

PAM is never done: Fudo Enterprise 6.0

Operational resilience,
business continuity, and
accountability in 2026

Table of contents

- 03 **Introduction**
A message from the CEO: Building a digital sovereignty
- 04 **Chapter 1**
The regulatory push and AI threat actors
- 06 **Chapter 2**
Automated trust vs credential theft
- 08 **Chapter 3**
Guardians of integrity
- 10 **Chapter 4**
Securing the distributed frontier – Supply Chain & IoT
- 13 **Chapter 5**
Stronger authentication, safer secret handling
- 14 **Chapter 6**
UI refinement to make you focus on what's important
- 15 **Chapter 7**
Conclusion – The roadmap to continuous resilience
- 16 **Glossary**

Introduction

A message from the CEO: Building a digital sovereignty

Trust is not a marketing claim; it is earned through engineering discipline and ethics. This principle has guided my journey in cybersecurity for over two decades from early contributions to the FreeBSD project to the development of Fudo Security. I have always believed that true protection is built on strong architecture, security-by-design, and a relentless attention to detail. Our mission is to transform these core engineering values into the bedrock of global digital accountability.

We are at a pivotal moment. The global cybersecurity landscape is shifting, and Europe's challenges are growing in both scale and complexity. With that growth comes a profound responsibility to protect our collective digital future. Fudo Security was built to address this need: to secure Europe's digital sovereignty and to harden the operational resilience of organizations worldwide through transparent and uncompromising standards.

Our headquarters and R&D operations are returning to Warsaw - the place where it all began. We are focused on European engineering talent to prove that security solutions built here can set the global benchmark. We are not just building software but a product that can stand with the best in the world, rooted in a culture of technological strength.

Fudo Enterprise 6.0 is the embodiment of this vision. We have moved beyond passive defense to build a solution that stands as a guardian of integrity, ensuring business continuity in an era of relentless threats. Our goal is to raise the bar for the entire ecosystem, ensuring that cyber resilience becomes a standard, not an exception.

The work ahead of us is demanding, but it is deeply meaningful. We are ready to set the standards for modern protection.

Paweł Dawidek
CEO & Co-founder
Fudo Security

The regulatory push and AI threat actors

In 2025, cybercrime was predicted to cost the world \$10.5 trillion USD. If it was measured as a country, cybercrime would be the world's third largest economy after the U.S. and China.

Cybersecurity Ventures

At the end of 2025, the prediction remained unchanged (Government Technology).

In 2026, the global cybersecurity market will undergo a structural reorganization shifting towards protection of identity, infrastructure and managed services, according to new insights from global market intelligence firm CONTEXT (Context, 2026). Reasons behind that shift can be related to the ongoing implementations of DORA (Digital Operation Identity Resilience Act) regulation and NIS2 (Network and Information Security 2) framework.

Under NIS2 and DORA, effective cyber risk management and senior management's personal accountability are core elements of business strategy. This foundation of operational resilience guarantees stable and secure operations within the EU market.

With NIS2 and DORA in force, maintaining and regularly updating a Business Continuity Plan (BCP) has shifted from a best practice to a strict legal requirement. CEOs must ensure these plans move beyond theory to reflect real-world risks and actual recovery capabilities. Today's digital landscape leaves boards with no room for error.

Global Cybersecurity Outlook 2026 introduced by World Economic Forum points out that CEOs of even highly resilient companies are mostly concerned with AI vulnerabilities. Threat actors gain expertise in this field and deepfakes prove to become hardly recognizable.

Having in mind compliance and real threats, organisations must therefore change their way of thinking from one-time solution implementation to ongoing cybersecurity discipline.

That's why we give you Fudo Enterprise 6.0 - the newest version of our reputable and acclaimed Privileged Access Management (PAM) solution to provide you with a solid answer to ongoing and emerging threats.

What's new?

Below you'll find links to official documentation.

01

Password vault

09

Reverse SSH tunnel support

02

Reverse proxy

10

Anonymous account support for SSH tunnel sessions

03

New user interface languages

11

Custom hostname in the title of RDP sessions

04

Complete user interface refresh

12

Session source visibility

05

Redesigned table interface

13

Fullscreen mode in webclient

06

CHAP and MS-CHAPv2 authentication for Radius

14

Secure clipboard

07

Support for the PostgreSQL protocol

15

API changes

08

VNC over TLS support

We maintain a continuous solution improvement and stick to the philosophy that PAM is never done.

