RFI Response

Ensuring the Continued Security of the United States Critical Electric Infrastructure

Prepared By:

Merlin Cyber
8330 Boone Blvd,
8th Floor
Vienna, VA 22182

June 7, 2021

Energy Resilience Division of the Office of Electricity
U.S. Department of Energy
1000 Independence Avenue SW, Washington, DC 20585
Attention: Michael Coe

Reference: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

To Whom It May Concern,

Merlin International, Inc. (Merlin) is pleased to provide the Energy Department (DOE) with the following submission in support of Ensuring the Continued Security of the United States Critical Electric Infrastructure.

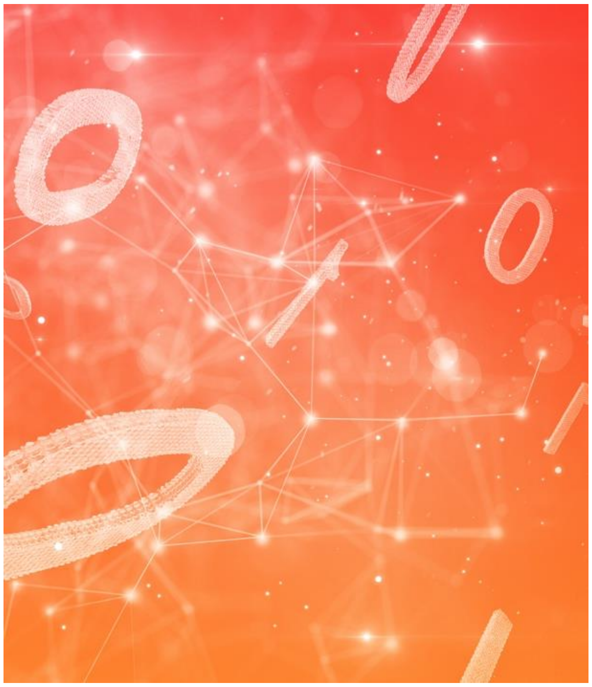
Merlin International is a leading provider of next-generation cybersecurity solutions that protect government and commercial organizations. Merlin offers a broad portfolio of solutions that secure the enterprise from endpoints to networks, from governance to risk management, from infrastructure to information. Combining solutions with deep industry expertise and experience, Merlin delivers the cybersecurity solutions that organizations need to protect their most critical business assets while furthering their mission.

Merlin appreciates your consideration of our response. We look forward to building an enduring, long-term professional relationship, and will do our utmost to ensure complete satisfaction. Should you have any questions regarding this RFI response, please do not hesitate to contact Tom Steiner at 404-444-4856 or tsteiner@merlincyber.com.

Sincerely,

Julie Xiang
General Manager
Merlin International®
703.752.8361

Strengthening DOE's Supply Chain Risk Management (SCRM) through the Executive Order's Direction to Adopt Zero Trust IT Architecture



The Energy Department (DOE) has critical cyber security requirements in support of ensuring the continued security of the United States critical electric infrastructure. Like much of the government, DOE's Cybersecurity team performs its essential functions while fending off an increasing number of novel and advanced attacks. Always in pursuit of new technologies to help improve visibility and address cyber threats from malicious adversaries, DOE would benefit from novel ways to monitor and protect the supply chain that feeds into its IT infrastructure.

With a focus on strengthening overall supply chain risk management (SCRM), the following response features several best-of-breed IT security technology solutions that address various layers of an enterprise's IT infrastructure backbone. Many of these security tools are well-known and industry-leading, and a few that Merlin has included are more emerging, "bleeding edge" approaches that DOE should consider adopting to stay ahead of the cyber threat landscape.

Per the May 2021 Executive Order, Zero Trust Architecture is a modern lens through which DOE should assess its IT readiness and supply chain risk. Merlin understands that Zero Trust is becoming an agreed upon framework that over time will drive the direction of cybersecurity posture across the Federal government. NIST's Publication 800-207 addresses Zero Trust Architecture, which is the recent step taken by the Federal government toward security based on Zero Trust principles.

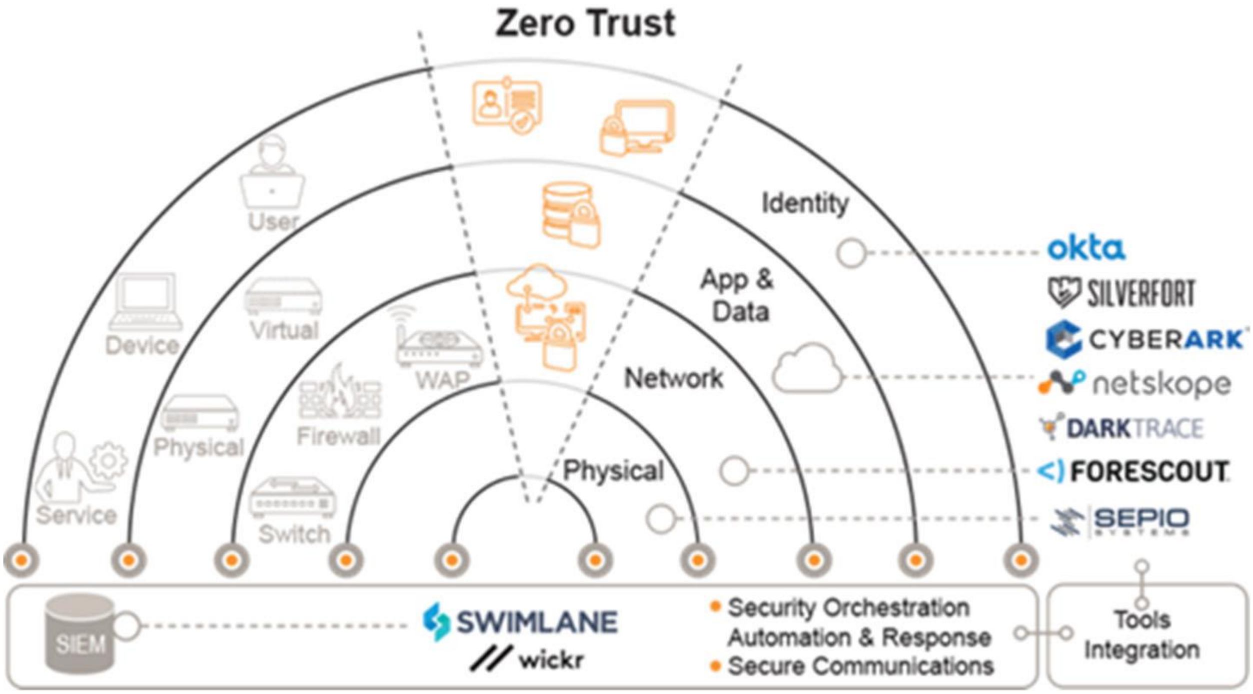
As a cybersecurity provider, Merlin has a handpicked portfolio of leading technologies that we prescriptively provide to Federal agencies to help in their SCRM strategies and secure their IT Operations as they fulfill their missions.

For DOE and its evolving cybersecurity needs as the momentum moves toward Zero Trust, Merlin is accessible to address any gap in security coverage that any DOE agency or office may have. This response discusses how cybersecurity tools, many that DOE know and some that will be new to the Department, ***when synergistically used together***, can help DOE organizations move toward Zero Trust.

We discuss several key IT layers that should be in part considered in DOE's Zero Trust strategy. Merlin articulates how the layers are interconnected and secured with market leading technologies. Note throughout this response that Merlin has partnered with best-of-breed, Gartner-rated Original Equipment Manufacturers (OEMs) to help support your cybersecurity goals.

Merlin has a strategic advantage for DOE: We are highly skilled experts in understanding how the synergy of cybersecurity tools, when deployed together can deliver exponential impacts to security posture. The alternative is engaging one OEM on their single technology which may present bias in understanding the interconnectedness of cyber tools and alignment with Zero Trust. Since Merlin has strong expertise in more than a dozen OEM tools and cycles-in new technologies into our portfolio to continuously meet new cyber threats, we can help DOE figure out how to blend new technologies into the existing technology stack to strengthen security posture and move toward Zero Trust.

