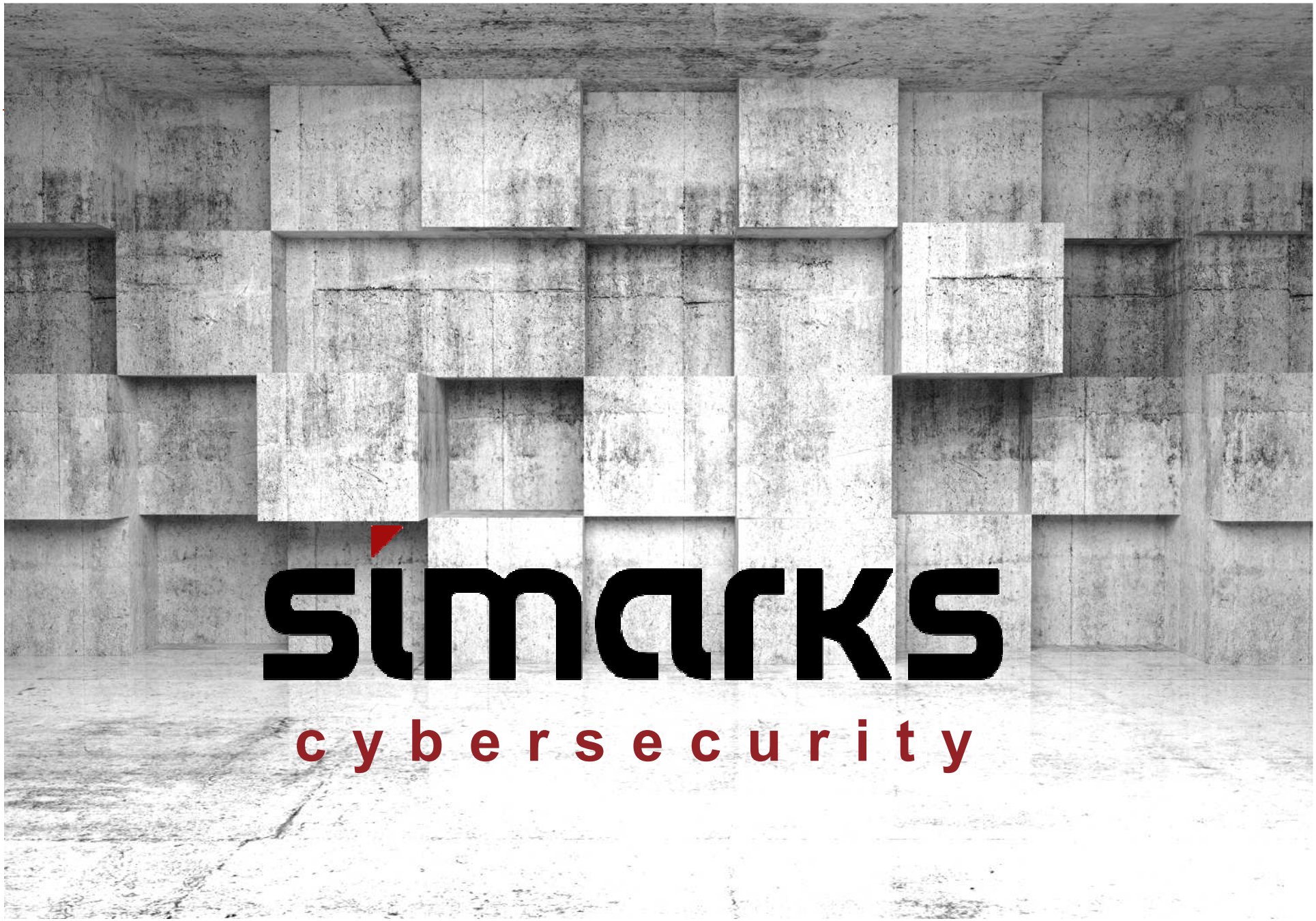


simarks

Zero Privileged Accounts

“removing the human threat”

Privacy & Trust: How to ensure management and control of identities and rights

Principle of Least Privilege

POLP

Privileged accounts are involved on most of cyber attacks.