Automated trust vs credential theft

Privileged access is still the most critical pathway for threat actors to invade sensitive systems and data.

Keys to the Kingdom, Mandiant

It is a foundation of organizational resilience. Through the past few years lots of IT environments have modernized, moved to the cloud, applied both human and non-human identities. The overall attack surface expanded encompassing compromising privileged accounts and virtual systems including virtual machines (VMs).

Credential theft still remains the highly exposed attack vector. The World Economic Forum's 2026 report praises AI agents as an efficiency enhancing factor and support in scalability as well as automation of complex and repetitive tasks. Yet, at the same time the report indicates that managing credentials, permissions and interactions becomes more critical than ever. AI agents can store excessive privileged accesses, be manipulated through prompt injections and design flaws (Global Cybersecurity Outlook 2026).

Keys in the vault

Fudo Enterprise 6.0 neutralizes credential theft with the **Password Vault** solution. It involves secure credential storage supporting organizing, and controlling access to sensitive credentials such as passwords, SSH keys, API keys, certificates as well as secure notes. What is more, Password vault brings the **lifecycle management** which means an automated credential rotation directly to stored secrets. It enforces **Credential Hygiene**, ensuring that even if a "secret" is somehow compromised, its lifespan is too short to be of use.

The Password Vault is governed by a Role-Based Access Control (RBAC) model that defines who can manage collections and perform administrative actions such as creating, modifying, deleting, and moving them. Access to the secrets stored within collections is additionally governed through dedicated permissions, ensuring that sensitive information is available only to authorized users.

Collection notifications keep users informed about important events and changes related to their assigned collections. This feature helps maintain security awareness and ensures proper oversight of secret management activities.

To further strengthen security and compliance, administrators can use the Secret Access view to track exactly who accessed which secret and when, making audits easier and helping identify potential issues at an early stage.

Automation eliminates "security friction." By automating complexity, rotation, and audit trails, Fudo ensures compliance is a byproduct of daily operations, not a manual burden on the IT team.

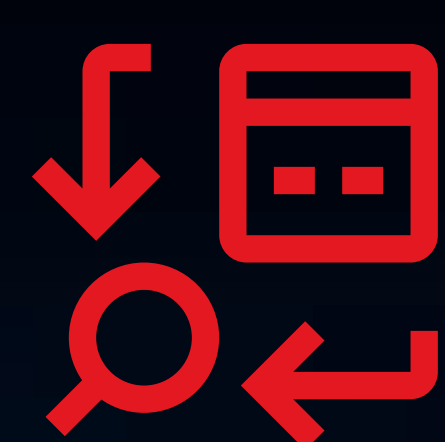
Guardians of integrity

Are you paying enough attention to your infrastructure?

In many of the 2025 investigations Mandiant identified evidence of data thefts. Threat actors targeted credentials and reconnaissance data useful for maintaining persistence, lateral movement, and escalating privileges (Mandiant M-Trends, 2026).

While most attention is placed on external activity, an attacker's dwell time can last up to 277 days from detection to containment (IBM/Baker Donelson, 2025/2026). Conversely, ransomware actors like those described in the 2026 Sophos Active Adversary Report may reveal themselves in just 3 days to extort a ransom (Sophos, 2026). Having in mind that a threat actor can operate under the radar for a long time, it's crucial to focus more on the internal environment and secure access to most valuable assets and secrets.

Why internal security matters



An attacker's dwell time can last up to 277 days from detection to containment



Ransomware actors may reveal themselves in just 3 days to extort a ransom

Proxies, PostgreSQL & operational security

In Fudo Enterprise 6.0, this logic translates into capabilities that reduce exposure and increase control where it matters most.

Reverse Proxy helps organizations make selected internal services available without relying on direct inbound access to the protected environment. By using an outbound SSH tunnel to an intermediary host, it fits segmented networks and gives administrators clear visibility into tunnel state, mappings, and operational status.



Enhanced security

Internal resources can be exposed externally without direct inbound access to Fudo Enterprise.



Total oversight

Clear tunnel status monitoring and simple toggle-based control.



Flexibility

Precision control over which specific services are made available externally.