Merlin Technology Stack



How do Merlin products fit into the logical design of a Zero Trust Architecture as documented in the latest draft of NIST SP 800-207 "Zero Trust Architecture"?

Our cybersecurity solution portfolio for Zero Trust is comprised of industry leaders such as Okta and CyberArk along with innovative, disruptive companies like Silverfort, Darktrace and Sepio. Each of our vendor partners bring unique and critical capabilities for Zero Trust while providing integration and policy enforcement points that allow solution interoperability.

Our strategic solutions portfolio aligns with the Zero Trust Pillars and CDM as described below.

Users:

- Following our core tenets of "Identity as a Perimeter" and "Least Privilege", our solutions focus on user identity as an integral policy enforcement point. We enable cloud scalability and agility with an identity-as-a-service offering. Our solutions protect administrative and non-administrative users enterprise and all assets whether legacy on-premise or in the cloud.

Both Okta and CyberArk are approved products on the CDM APL and meet the PRIV, CRED and TRUST requirements when assessing and reporting on the users in the enterprise.

Devices:

- Our solution can use both agent-based or agentless discovery and management of endpoints on your network. With Forescout, we provide a platform that discovers, manages, and protects IT/OT devices on your network. It is the primary solution leveraged by CDM for HWAM and advanced network access control. To extend Forescout's capabilities, we provide rogue devices and rogue peripherals mitigation with Sepio Security. We uniquely discover these rogue devices that are often missed by traditional network security solution by detecting the physical or OSI layer 1 characteristics. We create a database of these rogue devices and alert administrators when they are detected on the network. Lastly, the Darktrace solution creates device and network models that alert when anomalous behaviors are detected. Each of these solutions can report up to the CDM Dashboard.

Network:

- Our core tenets provide us with fundamental principles for the design and management of secure networks. We practice the design principle of the identity as the perimeter and granular policy enforcement point. When user or device identity are established as the security boundary, it provides the ability to create micro-segmented networks and build intrinsic workload security, thus bringing good network security practices to the forefront.

- Forescout, Darktrace and Sepio the foundation for our network security. We extend security capabilities to networks and resources in the cloud through the Netskope Cloud Security platform. With Netskope Private Access, we can ensure that remote users are directly connected only to the applications they are authorized to use and do not have broad network-level access to environments. Reporting on network access can be pulled via API and ingested into DHS's CDM capabilities to enrich analytics and mitigation protocols.

Application:

- Our solutions protect applications whether on premise or in the cloud. Our identity security solutions ensure that only the right individuals have access to the applications through entitlements using least privilege principles. The Netskope Cloud Security solution has catalogued and assessed the risks of 30,000+ cloud applications. With Netskope, we can securely connect users to applications, monitor and govern the users' access. Each of these solutions provide rich APIs that can inform the DHS CDM dashboards.

Automation:

- Integration & Automation is a core tenet of our Zero Trust architecture. Our solutions provide a rich set of open APIs that allow security capabilities in each of the Zero Trust pillars. We extend using policies at the identity, application, data, and network domains.

- A key component of our automation capabilities is the use of a security orchestration and automation platform. Swimlane provides an extensible framework for creating playbooks that can automate the response to events and incidents. Swimlane helps automate and orchestrate all the manual, recurring, and repetitive tasks that come with managing an increasingly diverse security stack. The solution accelerates threat management by correlating alerts across security tools.

Analytics:

- Analytics capabilities for our Zero Trust framework span each of the IT domains. Risk-based authentication can detect user and device posture prior to allowing access to resources. Using AI/ML, Darktrace uses analytics to create network and device models. This approach leverages analytics for early threat detection and autonomous response. The solution uses AI/ML to understand the unique "patterns of life" for every user, device, and technology that are on the network, constantly learning and adapting as your agency evolves. This powerful feature recognizes malicious behavior without a pre-configured definition of "good" or "bad," spotting even the most subtle anomalies that may point to a novel or advanced cyberattack.

Zero Trust is an incremental journey with risk tolerance, speed of execution, and breadth of implementation, all as key considerations. No matter where an agency is in its path to Zero Trust, we deliver the solutions needed at the pace and scope desired. With our portfolio of best-in-class security partners and emerging technologies, we can secure every layer of DOE's IT stack, from endpoints to applications, to data and users.

A Closer Look at Each Merlin Technology

Sepio

Founded in 2016 by cybersecurity industry veterans, Sepio HAC-1 is the first hardware access control platform that provides visibility, control, and mitigation to C2C, Zero Trust, insider threat, BYOD, IT, OT and IoT security programs. Sepio's hardware fingerprinting technology discovers all managed, unmanaged and hidden devices that are otherwise invisible to all other security tools. Sepio is a strategic partner of Munich Re, the world's largest reinsurance company, and Merlin Cyber, a leading cybersecurity federal solution provider.

Federal agencies and the nation's critical infrastructure - such as energy, transportation systems, communications, and financial services-depend on IT systems to carry out operations and process essential data. But the risks to these IT systems are increasing insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. As per GAO's recommendation - Establishing a comprehensive cybersecurity strategy and performing effective oversight with regards to mitigation of global supply chain risks and possible malicious hardware is of the utmost importance, further emphasized by section 889b directive. Tackling this challenge requires complete visibility to your Hardware assets, regardless of their characteristics and the interface used for connection, as attackers take advantage of the "blind" spots - mainly through USB Human Interface Device (HID)emulating devices or Physical layer network implants. These challenges are also supported by the Comply-to-Connect and various Zero Trust guidelines. Securing your network assets at the hardware layer by using a field proven solution developed by Cyber Physical Security experts, will be the first step in bringing your cyber security posture to the next level.

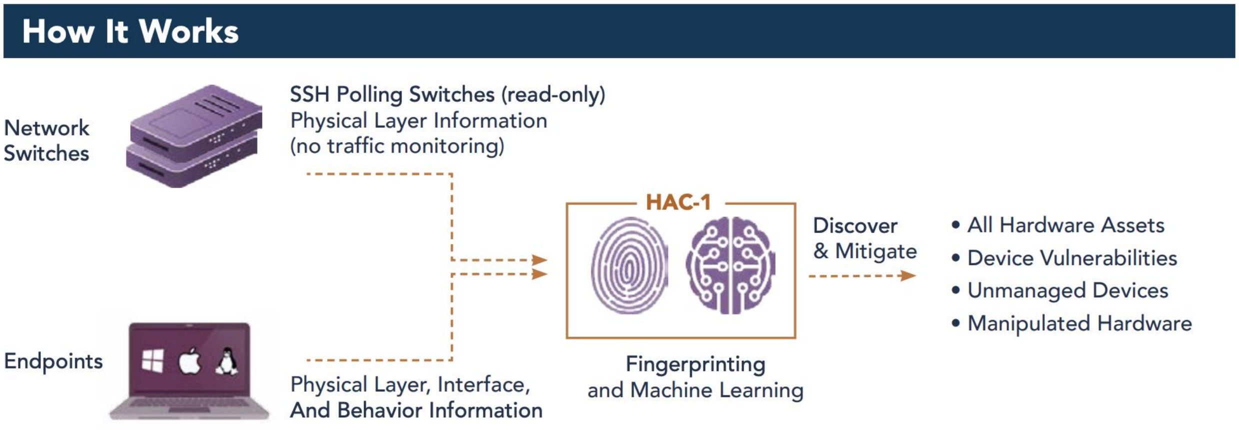
Some of the key challenges that federal agencies face are:

- Total visibility is required to account for all of the agencies' IT/OT/IoT assets - Knowing what you have, verifying what you own and only then trusting it.

- Spoofed devices, physical layer implants, “hiding” in the physical layer or impersonating as legitimate devices while sharing the same logical identification are hard to identify using existing technology.
- Rogue wireless AP’s that can be used for attacks both in the enterprise and WFH environment.

Sepio’s HAC-1 solution uses a unique algorithm based on physical layer fingerprinting module augmented by Machine Learning techniques. The unique approach allows HAC-1 to discover and report ALL devices, rogue devices included, enforce usage policies, deliver risk insights and device scoring. By enabling organizations full visibility of their IT/OT/IoT assets, a stronger cybersecurity posture and true Zero Trust methodology are achieved with the following highlights.

