following resources and information:



For additional resources:
carah.io/beyondtrustresources



For upcoming events:
carah.io/beyondtrustevents



For additional InQuisient solutions:
carah.io/beyondtrustsolutions



For additional Cybersecurity certified solutions:
carah.io/cybersolutions



To set up a meeting:
beyondtrust@carahsoft.com
(866)-421-4683



To purchase, check out the contract vehicles available for procurement:
carah.io/beyondtrustcontracts