PAM

Privilege Account Management

US-CERT

"National Cyber Defense Strategy"

The United States Computer Emergency Readiness Team (CERT) best practice guidelines recommend to "Use extra caution with system administrators and technical or privileged users." **Link**

Gartner

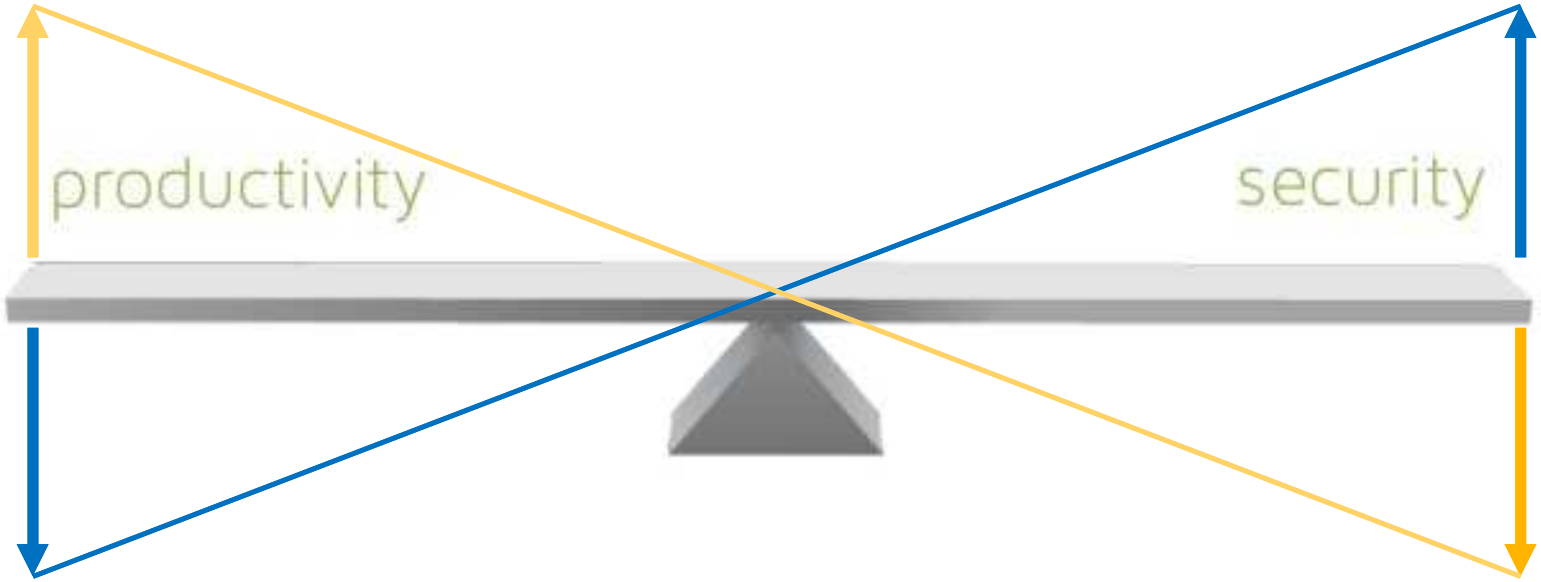
According to Gartner's Neil MacDonald, "organizations should remove administrative rights from all users." **Link**

simarks

Consequences of applying POLP

- Administrative tasks.
- VIP Users.
- Application Management(*).
- Control of TCO.

- Fight against *malware*.
- Confidenciality.
- Information leakage.



(*) *Main reason why adminitrator privileges are granted.*

simarks

What would be the ideal solution?

- ✓ NO administrator users.
- ✓ Only authorized applications must be executed with administrator privileges.
- ✓ Some kind of applications must always be executed with restricted privileges(*).
- ✓ Users can install only authorized applications.

(*) *100% effectiveness against most of malware on the internet.*

simarks

Market Approach

Gartner Top 10 Security Projects for 2018

June 6, 2018
Contributor: Jill Beadle

SECURITY

CISOs should focus on these ten security projects to reduce risk and make a large impact on the business.

No. 1: Privileged account management

This project is intended to make it harder for attackers to access privileged accounts and should allow security teams to monitor behaviors for unusual access. At a minimum, CISOs should institute mandatory multifactor authentication (MFA) for all administrators. It is also recommended that CISOs use MFA for third-party access, such as contractors.

PAM

No. 4: Application control on server workloads

Organizations looking for a "default deny" or zero trust posture for server workloads should consider this option. This project uses application control to block the majority of malware as most malware is not whitelisted. "This is a very powerful security posture," said MacDonald. It has proven to be successful against Spectre and Meltdown.

Tip: Combine with comprehensive memory protection. Is an excellent project for the Internet of Things (IoT) and systems that no longer have vendor support.

No. 6: Detection and response

This project is for organizations that know compromise is inevitable and are looking for endpoint, network or user-focused approaches for advanced threat detection, investigation and response capabilities. There are three variants from which to choose:

- Endpoint protection platforms (EPP) + endpoint detection and response (EDR)
- User and entity behavior analytics (UEBA)
- Deception

The latter is a small but emerging market ideal for organizations looking for in-depth ways to strengthen their threat detection mechanisms with high-fidelity events.