- Asset visibility
- Policy management
- Device risk scoring
- Risk insights & actionable playbook
- Embedded Device Threat intelligence database
- Extensive device hunting, IR & Forensic features
- Fully integrated with popular orchestration & automation products



Current technologies such as Network Access Control (NAC), End Point Protection (EPP), and Endpoint Detection and Response (EDR) solutions all suffer from a severe blind spot. They rely on the network and end point peripherals to “self-identify with Vendor ID, Product ID, MAC Address, or thru traffic analysis.

Those tools are blind to Rogue, Spoofed, Out-of-Band (Man in the Middle), MAC-less, and many OT and IoT devices.

Sepio's Hardware Access Control (HAC) platform requires only read-only access to pull existing metadata from network switches such as Voltage, Resistance, Noise, Power over Ethernet, etc. There are about 25 electronic characteristics that every device emits that Sepio's HAC system uses along with Machine learning and an 80M fingerprint Knowledge Base to detect and identify IT, OT, and IoT device on the network.

Darktrace

In today's complex digital environments, machines are fighting machines, and advanced attackers and criminal groups are contriving sophisticated new ways to perpetrate their missions. The corporate network has become a battlefield, where the stakes are control of digital assets and, ultimately, the ability of the organization to function.

The danger today is not just the classic scenarios of data theft, or a hacked website, but the silent threat lurking beneath the surface. These attackers are quiet, creeping in unannounced, and surreptitiously changing data at will, or installing kill switches ready to be activated. Using custom code, only crossing the perimeter boundary once and never sending information outside, such threats are almost impossible to find.

Against this new reality, legacy security systems are failing because the traditional approach to cyber security relies on being able to define the threat in advance. Rigidly programmed to only detect known threats, this approach is no longer viable. From novel and fast-spreading attacks to insiders gone rogue, from hacked IoT devices to compromised supply chains, the threat landscape evolves in unpredictable ways and a new approach to cyber defense is urgently required. Even systems designed to look at anomalous behavior do so via deep packet inspection and require significant tuning. At the same time these solutions look only at the network session data and headers rather than the behavior of the user or the application. This can lead to massive numbers of false positives that simply get tuned out and turned off

Under this new paradigm, AI technology can identify and neutralize previously unseen cyber-threats. While machine learning has the power to transform cyber defense, the challenge of getting it to work at scale, in a variety of dynamic data environments, while detecting genuine threats in real time, without human intervention, is not trivial.

With the first AI for cyber defense proven to work across diverse digital enterprises, Darktrace is the world leader in detecting and autonomously responding to cyber-threats that legacy systems miss. Powered by machine learning and AI algorithms, Darktrace's 'immune system' technology is used by thousands of organizations worldwide.

Darktrace provides its unique approach to machine learning and shines a light on the unique interplay between unsupervised machine learning, supervised machine learning, and deep learning behind the world's leading cyber AI technology.

Machine Learning & Cyber Security

Traditional approaches to cyber security are based on identifying activities that resemble previously known attacks – the "known knowns." This is usually done with a signature- based approach, whereby a database of known malicious behaviors is created. New activities are cross-referenced with the database, and those that match are flagged as threats. While this is an improvement it is still limited in its approach.

These solutions sometimes also use methods based on supervised machine learning, which help to classify the output of the signatures. Using this supervised approach, a system is fed a training data set in which each entry has been labeled as belonging to one of a set of distinct classes.

In the information security context, the system is trained using a database of previously seen behaviors, where each behavior is known to be either malicious or benign and is labeled as such.

New activities are then analyzed to see whether they more closely match those in the malicious class, or those in the benign class. Any that are evaluated as being sufficiently likely to be malicious are again flagged as threats.

Systems that rely entirely on supervised machine learning have fundamental weaknesses:

- Malicious behaviors that deviate sufficiently from those seen before will fail to be classified as such, hence will pass undetected.
- A large amount of human input is needed to label the training data.
- Any mislabeled data or human bias introduced can seriously compromise the ability of the system to correctly classify new activities.

Machine learning has presented a significant opportunity to the cyber security industry. New machine learning methods can vastly improve the accuracy of threat detection and enhance network visibility thanks to the greater amount of computational analysis they can handle. They are also heralding in a new era of autonomous response, where a machine system is sufficiently intelligent to understand how and when to fight back against in-progress threats.

Darktrace's combination of machine learning approaches

While supervised machine learning can be powerful, Darktrace was founded with the vision to build the first self-learning cyber defense platform. Using unsupervised machine learning instead allowed the system to uncover rare and previously unseen threats, which did not rely on inherently imperfect training data sets. Data relating to historical attacks does not necessarily protect against future ones.

Having built the world's leading machine learning system for cyber security, which is based on this unique approach, Darktrace also uses deep learning techniques to supplement its AI engine with the specialized domain expertise of Darktrace's world-class cyber analysts.

Deployed extensively in thousands of real-world network environments, these new techniques are increasingly powerful, feeding our neural networks and allowing the power of unsupervised machine learning to be further augmented.

Unsupervised Machine Learning

Darktrace's unsupervised machine learning is critical because, unlike supervised approaches, it does not require labeled training data. Instead it is able to identify key patterns and trends in the data, without the need for human input. Unsupervised learning can therefore take computer processing beyond what programmers already know or can imagine and discover previously unknown relationships.

Darktrace uses unique unsupervised machine learning algorithms to analyze network data at scale and make billions of probability-based calculations based on the evidence that it sees. Instead of relying on knowledge of past threats, it independently classifies data and detects compelling patterns. From this, it forms an understanding of 'normal' behaviors across the network, pertaining to devices, users, or groups of either entity, and detects deviations from this evolving 'pattern of life' that may point to a developing threat.

Here are the core principles of Darktrace's machine learning:

- It learns what is normal within a network 'on the job' – it does not depend upon knowledge of previous attacks.
- It thrives on the scale, complexity and diversity of modern businesses, where every device and person is unique.
- It turns the innovation of attackers against them – any unusual activity is visible.
- It constantly revises assumptions about behavior, using probabilistic mathematics.
- It is always up to date and not reliant on human input.

The impact of Darktrace's unsupervised machine learning on cyber security is transformative. Its cyber AI technology has quickly proved itself capable of seeing hitherto undiscovered cyber events, from a variety of threat sources, which would otherwise have gone unnoticed. These include:

- Insider threat – malicious or accidental.
- Zero-day attacks – previously unseen, novel exploits.
- Latent vulnerabilities – dormant vulnerabilities that are undiscovered, often due to the lack of network visibility.
- Machine-speed attacks – ransomware and other automated attackers that propagate and/or mutate very quickly and are virtually impossible to stop and neutralize using human-dependent response mechanisms.
- Silent and stealthy attacks that lurk in networks undetected.

Technical Overview

Darktrace's transformative approach to cyber defense relies on probabilistic methods developed by Cambridge mathematicians. Employing multiple unsupervised, supervised, and deep learning techniques in a Bayesian framework, the Enterprise Immune System can integrate a vast number of weak indicators of anomalous behavior to produce a single clear measure of threat probabilities.

For each unique environment, Darktrace generates millions of interrelated mathematical models which are correlated to ensure that only truly anomalous behavior is detected without a profusion of false positives. Unlike rules-based computation, the results that probabilistic mathematics generate cannot simply be categorized as 'yes' or 'no' but instead indicate degrees of certainty, reflecting the ambiguities that inevitably exist in dynamic data environments.

Darktrace provides a living dashboard for analysts to investigate, document, and take action against threats within the environment. The intuitive nature of Darktrace threat dashboard combined with powerful RBAC allows analysts to see what they need to see, when they need to see it.

Autonomous Response with Darktrace Antigena

Because Darktrace's machine learning is capable of understanding, at a granular level, the 'pattern of life', and therefore detecting specific deviations from normal activity, it is also uniquely capable of generating an appropriate autonomous response to an in-progress attack.

