BeyondTrust

EDUCATION
FEDERAL
STATE & LOCAL
FOR PUBLIC SECTOR

Reshaping Adversary Behaviors

Kevin E. Greene
Chief Cybersecurity Technologist, Public Sector

Reshaping Adversary Behaviors

Abstract: Reactive cyber defense is no longer enough. The path forward is a **proactive posture** grounded in **deterrence by denial** — the core of ONCD's National Cybersecurity Strategy — designed **to impose real cost**, **risk**, and **uncertainty** on threat actors' operations. Today, identity has become the **primary battleground in cyberattacks**, with privilege serving as the fuel that powers adversary progression. Embracing a **Privilege Disruption** philosophy and mindset is essential to denying threat actors **meaningful advancement and strategic impact**. This talk dives deeper into practical strategies for building cyber deterrence and formalizing Privilege Disruption — ensuring initial access never escalates into persistent control.


97% of all NHIs are granted excessive privileges that are unnecessary for their functional requirements
Non-human identities now outnumber human identities by a ratio of 144 to 1 in the average enterprise environment
IDENTITY IS THE NEW BATTLEGROUND
FOR CYBERATTACKS
Non-Human Identities
66% of organizations have experienced a cyberattack resulting from compromised NHIs (API keys, service accounts, secrets)
Identity is the new battleground for cyberattacks, with fewer attackers "breaking in" via hacking or other offensive tactics.
AI Identities
97% of organizations lack proper access controls for AI models
Gartner predicts that by 2028, 25% of all enterprise security breaches will be traced back to AI agent abuse or manipulation
42% of machine identities (including AI agents) currently hold sensitive or administrative-level access
Human Identities
32% of human-centric breaches involve sophisticated "MFA-bypass" techniques like session hijacking or MiTM attacks
Breaches involving stolen credentials take the longest to identify, averaging 292 days to detect and contain
1% of all permission granted across AWS, GCP, Azure are actually being used
OWN THE STAGE
CONFIDENCE • PRESENCE • LEADERSHIP

Attacks on US Infrastructure

Midnight Blizzard
(Microsoft Hack) 2024

STORM-0501
(Hybrid Cloud Ransomware) 2025

Salt Typhoon
(Telcom Industry) 2024

Volt Typhoon
(IT/OT Infrastructure) 2024

attacks across
multiple privilege
control planes

Ubiquitous Control

Plane Jumping

Attacks Across Sectors

CBS Evening News

Cyberattack that crippled Nevada's systems reveals vulnerability of smaller government agencies to hackers

Twin Cities News

Gov. Walz activates Minnesota National Guard to aid St. Paul after cyberattack

PowerSchool customers hit by downstream extortion threats

The large education tech vendor was hit by a cyberattack and paid a ransom in December. Now, a threat actor is attempting to extort the company's customers with stolen data.

CYBERSECURITY

Hoboken, N.J., Wraps Investigation Into Cyber Attack

Officials are offering free credit monitoring and identity protection to those affected. The incident in late November shuttered City Hall and impacted municipal court and city services.

ADMINISTRATION

Princeton Database Breached in Targeted Phishing Incident

The database kept by the University's Advancement department contains information about alumni, donors, and other Princetonians

Politics

DHS and HHS among federal agencies hacked in Microsoft SharePoint breach

CYBERSECURITY

The Congressional Budget Office was hacked. It says it has implemented new security measures

What's left to worry (and not worry) about in the F5 breach aftermath

Researchers say the nation-state attacker could cause more serious problems with the BIG-IP source code it nabbed during the attack on F5's systems.

Hackers Spied on 100 US Bank Regulators' Emails for Over a Year

Sean Cairncross – ONCD

> With artificial intelligence amplifying the threat landscape and ransomware remaining a persistent menace, the Administration's message was clear: **cybersecurity** is no longer a **reactive exercise** but a ***proactive campaign to shape adversary behavior*** through coordinated federal action and strengthened industry partnership.

Government Cyber Priorities

ONCD Cyber Strategy = Cyber Deterrence

1. **Shaping Adversary Behavior**
2. Promoting Common Sense Regulation
3. **Modernizing and Securing Government Networks**
4. **Securing Critical Infrastructure**
5. Sustaining Superiority in Critical and Emerging Technologies
6. Build Cyber Talent and Capacity

Impose Meaningful Cost

Increase Risk and Uncertainty

Make targets less attractive

Security Magazine Bylined Article

SECURITY

Privilege Disruption: The Key Choke Point for Cyber Deterrence

By Kevin Greene


ADMIN
ROOT
ROOT
ROOT
PRIVILEGE
DISRUPTION
OWN
THE
STAGE
CONFIDENCE
PRESENCE
LEADERSHIP

Alignment with ONCD Cyber Strategy

PRIVILEGE DISRUPTION

Privilege disruption is the deliberate denial and containment of privilege access, escalation, and misuse by cyber defenders, ensuring that initial access does not become control and persistence for threat actors.

