

IGEL On IGEL: Cybersecurity Best Practices

The Ultimate EUC Event

Agenda

- IGEL’s Security Latest News
- Latest research on effective Cybersecurity Policies
- IGEL’s Preventative Security Model
- Zero Trust?
- Resources for security configuration and settings for IGEL’s products.



IGEL Security News

- IGEL is now ISO 27001:2022 certified
  - SOC 2 Type II is next
  - For our Federal Customers we are working on FedRAMP, FIPS, DISA/STIG/CIS.
- UMS 12.4+ with full remote security logging
- OS 12.4+ User Login History for login types AD/Kerberos, SSO (ID Provider) and Local User.
- 50+ Apps added to the App Portal for OS12, several security apps from our partners (Imprivata, DeviceTrust, 90meter, and more)
- Reverse Proxies compatibility + documentation added to KB (NGNIX, F5, Azure Application Gateway, Netscaler)




ISO
NIS2
DIRECTIVE
NIST
National Institute of
Standards and Technology
GDPR
PCI DSS
COMPLIANT
THE WHITE HOUSE
WASHINGTON
HIPAA
COMPLIANT

Research Article

Evidence-based cybersecurity policy? A meta-review of security control effectiveness

Daniel W. Woods & Sezaneh Seymour

Received 04 Aug 2023, Accepted 19 Jan 2024, Published online: 07 Apr 2024

TLDR:

- **Attack surface management** and **patch cadence** were consistently the first and second most effective interventions.
- Multi-factor authentication was effective in protecting individual accounts, although inconsistent MFA-implementation undermines efficacy when rolled out across an organization.
- **…effectiveness is driven by how a control is implemented more than by a binary yes-no regarding whether it is implemented.**

Compliance != Security

Attack Surface Management

How to reduce your attack surface?

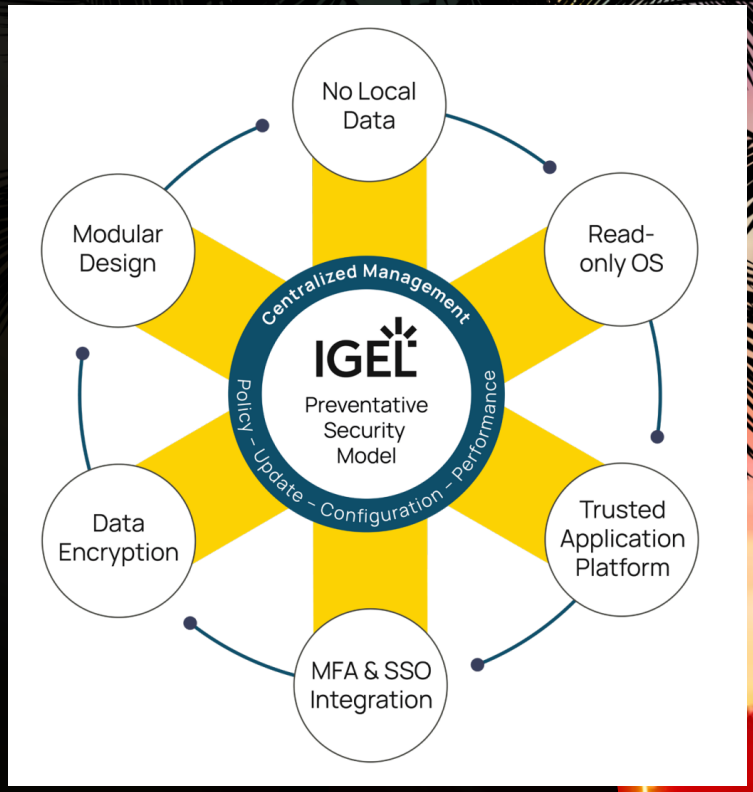
- Systems Hardening
- Closing ports
- Complexity management
- Hiding version information

The most secure assets in your systems are the ones you don’t have in the first place; the next best are your assets that are inventoried and monitored.