Fudo Enterprise 6.0 also brings PostgreSQL support, extending PAM deeper into the data layer.

This is a major step forward for organizations that need to protect not only access to systems, but also the actions performed on business-critical data. By enabling control over risky SQL activity in real time, Fudo helps reduce the risk of harmful operations performed by highly privileged users, such as DBAs or superusers.

Finally, Fudo Enterprise 6.0 adds TLS support for VNC, helping organizations better protect access to graphical environments where visual consoles remain essential. From SCADA systems to medical and operational interfaces, these sessions often support sensitive tasks that should not remain outside the PAM model.

Securing the distributed frontier – Supply Chain & IoT

Devastating chain of events

Third party and supply chain vulnerabilities are the greatest challenges to become cyber resilient according to CEOs of highly resilient organizations in the World Economic Forum's Cybersecurity Outlook 2026 survey ([Global Cybersecurity Outlook 2026](#)). It is hard to be surprised as this type of attack is difficult to detect. In one scenario, a malicious actor compromises legitimate industrial control system (ICS) software. First, he takes control of the websites of ICS software vendors, and then replaces the legitimate files in their repositories with his own versions infected with malware. Then, when the ICS software is downloaded from the vendor's website, it contains embedded malware that may include capabilities enabling remote takeover of the systems.

Last year's devastating cyber attack on Jaguar Land Rover - the United Kingdom's largest automotive manufacturer - proves CEOs' concern to be justified ([Jaguar Land Rover Automotive](#)).

Consequences of Jaguar Land Rover cyber attack



**Global operations
halted for 5 weeks**



**More than 5,000
suppliers affected**



**Cyber-related costs were
estimated at £196 million**

(\$260 million)