Source: https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/

simarks

Market Approach

BOMGAR

BOMGAR PRESS

Bomgar Acquiring Avecto to Create Leading Privileged Access Management Solution

July 10, 2018

Source: https://www.bomgar.com/press/bomgar-acquiring-avecto/

BOMGAR

BOMGAR BLOG

INDUSTRY UPDATES

Bomgar Acquires BeyondTrust to Build Privileged Access Management Leadership

by Matt Dircks | September 13, 2018

Source: https://www.bomgar.com/blog/entry/bomgar-acquires-beyondtrust-to-build-pam-leadership

In my recent post announcing Bomgar's acquisition of Avecto, I summarized our ambitions to lead the Privileged Access Management (PAM) market by stating "we're only getting started."

I wasn't kidding. Today, I am pleased to announce that Bomgar is planning to acquire BeyondTrust, a recognized front-runner in the PAM industry.

BeyondTrust's impressive pedigree as a cyber security vendor spans three decades. Over the years, the company has continuously delivered innovative solutions as it fought its way to the top of the highly competitive PAM field. Today, BeyondTrust's 4,000 satisfied enterprise customers are testaments to its achievements.

But it's not just BeyondTrust's innovative technology and loyal customer base that attracted Bomgar. It's also the company's recognition as a top-tier performer by industry analysts; its established global partner network; its talented staff of cyber security professionals; and its exceptional, recognizable brand.

For all these reasons and more, we've decided that the combined company will carry forth under the BeyondTrust name, but with the same great Bomgar culture that's earned us more than 16,000 loyal customers. The combined company will not only offer customers and partners a more powerful solution portfolio, but also accelerate innovation and increase resources for service and support.

The combined Bomgar / BeyondTrust entity will be a PAM industry leader from day one. And there's no ceiling. PAM is an ascending sector of the security industry, and according to Gartner Vice President and Distinguished Analyst Neil MacDonald, a Top 10 Security Project for 2018. PAM solves the most common cyber security threats faced by organizations today: stolen or misused privileged credentials, excessive admin rights on endpoints, and unsecured remote access pathways. It's applicable to companies in every vertical market segment and all regions worldwide.

We remain committed to delivering PAM and Remote Support solutions that help secure your organization while enabling users to quickly and efficiently access systems and support your business.

We will be sharing more about the combined company and solution portfolio in the coming weeks and months, but we're already well on our way. Bomgar / BeyondTrust is not only here to stay; we're here to lead, for a long time to come.

simarks

Simarks Approach

Focus on:

- ✓ Consequences of applying POLP.
- ✓ Protecting the most vulnerable element: The Human Behaviour.

Security at Application Level

- ✓ Simarks has developed a core designed to control the security context at process level, capable for assigning privileges to each one, no matter the user's privileges.

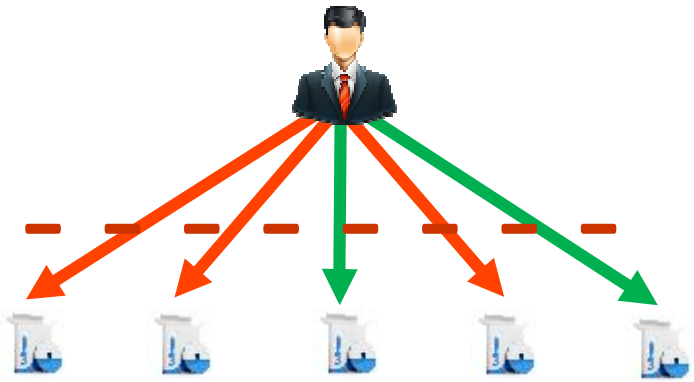
- ✓ Innovative approach that grants the real opportunity to reach zero privileged accounts.

simarks

Simarks Approach

Security at Application Level

- ✓ No matter the user's credentials. All users are standard accounts.
- ✓ Innovative PAM solution.
- ✓ White Listing. Only authorized applications are executed with elevated privileges.
- ✓ Grey Listing. Internet aware applications are always executed with minimum privileges.
- ✓ Black Listing. Block processes matching distribution criteria.
- ✓ Corporate Application Store. Users can only install previously authorized applications.
- ✓ Ransomware.
  - ✓ Real-time cryptographic operations control.
  - ✓ Deny access to network resources per application.
  - ✓ Deny Access to protected folders per application.
  - ✓ Freeze process and ask SOC before continuing.



Simarks Solutions

BestSafe

SDM

Security at Application Level	Password Management	Lifecycle App Management	SOC / AI / SIEM Full Integration
Real-Time Ransomware Engine	Corporate Application Store	Remote Control	Emergency Actions

ZERO Privileged Accounts

Thanks!

Simarks Software
C/ Copenhague 12
Edificio Tifan Oficina 204
28232 Las Rozas
Madrid - Spain
www.simarks.com
+34 910 534 037
info@simarks.com

Contact:
Jorge Marcos
CTO
jorge.marcos@simarks.com

simarks