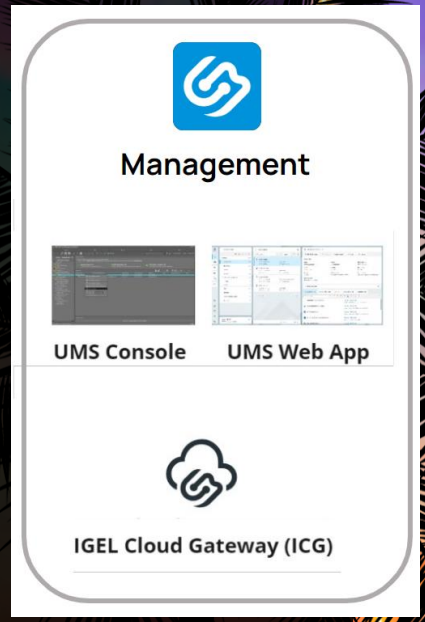
IGEL Reduces your Attack Surface

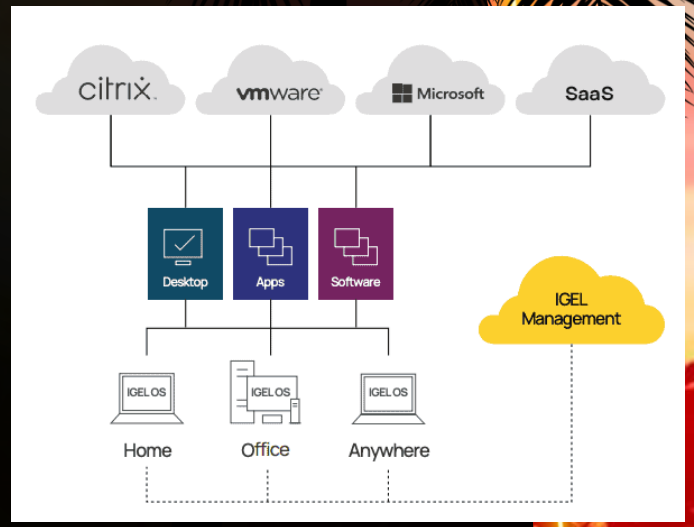
- Use the “Securing IGEL OS Endpoints” guide from our KB
- Encrypt your IGEL OS (TPM 2.0 support, TPM + PCR on select HW models)
- If your environment is based on AVD/Windows 365 you can lock down access so ONLY your managed IGEL OS endpoints can access your resources (conditional access). See new blog post by Fredrik Brattstig in igel.com – “Elevate AVD and Windows 365 access with insider tips for IGEL OS”



Tips on Hardening UMS

- Use external database with authentication.
- Enable the new security logging and collect/send to your SIEM
- Enable SSL Only (Default since UMS12)
- Use strong password, or ideally local AD/LDAP (SSO is being worked on)
- Limit the permissions of the administrators to minimum needed for their job.
- Limit access to host machine & java-console by using the UMS Web App (every release we add more functionality).
- Harden the host machine (CIS Benchmark)





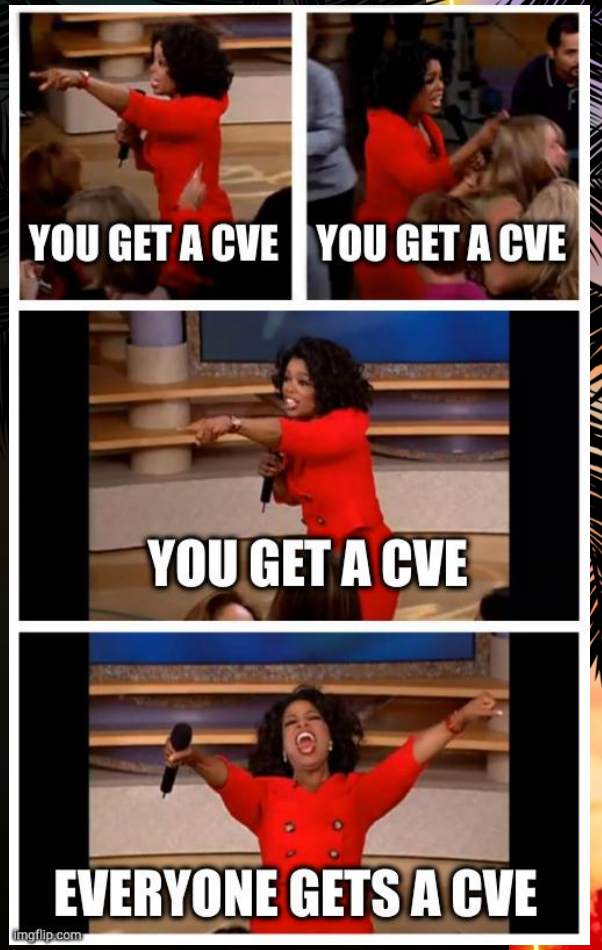
Patch Management

How to prioritize patching if you can't do it all?

1. Is the vulnerable service publicly exposed to the internet?
2. Does it run in production, as opposed to a development or test environment?
3. Is there exploit code available online, or instructions on how to exploit the vulnerability?