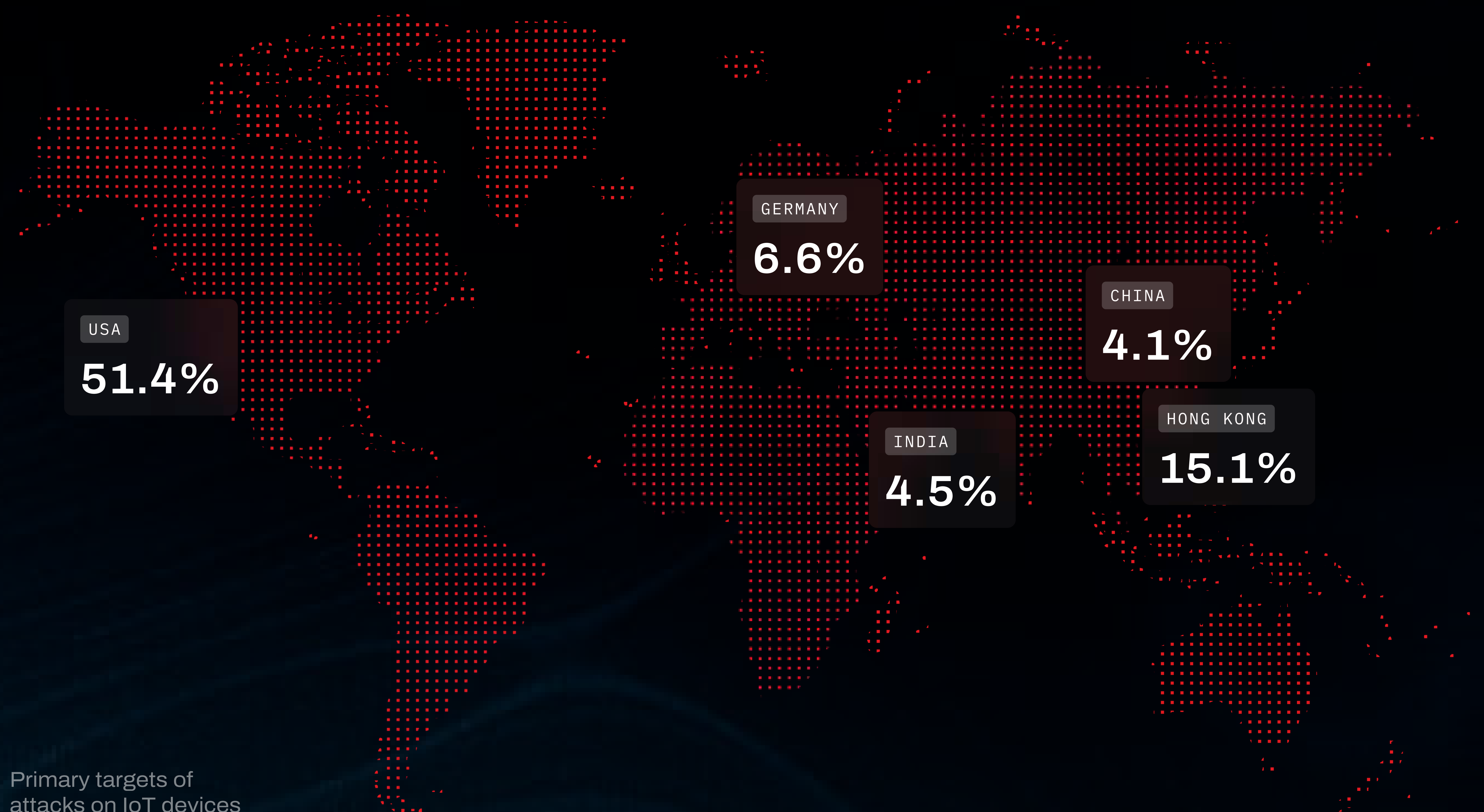
**Nearly 25% drop
in revenue**

Supply chain attacks are difficult to detect because they exploit trust between vendors and customers as well as computer to computer communications. According to the [Cost of a Data Breach Report 2025](#), it takes 267 days to detect and contain results of the supply chain attack.

From IoT compromise to paralysis of public services

According to the latest report by **Zscaler**, cyberattacks also surge against IoT, mobile devices in critical infrastructure. In 2025, manufacturing, energy, oil & gas, and retail & wholesale were the most targeted industries. Attacks on the energy sector increased by 387%, while attacks on the healthcare sector rose by 224.39% compared to the previous year.

The United States is the primary target of attacks on IoT devices, as evidenced by a 54.1% increase in cybercriminal activity. Furthermore, the increase was 15.1% in Hong Kong, 6.6% in Germany, 4.5% in India, and 4.1% in China. The manufacturing and transportation sectors were hit hardest by attacks on IoT devices, which accounted for 40% of all malware attacks, with each sector accounting for 20% of the total.



Attacks of this kind occur for several reasons

Cybercriminals hope to reap substantial financial gains and also seek to destabilize the functioning of governments and citizens. The energy and healthcare sectors play a vital role in daily life, and a disruption in these areas can significantly degrade its quality. For this reason, the management of targeted companies may be more inclined to pay ransoms following a successful ransomware attack; however, the truth is that paying the ransom does not guarantee security. There have been numerous reports in the media of cybercriminals continuing to harass companies even after their demands have been met. So what should be done? Strengthen cybersecurity.

Enhanced security for remote devices and suppliers



Reverse SSH

Secure inside-out connections

Fudo Enterprise 6.0 adds a safer way to connect to remote devices, such as IoT sensors or factory equipment, located in hard-to-reach locations. Instead of relying on a direct network path, the connection can be established through an SSH reverse tunnel. This creates a secure tunnel endpoint that allows authorized users to manage the equipment while limiting direct exposure of the target service. This approach is especially valuable in distributed and supplier-managed environments, where tighter control over how connections are established helps reduce risk.



Anonymous account support

Clear accountability for guest access

Sometimes, external vendors or automated systems use anonymous or shared keys to log in. Our system now automatically links these sessions to the specific person who started the connection. This means even if a generic account is used, we always know exactly who is responsible.



Session source visibility

Full transparency

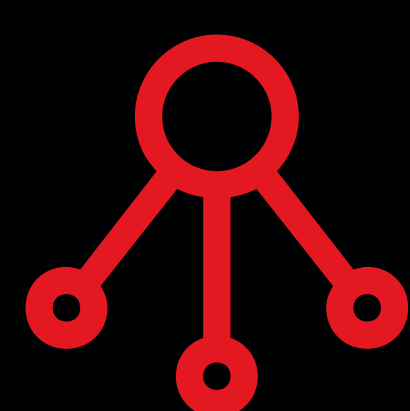
We have enhanced session visibility by showing where each connection originates within the Fudo ecosystem. In the Sessions view, administrators can now see which product initiated the connection, such as Fudo Enterprise or ShareAccess, as well as the connection method used, including WebClient or Native Client. This gives security teams clearer context for session analysis and helps them better understand how users access protected resources.