Empowering the machine to fight back autonomously for the first time, Darktrace Antigena works like antibodies within the immune system, neutralizing a threat by enforcing the known 'pattern of life' of a device or user.

Thanks to Darktrace's core unsupervised machine learning, this solution can also learn from itself, as well as learning passively from the data that it observes. For example, when Darktrace Antigena generates an autonomous response action, a feedback reinforcement loop is triggered. The resulting behaviors on the network are analyzed in turn to facilitate diagnosis and inform any further actions. Unlike guided reinforcement learning, this process is driven autonomously by the machine itself rather than a human operator.

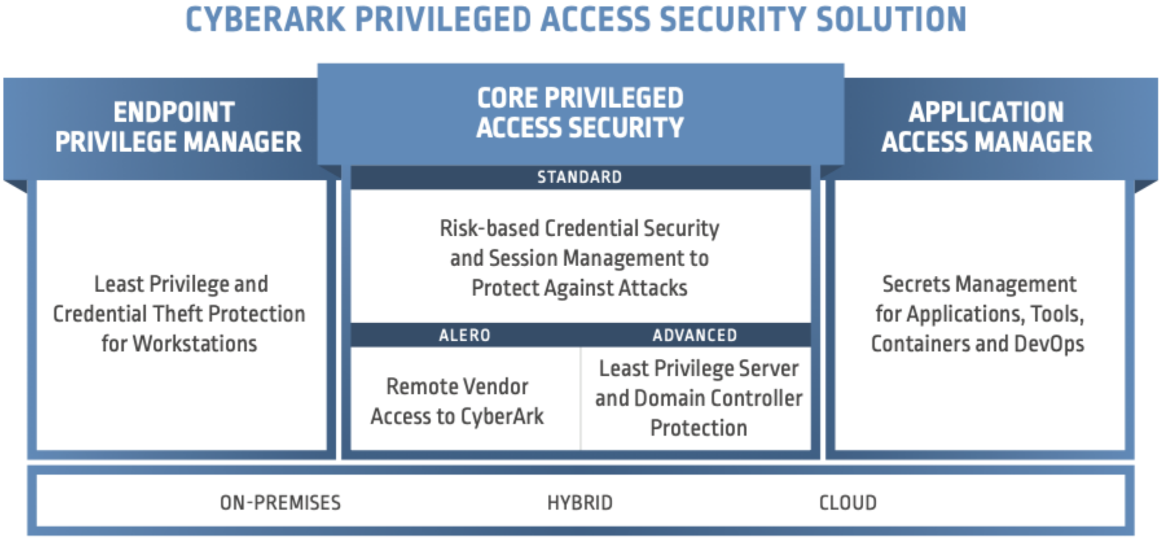
Critically, Darktrace Antigena is built on unsupervised machine learning proven to detect only the most abnormal cyber events to a degree of accuracy that enables it to take precise action in response. Machine learning used in this way does not replace the human's function, but ultimately serves to enhance it. Antigena acts faster than a human, buying the operator precious time to catch up and take further measures if necessary.

SOAR Integration and Automated or Confirmed remediation

In the case of SOAR integration, Darktrace has been successfully connected via the market leaders and emerging technology SOAR solutions including Swimlane, Phantom, and Demisto. Often the SOAR platform will be used for additional threat enrichment, help desk ticketing or providing the capability for human confirmation for both Antigena, NAC or EDR remediation and response. The SOAR capabilities are further enhanced by a rich API set to allow interaction of modern technologies.

CyberArk

CyberArk is the market leader and trusted expert in privileged access management. Designed from the ground up for security, the CyberArk Privileged Access Security Solution provides the most comprehensive solution for all systems on-premises and in the cloud, from every endpoint, through the DevOps pipeline. This complete enterprise-ready Privileged Access Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.


CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION
ENDPOINT PRIVILEGE MANAGER
Least Privilege and Credential Theft Protection for Workstations
CORE PRIVILEGED ACCESS SECURITY
STANDARD
Risk-based Credential Security and Session Management to Protect Against Attacks
ALERO
Remote Vendor Access to CyberArk
ADVANCED
Least Privilege Server and Domain Controller Protection
APPLICATION ACCESS MANAGER
Secrets Management for Applications, Tools, Containers and DevOps
ON-PREMISES
HYBRID
CLOUD

Core Privileged Access Security (PAS)

Credential protection and management

The CyberArk solution centrally secures and controls access to privileged credentials based on privileged access security policies. Automated password and SSH key rotation reduces the time- consuming and error-prone task of manually tracking and updating privileged credentials to easily meet audit and compliance standards.

Isolate, control, monitor, and record privileged sessions

The CyberArk solution isolates and secures privileged user sessions, protects target systems from malware on endpoints, and enables privileged account access without exposing sensitive credentials. The solution supports broad connection methods with native access for cloud administrators and privileged business users, Windows clients (e.g. RDP, SSMS, etc.) and native command line SSH device connectivity. Monitoring and recording capabilities enable security teams to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions, and maintain a comprehensive, searchable audit trail of privileged user activity.

Analytics and alerting on malicious privileged access activity

Threat detection and analytics enable organizations to detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. The solution collects a targeted set of data from multiple sources and applies a complex combination of statistical and deterministic algorithms. This allows organizations to detect indications of compromise early in the attack lifecycle by identifying malicious privileged access activity.

The solution uses machine learning algorithms to examine typical patterns of individual privileged users, privileged accounts, and system activities to determine a baseline of “normal behavior.” It compares real-time activity to the baseline to identify unusual user behavior and system activity indicative of an attack including suspected credential theft, lateral movement, and privilege escalation.

Least privilege access control for *NIX and Windows

The CyberArk solution allows privileged users to run authorized administrative commands from their native Unix or Linux sessions while eliminating unneeded root privileges. This secure and enterprise ready, sudo-like solution provides unified and correlated logging of all super-user activity, linking it to a personal username while providing the freedom needed to perform various job functions.

Additionally, organizations have the ability to block and contain attacks on Windows servers to reduce the risk of information being stolen or encrypted and held for ransom. The solution protects against advanced threats that exploit privileged credentials by interlocking privilege management, application control, and targeted credential theft protection to stop and contain damaging attacks on critical servers.

Domain controller protection

Attackers can exploit vulnerabilities in the Kerberos authentication protocol to impersonate authorized users, gaining access to confidential data and critical IT resources. CyberArk offers an ultra-light weight Windows agent that performs network behavior analytics to detect in-progress Kerberos attacks. The solution provides comprehensive domain controller protection, safeguarding against impersonation and unauthorized access. It enforces least privilege and application control on the domain controllers and helps protect against a variety of common Kerberos attack techniques including Golden Ticket, Overpass-the-Hash, and Privilege Attribute Certificate (PAC) manipulation.

Alero

Remote vendor access to Core PAS

CyberArk® AleroTM is a SaaS-based solution that provides fast and secure access to the CyberArk Privileged Access Security Solution for remote vendors. Until now, remote vendors have typically relied on a combination of VPNs, agent-based corporate workstations and password or token-based MFA solutions to verify identity and access critical systems from outside of the network.

AleroTM combines Zero Trust access, biometric authentication and just-in-time provisioning to provide remote vendors and organizations with a secure, easy and modern way to of accessing critical internal assets that are managed by CyberArk; all without VPNs, agents, or passwords.

Application, Container and DevOps Secrets Management

Application Access Manager is designed to provide a strong security solution that enables organizations to control, manage, and audit all non-human privileged access for applications, across hybrid, containerized and multi-cloud environments.

Manage credentials for commercial off-the-shelf solutions with validated integrations

Secure the credentials that third-party tools and solutions such as security tools, RPA, automation tools, IT management, etc. need to complete their jobs.

Protect internally developed traditional applications by eliminating hard-coded passwords

Protect business-system data and simplify operations by managing credentials and eliminating hard-coded credentials from internally developed applications and scripts.

Secure cloud-native applications built using DevOps methodologies

Leverage a secrets management solution tailored specifically to meet the unique requirements of native cloud, containers, CI/CD tools chains and DevOps environments.