   About 5% of vulnerabilities are ever exploited in the wild. Monitor CISA's Known Exploited Vulnerabilities Catalog

"Attackers will only do what is necessary to accomplish their goal. Make them hack you with 0-days." Maddie Stone, ex-Project Zero



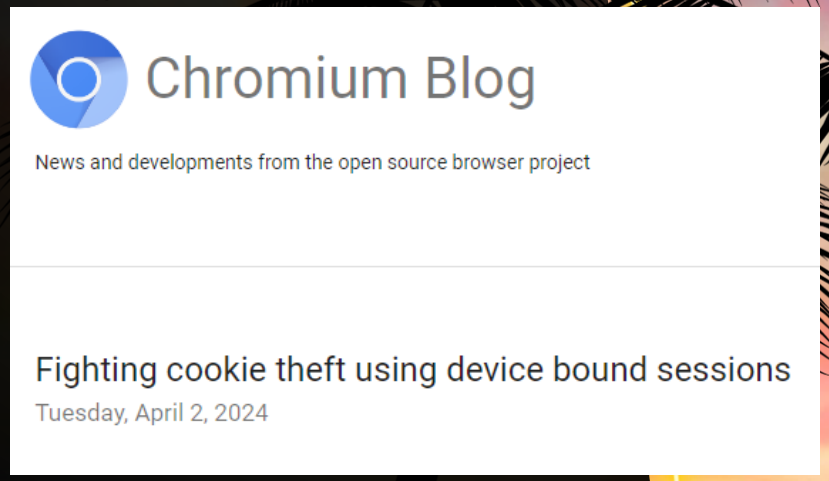
IGEL Security Notices (ISNs)

- Subscribe to receive email with information about major (critical/high) vulnerabilities that have been found in IGEL software products, and how to fix or mitigate them.
- More details in our Knowledge Base.



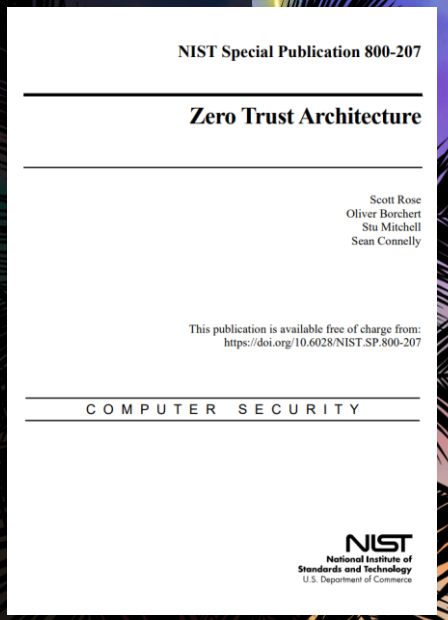
Multi-factor Authentication (MFA)

- Great at protecting accounts from phishing and password leaks/spraying.
- Key part of everybody's overall security strategy, but not enough. Should be mandatory for high-risk accounts, ideally rolled out in the entire organization.
- Not so great when token gets leaked



Zero Trust?

- Term is a little confusing, and it does not help that vendors bend the term to fit their products.
- This is NOT a product that you can buy and say you are “Zero Trust Certified”, not a “yes-no” check.
- It is an overall strategy & framework focused on improving organizations entire cybersecurity posture.


NIST Special Publication 800-207

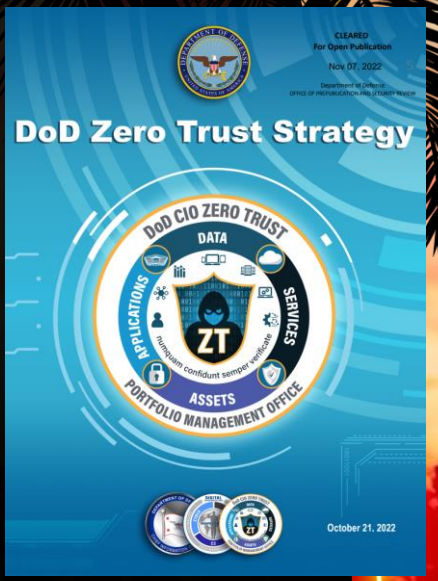
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Objectives