- **Make threat actors' operations less effective and attractive.**
- **Robust privilege management and least privilege enforcement.**
- **Prevent progression and strategic impact.**

Deterrence by Denial

Driving Toward a Prevention First-Approach

Leave No Privilege Behind + **Privilege Disruption** = **Effective Cyber Deterrence**

THE FOUNDATION

Leave No Privilege Behind

Ensures every privilege — human, machine, AI — is discovered, governed, minimized, and continuously validated. Establishes the conditions for disruption.

Comprehensive Visibility and Identity Intelligence

THE CHOKEPOINT

Privilege Disruption

Active, deliberate denial and containment of privileged access, escalation, and misuse. Denies threat actors the ability to convert initial access into control.

Control and Manage Privilege

THE OUTCOME

Cyber Deterrence

Imposes cost, risk, and uncertainty on adversary operations. Forces threat actors to change behavior when repeated attempts fail to convert access into control.

Reshape Adversary Behavior

Privilege-Centric Identity Security

BT Alignment With Privilege Disruption

DENY ESCALATION	BUILD EPHEMERAL	REDUCE PLANES	RESTRICT MOVEMENT	LEAVE NO PRIV BEHIND
EPM	**Entitle**	**Insights**	**PRA**	**Password Safe**
Endpoint Privilege Management	Cloud Entitlement Management (CIEM)	Identity Security Insights (ITDR)	Privileged Remote Access	Credential Vaulting & Rotation
DETERRENCE Denies access from becoming control	**DETERRENCE** Denies access from becoming reach and scale	**DETERRENCE** Accelerates early disruption and exposure	**DETERRENCE** Denies stealthy privileged movement	**DETERRENCE** Denies persistence through credentials
DISRUPTION Disrupts escalation at the moment it would become control	**DISRUPTION** Disrupts excessive and implicit identity privilege	**DISRUPTION** Enables early identification of exposed privilege paths	**DISRUPTION** Disrupts stealthy use and lateral movement	**DISRUPTION** Disrupts privilege persistence through credentials
CONTROL PLANE Endpoint / OS Plane	**CONTROL PLANE** Cloud + Identity Plane	**CONTROL PLANE** Cross-Plane Visibility	**CONTROL PLANE** OT /Edge / Network Fabric	**CONTROL PLANE** All Planes (Credentials)

Unified privilege disruption across all control planes → Continuous Policy Enforcement → Cyber Deterrence Engine

Driving Toward a Prevention First-Approach

Mission Assurance, Resiliency, Trust

Cost | Uncertainty | Denial | Risk

Deny Escalation, Movement, Prepositioning, Persistence

Least Privilege, Assume Compromise, Explicit Trust, Continuous Validation

Security controls and capabilities

CYBER DEFENSE

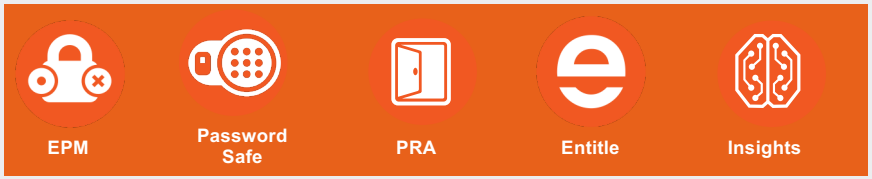
Strategic Outcomes

CYBER DETERRENCE

LEAVE NO PRIVILEGE BEHIND

PRIVILEGE DISRUPTION

Least Privilege | Explicit Trust | Assume Compromise



Ultimate Goal

Ensure Mission Capabilities

Shape Behaviors

Doctrine and Philosophy

Operationalizes Deterrence

Zero Trust Fabric

Continuous "Zero Trust" Policy Enforcement

Cyber Deterrence Engine

Identity alone has no risk…

Privilege is what gives ”Identity” risk

Disrupt and control privilege — and the chain collapses before lateral movement, before prepositioning, before persistence.

ACCESS ≠ CONTROL → PRIVILEGE DISRUPTION
is the gap between them