Endpoint Least Privilege, App Control, and Credential Theft Protection

Enforce privilege security on the endpoint

Endpoint Privilege Manager secures privileges on endpoints and contains attacks early in their lifecycle. It enables revocation of local administrator rights, while minimizing impact on user productivity by seamlessly elevating privileges for authorized applications or tasks. Application control combined with credential theft protection helps to prevent malware from gaining a foothold on the endpoint.

Swimlane

Cybersecurity Threats and Critical Infrastructure

The energy and utilities industry faces many of the same security challenges as other industries, but the stakes are often much greater. While financial gain and data theft are issues that span industries, energy and utilities companies are increasingly seeing attacks aimed at disruption or destruction. According to a recent study by Deloitte, the energy sector is one of the three most targeted industries, behind only critical manufacturing and communications.

As digital transformation results in a confluence of information technology (IT) systems and operational technology (OT) systems and their data, organizations incur more risk as the attack surface increases. With an ever-expanding threat landscape, more sophisticated nation-state threat actors, and the risk to human safety and economic activities, the need for better energy infrastructure risk management is greater than ever.

Reduce Risk Through Orchestration and Automation

Readiness to respond to cyber threats is a major challenge facing the utilities sector. Whether this is due to internal organizational failures, technical deficiencies or other reasons, the result is blind spots that leave your organization vulnerable.

Swimlane helps you respond to cyberattacks at machine speeds using intelligent automation and orchestration. The vendor-neutral security orchestration, automation and response (SOAR) platform integrates with your existing IT and OT security tools and manages the influx of alerts generated by these disparate solutions. With Swimlane, you can automate the incident response process easily and effectively.

Energy and utilities companies around the globe rely on Swimlane to understand their unique security orchestration and automation needs. Backed by the leading energy investment and innovation firm Energy Impact Partners (EIP), Swimlane is designed to help energy and utility companies:

- Minimize energy infrastructure and industrial control (SCADA/IT/OT) security risks.

- Optimize SOC/NOC operations security effectiveness, analyst resources, and costs.

- Integrate all IT and security operations tools for cross-ecosystem visibility.

- Automate complex workflows and incident response processes.

Address Top Security Challenges with Swimlane

Alert Triage - Security teams are overwhelmed by the number of alerts from their SIEM tools. Organizations are left vulnerable as analysts can only investigate a fraction of the true alerts that come in each day. Swimlane automates your alert triage processes, quickly identifying and eliminating false positives while escalating valid threats and performing a range of activities from initial analysis and validation to full remediation.

Phishing - Phishing is one of the most common types of cyberattacks and thus can produce a large number of alerts. Additionally, manually investigating and remediating all phishing attempts takes more time and manpower than exists in many organizations. Swimlane integrates with your existing security solutions and provides a centralized platform to automate the investigation and quarantine of suspecting phishing emails.

Insider Threat - Whether malicious or negligent, insider threats represents the majority of breaches. Researching and validating these threats requires extensive effort. Swimlane uses orchestration to integrate multiple tools for rapid insider threat detection and response. Security automation then triggers workflows, pushing threat incidents through the investigation and response process and only alerting teams when human intervention is required.

Compliance Tracking - Maintaining compliance is a large challenge for many organizations in the energy and utilities sector. Swimlane is ideal for helping track compliance. The platform integrates with tools across your security stack, enabling you to automate the collection of audit evidence and the building of audit packages.

Proving Security ROI for Energy Customers Worldwide

The unique architecture of Swimlane's SOAR platform—as a solution that aggregates data from multiple sources—makes it easy to track metrics across your entire technology stack:

- **Reduce mean time to resolution (MTTR)**.

Swimlane connects to your existing security tools, aggregating incident data and actions inside the platform. Faster access to relevant alert data and the ability to execute remediation actions at machine speeds reduces your MTTR. Every step in the process is tracked, so you can see how each part of your SecOps program contributes to resolving incidents effectively while also surfacing optimization opportunities.

- **Maximize staff efficiency**.

Swimlane decreases errors and increases staff efficiency by allowing your analysts to engage in investigation and enforcement actions directly within the platform. This removes the need to toggle between different tools to complete incident resolution steps. In-depth activity tracking and flexible dashboards provide detailed performance metrics that measure how both individual employees and teams respond to different types of incidents.

- **See the value of automation**.

Swimlane allows you to cut costs through automating time intensive incident resolution tasks. The platform calculates ROI for you by tracking the difference between manual incident response execution versus an automated response. This presents a quantifiable ROI, making it easy to justify the value of SOAR to your executive staff.

Contrast Security

Open-source software (OSS) affords developers many freedoms to build feature-rich applications on aggressive timelines. However, reliance on OSS adds layers of complexity across an organization's software supply chain. Some of the resulting risks are as follows:

RISK FROM INACTIVE LIBRARIES AND CLASSES

The 2021 State of Open-Source Security Report from Contrast Security found that 62% of libraries found in applications are inactive—that is, not used at all by the software in runtime.[1] And within active libraries, only 31% of library classes are invoked by the application. The derivative outtake is that only 9.4% of code in applications is active library and class code. As a result, developers are often overwhelmed by high volumes of erroneous security findings and do not have the means to prioritize their most utilized and at-risk libraries.

DEPENDENCY RISK

Dependencies introduced during continuous integration/continuous deployment (CI/CD) workflows create additional layers of unaccounted risk. For example, new attack vectors like dependency confusion, in which attackers trick an application into using the wrong library, can be a vehicle for malicious code.[2]

LEGAL AND COMPLIANCE RISK

Third-party software presents a variety of organizational risks that must be managed. For instance, some third-party libraries use risky licenses that could require an organization to open-source an entire application.[3] In response, application security teams need an automated means to baseline their OSS security posture while legal and compliance teams need to track licensing risk by building a software bill of materials (SBoM) that scales with their application portfolio.

These and other risks make safeguards like software composition analysis (SCA) a necessity to ensure visibility and governance into the code developers are shipping. Contrast OSS delivers automated SCA by embedding open-source security and compliance controls into applications throughout their life cycle. By leveraging instrumentation, **Contrast OSS** reduces friction between development, security, and operations teams by showcasing critical insights, such as runtime library usage, that can help drastically reduce manual triaging and prioritize remediation efforts for developers.

Contrast OSS provides real-time feedback to developers by integrating into their native CI/CD workflows. It provides context into how vulnerable libraries are introduced—no scanning required. This enables developers to take advantage of the many benefits of OSS while providing application security teams the necessary safeguards they need to be confident that the libraries used in their code are secure.

CAPABILITIES

- Prioritize remediation efforts by accurately identifying whether vulnerable open-source libraries are actually used by the application—all the way down to the specific class, file, or module.
- Flag dependency risk and contextualize how vulnerable dependencies are introduced and highlight potential supply chain attack vectors like dependency confusion.
- Check for vulnerable libraries before commit and institute security and license governance in native CI/CD workflows with the Contrast Command Line Interface (CLI).
- Automatically catalog third-party software assets—both commercial off-the-shelf (COTS) and OSS—and receive alerts when new vulnerabilities are detected in deployed libraries.
- Automatically create and maintain an organization-wide inventory of open-source components mapped to applications, servers, and environments to identify what runs where and what needs to be secured.
- Continuously evaluate OSS components in the application portfolio for both open-source vulnerabilities and open-source license risk.
- Set and automatically enforce custom OSS security and license policies within native CI/CD workflows and provide real-time feedback to security and development teams.

KEY BENEFITS

ENABLE FASTER REMEDIATION BY PRIORITIZING THE VULNERABILITIES THAT MATTER

Because Contrast OSS can identify active library components down to the class, module, or file, this extra layer of insight allows security and development teams to prioritize remediation efforts by identifying the most heavily used libraries. This enables developers to avoid hours of remediating vulnerabilities in inactive code and verifying results.

EMBED SECURITY WHILE ELIMINATING BOTTLENECKS WITH END-TO-END AUTOMATION

Contrast OSS inventories libraries and vulnerabilities within native CI/CD workflows with no manual scanning or false positives that distract developers from shipping code on time. Instead, Contrast OSS embeds into existing testing and build tools to provide real-time insights into third-party software assets. An embedded approach to SCA ensures dramatically fewer false positives—and results in less overwhelmed development and security teams.