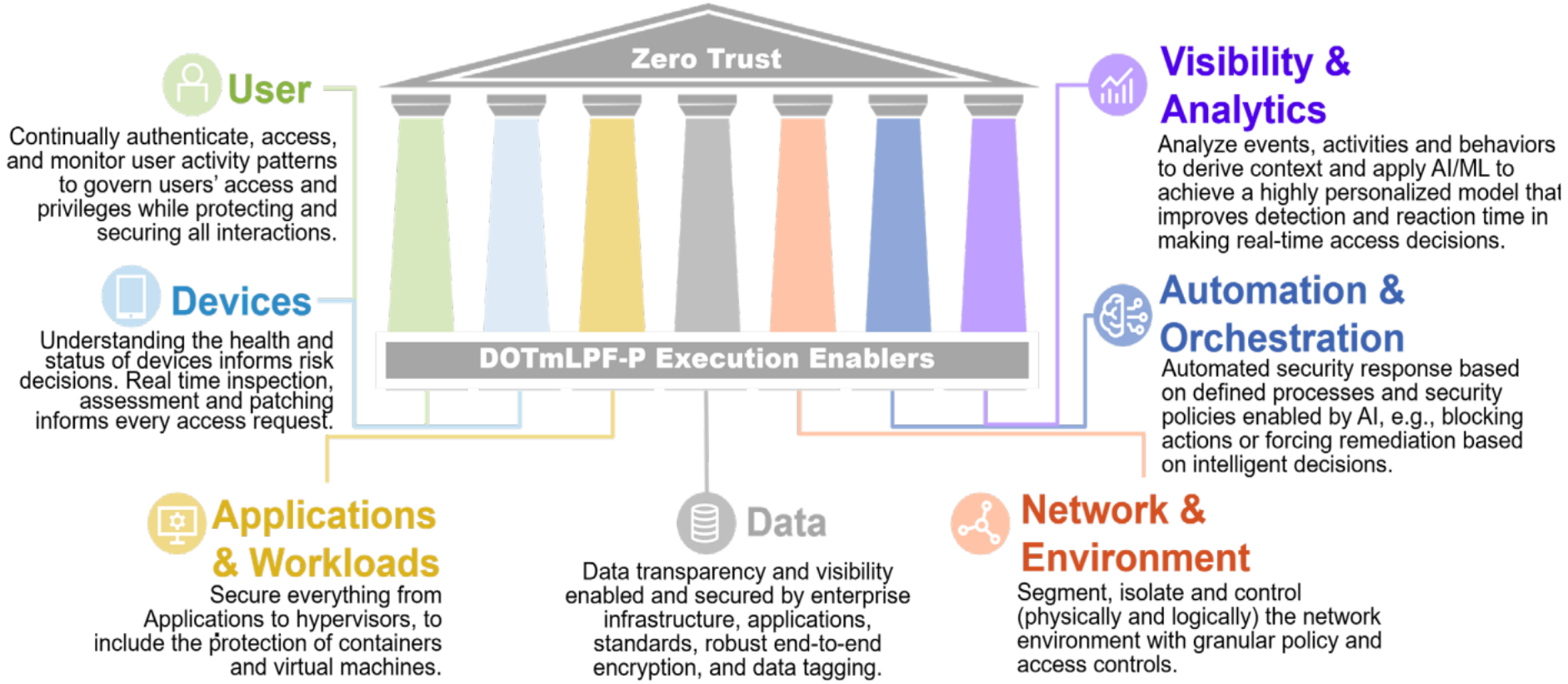
- Implement and enforce the fundamentals.
- Make no assumptions “Never trust, always verify”
- Enforce least privilege
- Granular network segmentation
- MFA++



Benefits

- Risk reduction by decreasing attack surface and impact radius when compromised
- Improve Governance and Compliance
- Business Continuity
- Align the culture with the leadership risk appetite

Figure 3. DoD Zero Trust Pillars



Resources

- Evidence-based cybersecurity policy? – Paper https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2335461
- IGEL OS11 “Hardening” Guide, most still works on OS12: https://kb.igel.com/igelos-11.09/en/securing-igel-os-endpoints-101059859.html
- Device Encryption: https://kb.igel.com/base_system/12.3.2/en/device-encryption-119868588.html
- IGEL Security Notices (ISNs): https://kb.igel.com/securitysafety/en/igel-product-security-information-10346597.html
- NIST SP800-207– Zero Trust Architecture: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- DoD Zero Trust Reference Architecture: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
- Cloud Security Alliance – Zero Trust training: https://cloudsecurityalliance.org/education/zero-trust-training
- DEFCON Talk -- WAF: Making a Problematic Security Tool Suck Less https://www.youtube.com/watch?app=desktop&v=4eDtrbPpZyU
- Elevate AVD and Windows 365 access with insider tips for IGEL OS -- https://www.igel.com/blog/elevate-avd-and-windows-365-access-with-insider-tips-for-igel-os/

Even More Resources

- Maddie Stone's Bsides Canberra Presentation: https://github.com/maddiestone/ConPresentations/blob/master/BSidesCanberra2023.WhenExploitsArentBinary.pdf
- Chromium -- Fighting Cookie theft using device bound sessions: https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html
- CISA's Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- IGEL Preventative Security Model: https://www.igel.com/wp-content/uploads/2024/04/IGEL-Security-Whitepaper_Preventative-Security-Model.pdf
- DoD Zero Trust Strategy: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf



IGEL DISRUPT 24

The Ultimate EUC Event

THANK YOU!

security@igel.com

Juan Zapata
Product Security Manager

Mathias Huber
Senior Product Security Manager