CONTINUOUS VISIBILITY INTO YOUR SOFTWARE SUPPLY CHAIN

Contrast OSS monitors the entire application portfolio, including third-party and custom code, automatically applying new vulnerability intelligence for libraries already deployed. This eliminates the need for disruptive scans and re-scans of code repositories. Beyond top-level library CVEs, Contrast OSS benchmarks dependency risk by highlighting vulnerable dependencies introduced during native-build processes and flags dependency confusion risk. For early security testing, the Contrast CLI enables developers to rapidly test to their code to check for vulnerable libraries and dependency risk before committing.

SCALABLE GOVERNANCE WITHOUT IMPEDING INNOVATION

Contrast OSS automatically discovers open-source components in applications, provides critical versioning and usage information, and triggers alerts when risks and policy violations are detected at any stage of the software development life cycle (SDLC). Contrast OSS enables application security teams to institute custom policy standards across their entire application portfolio and to manage the use of open-source libraries and licenses within the software development workflow.

SINGLE DEPLOYMENT TO RAPIDLY RESPOND TO NEW THREATS

The Contrast Application Security Platform leverages a single deployment and assessment process to identify vulnerabilities in open-source and custom code. There is no need to implement multiple tools, orchestrate between different analysis engines, or run complex correlations. Beyond automatically detecting risk, Contrast provides runtime protection so that attacks on vulnerable open-source code are automatically monitored and blocked to prevent exploitation in production.

Silverfort

Silverfort's agentless and holistic authentication platform monitors user access across all systems and environments and enforces adaptive AI-driven MFA, enabling organizations to mitigate threats in real-time and achieve compliance with various regulations and industry standards including PCI DSS, GDPR, HIPAA, SOX, NIST and more.

Compromised and weak credentials are currently leveraged in four out of five data breaches. Mainstream MFA solutions can no longer handle the complexity and dynamic nature of today's networks. In many companies, the use of homegrown and proprietary systems that are not supported by current MFA solutions creates significant security and compliance challenges.

Agentless MFA for Any Sensitive Asset, including "Unprotectable" Systems

Silverfort's agentless MFA technology can seamlessly enforce MFA on access to any sensitive system or device, across all corporate networks and cloud environments. It enables MFA for sensitive resources without deploying software agents or inline proxies and without integrations with individual systems - an impossible task in large and dynamic networks. This enables Silverfort to extend protection to systems that were considered "unprotectable" until today, including: file shares, databases, IT infrastructure (e.g. hypervisors, DCs and network equipment), critical financial servers (e.g. SWIFT servers and Cardholder Data Environment), IoT devices, homegrown systems and more.

AI-Driven Adaptive Authentication Across All Systems and Environments

Silverfort's Authentication Platform analyzes user behavior across all devices, resources and environments, on-premises and in the cloud, to enable continuous risk and trust analysis and adaptive authentication policies with unparalleled coverage and accuracy. Silverfort's advanced AI-based risk engine detects identity-related threats, including account takeover, lateral movement, ransomware and brute-force attacks, enabling real-time threat mitigation without disrupting the user experience.

Holistic Visibility, Continuous Risk and Trust Assessment

Silverfort's agentless architecture and holistic approach provide a big advantage as they enable unparalleled visibility into all user and machine activities across all systems and environments, continuously assessing risk and trust for every access request with unmatched accuracy. Silverfort provides a consolidated audit trail of all user activity and assists organizations in achieving least privileges as part of periodic entitlement reviews, by clearly showing which entitlements are being used and which are redundant. Silverfort automatically maps vulnerabilities and risks, including use of weak authentication protocols, stale accounts and devices, old or expired passwords, shared accounts and more.

Netskope

Netskope provides a globally available, cloud-based security platform for securing remote workers' access to web, cloud, and private applications in the data center or public cloud. Netskope has the unique ability to decode cloud application and website traffic to understand remote workers' activities, inspect data movement, and detect threats hidden in SSL/TLS traffic. Netskope improves users' remote access experience by seamlessly and securely connecting them to their private applications using Zero Trust Network Access. Netskope requires a single, lightweight client installed on a device to manage web and cloud traffic, and tunnel private application traffic.

DATA PROTECTION

Data is increasingly at risk as it moves outside the enterprise perimeter and beyond the visibility and control of traditional security controls. Consistent data protection policies are now required across IT-managed services such as Salesforce, Microsoft Office 365 and AWS, plus thousands of unmanaged cloud services, and websites which allow the uploading of data. Cloud services make it all too easy for employees to put sensitive information in the wrong place or share it with the wrong people. Malicious insiders or disgruntled employees are more likely to attempt exfiltration of company sensitive data when outside the office environment, making robust protection of data all the more critical for remote workers.

Netskope DLP protects sensitive data from being uploaded by remote workers to cloud applications (SaaS), public cloud environments (IaaS), or any website. Netskope is also able to identify and prevent the movement of sensitive data that may indicate the actions of a malicious insider attempting to steal data. Netskope has the most advanced cloud-based DLP capabilities, designed for ease of implementation, low false positive rates, and detailed incident investigation.

THREAT PROTECTION

When remote workers connect directly to the internet and bypass traditional on-premises security controls they expose the organization to greater risk. Remote working ultimately increases an organization's attack surface—the size and extent of the network and devices open to compromise by today's elusive threats.

Netskope decodes TLS-encrypted cloud services and websites, to identify and mitigate against the current wave of cloud-enabled threats that are facing organizations. Cybercriminals are utilizing cloud services as the reliable and scalable infrastructure for implementing their cyber kill chain in the cloud. Consider phishing pages hosted in cloud storage services such as OneNote, Command and Control networks using collaboration apps such as Slack or GitHub, or malware payloads hosted in AWS S3 buckets or Microsoft Azure.

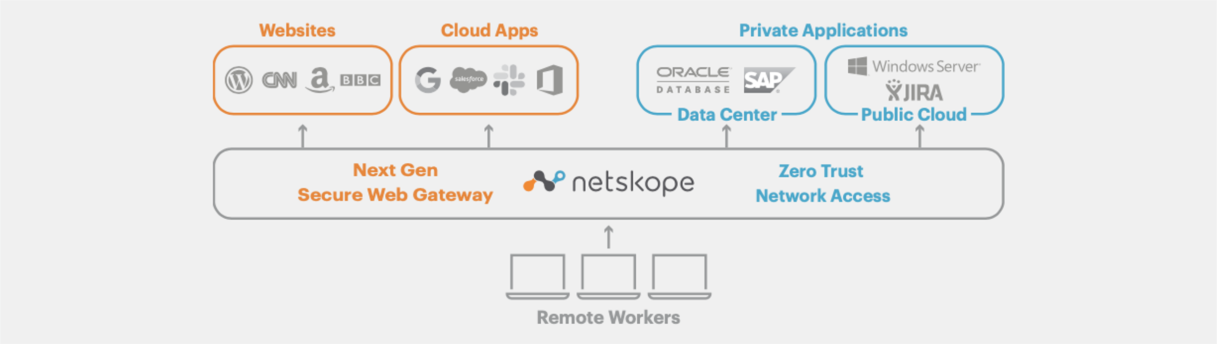
Backed by Netskope Threat Research Labs, a dedicated team focused on the discovery and analysis of new cloud threats, Netskope uses multi-layer defenses including antivirus, pre-execution script analysis and heuristics, bare-metal sandboxing, machine-learning anomaly detection, plus dozens of 3rd party threat intelligence feeds.

ZERO TRUST NETWORK ACCESS

The Netskope ZTNA solution allows an organization
to begin retiring legacy VPN hardware and make a move towards a more secure, cloud-first, remote access architecture. End the high capital investment, refresh cycles, and ongoing management costs of VPN appliances—and adopt ZTNA for your remote workers.

Netskope provides an alternative to backhauling (or hairpinning) remote users through the corporate network to access applications in public cloud environments, an inefficient legacy architecture that typically impacts the user experience. Netskope also removes the need to expose applications publically from public cloud environments, therefore, lowering the risk of compromise through unauthorized access.

Netskope directly and seamlessly connects remote workers to private applications running in public cloud environments or private data centers. Connectivity between remote workers and applications is secured by an end-to-end TLS encrypted tunnel and optimally routed through NewEdge—Netskope's high-performance, scalable global network infrastructure. Integration with strong authentication, and inspection of device security posture, ensures that only authorized users with secure devices can gain access to applications.



VISIBILITY

Netskope provides detailed and valuable insight into all the cloud applications and websites an organization's remote workers are visiting. Furthermore, Netskope's Cloud XD^{TM} technology is able to decode cloud and web traffic to understand the activities performed by users and distinguish between corporate and personal instances of cloud apps. With Netskope, you can obtain granular visibility into cloud app activity and the spread of sensitive data within and outside your organization. However, in order to provide a more robust security solution, security teams need to enact granular security controls across both managed and unmanaged cloud apps use. The greatest blindspot for security teams is the unofficial use of unmanaged apps that often proliferate across organizations.

GRANULAR CONTROL

Netskope's Cloud XD is the "engine" of the Netskope platform, Cloud XD makes sense of cloud services, apps, and web traffic to feed context and content into data and threat protection policies. Cloud XD understands the language of the cloud (APIs, JSON, etc.) to provide granular visibility into the users, devices, applications, instances, risk ratings, URL categories, and activities in cloud and web environments. It then takes smart actions, such as allow, block, delete, encrypt, quarantine and more, based on your enforcement policies.

Granular visibility and control of remote workers' activities when they use cloud applications or visit websites plays an important role in reducing the risk of data loss and protecting against threats. Netskope's NG SWG policies can differentiate between personal and corporate instances of cloud applications. Examples of how this instance-awareness can be used include; preventing uploads of sensitive data to personal instances of cloud storage, or preventing access to rogue instances of public cloud environments used to host phishing pages or malware.

Okta

From the smallest town agencies to the largest federal departments, new software solutions typically provide convenience and brand-new challenges in equal measure. Finding a mix of solutions that satisfy employee needs, meet public demands, and work well together is a challenge IT stakeholders run up against on a daily basis.

This is particularly important because government agencies are adopting new IT systems and upgrading current ones at a faster rate than ever before, which has created an environment where modern solutions—especially cloud-based ones—need to be compatible with legacy systems that have often been in place for years. Moreover, with robust security and data protection being absolutely essential in the public sector, IT teams are left trying to manage different users across different systems and applications in a way that will not put the organization at risk.

Taken together, these challenges underscore the need for a new solution in the public sector: one that weaves all systems into a cohesive whole, regardless of hosting location, creator, overall function, or the information it touches and transmits. It also has to meet this goal without adversely affecting security

or adding bloated cost to an agency's existing infrastructural opex/capex. Moreover, a worthwhile solution will centralize control, grant end-users useful self-service options, and automate time-consuming authentication tasks such as password reset requests and provisioning.

Finding a solution that meets this slate of identity and access management challenges may seem like a moonshot—but Okta can help your agency get there. With a collection of FedRAMP- and CAC/PIV-enabled tools that integrate with homegrown, on-premises solutions as well as the cloud-based SaaS

tools government agencies rely on most (such as Box, Office 365, Google, and Salesforce), Okta brings centralized identity control and integrated security solutions to any disparate collection of cloud-based and on-premises systems.

As a result, IT stakeholders can minimize access- and identity-based challenges as they consider their transition from legacy systems to the cloud, with tools that help them meet their goals along every step of the journey. Whether your agency is almost entirely making use of on-premises and homegrown solutions, or completing a planned cloud migration, Okta can assist.

Single Sign-On: Simplifying access, one user at a time

Challenge: Government perimeters tend to be broad and diverse. One solution may be on-premises and custom, while the next may be cloud-based and provided by a vendor. Because of this, finding a single sign-on (SSO) offering robust and versatile enough to manage every application in a government roster has long seemed like a white whale.

Solution: Not so with Okta's Single Sign-On. End-users can utilize the same credentials across an agency's local and cloud-based applications with SSO, regardless of source. Users have a significantly easier time managing their identities, while IT can condense a pile of system-specific password reset requests into a single-point, self-service function. Throw in over 5,500 pre-built integrations to the most popular cloud solutions (Office 365, AWS, Slack, Box) and the ability to support legacy systems, and your agency has the perfect SSO solution. Okta offers the option to provide PIV authentication to SSO-based applications using PIV and CAC smartcards.

Adaptive Multi-Factor Authentication: Flexible, context-sensitive security

Challenge: Over 80% of breaches involve weak or stolen credentials. It's a sobering fact, and one that becomes all the more serious when one realizes how frequently government institutions are targeted for digital theft and other cyberattacks. The same broad, diverse perimeters that make government systems so challenging to manage make them extremely attractive to attackers; this is especially true when considering the amount of valuable, sensitive data these solutions store and transmit.

Solution: Okta's Adaptive Multi-Factor Authentication (MFA) has been designed to add a number of agency-selected factors to the login equation. For instance, an agency could choose to verify with the Okta Verify app or with a One-Time Password (OTP) pushed to a known mobile device. Okta can even integrate with Personal Identity Verification and Common Access Cards (PIV / CAC), and is Federal Information Processing Standards (FIPS) 140-2 certified. To reduce login friction while improving security, Adaptive MFA also allows for contextual access management, so when a user logs in from a new location, device, or network, additional authentication factors can be asked for. With the FIPS certification Okta meets NIST 800-63v3 compliance requirements for strong authentication for AAL levels.

Universal Directory: Easy to use multi-source integration

Challenge: Managing users is at the core of any identity and access management activity, but it's also a task that can quickly eat into valuable time. Too often, chasing users across a collection of systems becomes an ongoing chore for IT personnel, who may have to help with everything from password resets to provisioning issues. By the same token, a single oversight—a near certainty when dealing with so many fine details—can carry serious security implications, granting former users access to systems they should no longer be able to access.

Solution: Okta's Universal Directory aims to meet the challenge of running a single thread through multiple systems. Users, groups, and devices from across systems are combined to a single point of truth, vastly simplifying life for IT teams and providing full lifecycle support for the accounts under its banner. With the ability to seamlessly integrate with AD, LDAP, and other directory stores, Universal Directory makes user management easier than ever: Changes made on one end (an HR system, for instance) are automatically reflected on the other end.

Okta Integration Network: Deep, pre-built integrations for your critical apps

Challenge: Box. AWS. Salesforce. Office 365. Government agencies at all levels rely on apps like these, and they need to work together seamlessly. With employees needing reliable access to the systems they work on and customers having heavier user-experience expectations than ever before, a lack of interoperability is simply unacceptable. So too is sustained downtime as systems are implemented and integrated.

Solution: The Okta Integration Network makes this challenge a thing of the past. Over 5,500 pre-built integrations help government agencies avoid vendor lock-in and keep their systems fluid, no matter what needs the future may throw at them. From SSO to user profiles and security analytics, the Okta Integration Network is designed to help agencies make better use of current software solutions and free them to choose whatever applications will make most sense in the future—a far cry from the siloed systems of old.

Lifecycle Management: Automated management and better security

Challenge: In the past, huge government userbases meant huge problems with provisioning and lifecycle management, a fact that holds for both internal and external accounts. Determining precisely who gets access to which systems can become a major chore and time-sink, and that's before considering the severe security risks that can occur when accounts aren't properly—and promptly—deprovisioned.

Solution: With its automated take on provisioning and management, Lifecycle Management offers huge savings in time and money. Provisioning and deprovisioning naturally become easier under an automated system, as do access audits and hunts for rogue accounts; the tool can also be highly beneficial in reducing instances of shadow IT, another phenomenon with real potential to introduce security problems. Okta Lifecycle Management can even be extended to provision your custom apps using SCIM.

SpyCloud

SpyCloud is an emerging technology company with headquarters in Austin TX. SpyCloud is doing business with the US Federal Government with customers in both Civilian and DoD Agencies.

Ransomware has been growing steadily since 2016 – and 2021 is no different including the high- profile attack on Colonial Pipeline. More than doubling its frequency from 2019, **ransomware as an action was present in 10% of breaches** last year. Bad actors look for easy access and prefer the use of stolen credentials or brute force as a tactic; in Verizon's annual 'Data Breach Investigation Report for 2020', 60% of the ransomware cases Verizon observed involved direct install or installation through desktop sharing applications.

With close to 4,000 companies in the nation's electric power network and countless suppliers, a fast and continuous dashboard of exposed credentials and 'credential stealing' malware infected user machine records for the electric companies and their suppliers' employee's, c-suite and visitors is a needed and obvious first line of defense against the use of the stolen credentials in brute force, credential stuffing, password phishing and social engineering attacks.

SpyCloud is the largest source of collected and curated breach data assets: 120 billion breach data assets, 29 million email addresses, 26 billion plaintext passwords and the only source for 200+ million 'credential stealing' malware infected user machines records from 14 families of malware.

What makes SpyCloud different from other breach data sources:

- 90% of data is collected using our HUMINT tradecraft from covert and private sources, days if not hours from when a breach happens. Our competitors are limited to using dark web scanning that cannot access these sources and the result is SpyCloud on average obtains breach data 180+ days prior to publication on the dark web.
- 90% of found passwords are cracked into plaintext. SpyCloud has built our own password passing platform to crack passwords at scale. No other source has this volume of crack passwords for exact and fuzzy matching to access the true risk of exposed credentials
- 50+ billion assets are from foreign domains including Chinese, Russian and Iranian domains. SpyCloud Investigations enable attribution to help de-anonymize the threat actors, their organizations and infrastructure.

- 250+ million ‘credential stealing’ malware infected user machines records collected by our HUMINT tradecraft directly from criminal sources. Approximately 10 million are monthly. The high risk, high fidelity, and data rich records include the infected machine id, IP address, infection timestamp, infected install path, and visited URLs. SpyCloud is the only known source for records from 14 families of malware.

SpyCloud’s go-to market solutions help proactively protect employees, consumers, and employees of suppliers of Federal Agencies from cyber threats using stolen credentials and malware infected user machines and to de-anonymize the threat actors and organizations from their historical exposed digital footprint. SpyCloud solutions include:

- **SpyCloud Employee Protection (EAP).** Monitoring, dashboard reporting and automated alerts of all exposed credentials and infected user machines records for multiple company domains, IP addresses, or VIP email addresses, and all infected user machine records for visitors to domains or IP addresses.
- **SpyCloud Active Directory Guardian (ADG).** Automates the matching, alerts and remediation of exposed credentials and infected user machine records to your active employee. ADG initiates a change to the password used and enforces password strengthening in compliance with NIST 800-63B.
- **SpyCloud Third Party Insights (3PI).** Monitoring, dashboard risk ranking and reporting, and alerts of exposed ‘plaintext’ credentials and infected user machines records for employee’s and c-c-suite for third party suppliers or sub organizations such as a DOE Laboratory. Actionable data for remediation of the risk can be shared with the third party with tracking of the remediation in the 3PI dashboard.

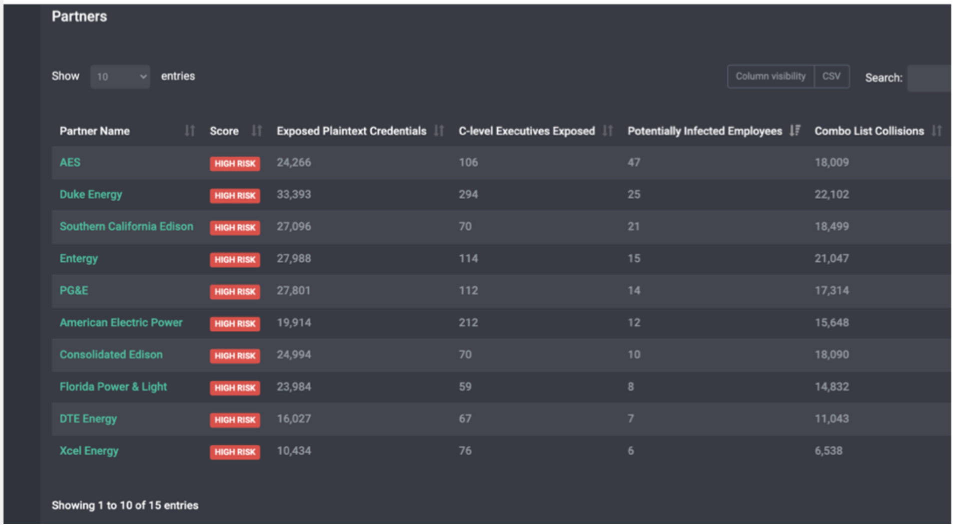
Ensuring the Continued Security of the United States Critical Electric Infrastructure Questions:

What Technical Assistance would States, Indian Tribes or units of local government need to enhance their security efforts relative to the electric system?

• The lowest and easiest path for criminals is using exposed credentials to launch attacks. With the explosion of work from home, personal devices and remote access has only complicated the attack surface. Early detection of exposed credentials, knowing the plaintext passwords and knowledge of any ‘credential stealing' malware infected user records is an easy and highly effective way for governments to close the most used and easiest path for criminals.

SpyCloud Employee Protection (EAP)/Active Directory Guardian(ADG):
Automate the monitoring of Government active directories to detect exposed 'exact match or closely matching' credentials and any infected user machine. Remove the exposures and strengthen new passwords in compliance with NIST 800-63b guidelines. SpyCloud is the largest source of breach data, earliest collection, largest source of cracked passwords and the only source of infected user machine records. SpyCloud has had States inquire if DHS CISA could make this service available to Government organizations to help the States, Indian Tribes and local governments to detect and remediate the most used source of attacks, exposed credentials. Cloud hosted by SpyCloud in AWS, EAP requires no implementation other than entering the domains, IP addresses and VIP emails to monitor and report. ADG does require loading of a module onto the active directory server and adds the automation to initiate a change to the password.

Following is an example of live example of 10 of the top 15 power suppliers and their exposures. As a proactive cyber threat reduction, DOE could offer **SpyCloud's 'Malware Infected User Machine Records' Employee and Consumer Portal** to a power grid company. In this scenario, the company would have instant alerts and access to all data on infected user machines for either an employee or for anyone visiting their domains. This includes machine id, IP address, visited URLs, cookies and screen shots at time of infection.



Partner Name	Score	Exposed Plaintext Credentials	C-level Executives Exposed	Potentially Infected Employees	Combo List Collisions
AES	HIGH RISK	24,266	106	47	18,009
Duke Energy	HIGH RISK	33,393	294	25	22,102
Southern California Edison	HIGH RISK	27,096	70	21	18,499
Entergy	HIGH RISK	27,988	114	15	21,047
PG&E	HIGH RISK	27,801	112	14	17,314
American Electric Power	HIGH RISK	19,914	212	12	15,648
Consolidated Edison	HIGH RISK	24,994	70	10	18,090
Florida Power & Light	HIGH RISK	23,984	59	8	14,832
DTE Energy	HIGH RISK	16,027	67	7	11,043
Xcel Energy	HIGH RISK	10,434	76	6	6,538

Showing 1 to 10 of 15 entries

Conclusion and Invitation to Learn More

The Merlin team would enjoy briefing the relevant DOE teams, aligning our technology stack with your efforts to secure the nation's electrical grid and fortify the supply chain. While various components of DOE already leverage Merlin technologies, we are committed to understanding your specific office's requirements and aligning our technologies to solving your most pressing use cases. To setup time to learn more, please contact DOE Account Manager Tom Steiner at 404-444-4856, and also at tsteiner@merlincyber.com.

About Merlin Cyber

Merlin is the premier cybersecurity platform with a unique business model that leverages technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help government agencies minimize risk and simplify IT operations. Merlin represents prominent cybersecurity brands and invests in visionary, emerging technologies, bringing everything together into its lab where cybersecurity engineers integrate, test, and deliver innovative security solutions. This approach helps the government save time, money, and other resources while more effectively securing its systems, data, and users no matter how requirements evolve.