Stronger authentication, safer secret handling

Not every improvement in PAM needs to be dramatic to matter. Some of the most practical gains come from reducing friction in authentication and limiting how easily secrets can be exposed during everyday administrative work.

More flexible trust at the authentication layer

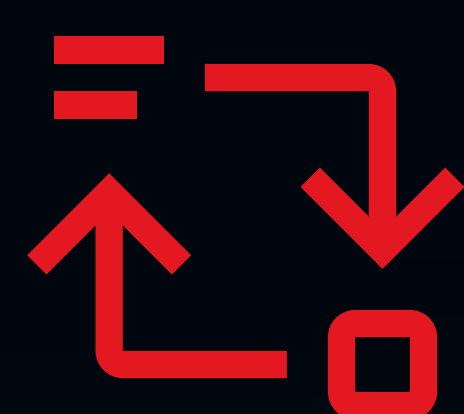
Fudo Enterprise 6.0 adds CHAP and MS-CHAPv2 support for RADIUS, giving organizations more flexibility in how privileged users are authenticated. Alongside existing PAP-based deployments, Fudo now supports challenge-response methods used in a wider range of enterprise environments. This improves compatibility with existing identity infrastructure and helps organizations align authentication flows with their operational requirements.



**CHAP and MS-CHAPv2
support for RADIUS**



**Expanded authentication options
for privileged access**



**Improved compatibility with
existing identity infrastructure**



**Flexible authentication flows for
operational needs**

Secure Clipboard Preventing visual data leakage

Fudo Enterprise 6.0 also introduces a simple but useful privacy improvement in the Web Client. When users copy a sensitive password or secret, they can now use the eye icon to hide its visible value in the interface. This helps reduce accidental visual exposure during screen sharing, remote support sessions, or work in shared environments.

These changes are small by design, but practical in daily use. Together, they make authentication more adaptable and secret handling more discreet – without adding unnecessary complexity.

UI refinement to make you focus on what's important

“

Don Norman
“The Father of
User Experience”

Good design is actually a lot harder to notice than poor design, in part because good designs fit our needs so well that the design is invisible, serving us without drawing attention to itself.

This is the guiding principle behind our efforts to improve the user experience. We strive to make the UI helpful and intuitive, which is particularly important in cybersecurity. In critical moments, you need a design that makes your work easier, so you can spend your time responding to suspicious activity rather than getting lost in the interface.

We introduced a comprehensive visual redesign across the Fudo platform, delivering a more modern and consistent look while preserving familiar workflows and functionality. The update also simplifies navigation through a restructured sidebar with collapsible sections and clearer grouping of related features.

Conclusion – The roadmap to continuous resilience

Transition from Check-box to discipline Treat cybersecurity as a living process

Experts from the World Economic Forum and leading technology thinkers agree: in 2026, cybersecurity has evolved far beyond a mere compliance requirement. For too long, security measures were often treated as reactive, check-the-box exercises – driven by audits rather than a fundamental commitment to operational health. We've seen that interest in these implementations often wanes once the audit is passed, leaving organizations vulnerable to shifting threats.

However, treating cybersecurity as a peripheral task is a risk that few can now afford. Beyond the immediate impact of a breach, the real challenge lies in maintaining business continuity and preserving the trust of customers and partners. True digital maturity means integrating security directly into the corporate DNA – not as an emergency response to a crisis, but as a proactive investment in the long-term resilience and reputation of the enterprise.

The dynamism and volatility of the digital battlefield, particularly due to the use of AI, necessitate a strategy of constant readiness and discipline in building a secure corporate environment. Cybercriminals are also observing new market changes, acquiring new skills, and do not hesitate to use them. We can no longer ask ourselves whether we will be attacked, but rather how we will respond to an attack.

Fudo Enterprise 6.0 is the bedrock of a modern **cyber resilience** strategy. In a world where cybersecurity

Glossary

Anonymous account support	Support for associating SSH tunnel sessions established through an anonymous account in Fudo with the initiating Fudo user, so administrators can identify who started the session.
Collections	A digital set of sensitive data, allowing administrators to manage group-level access without configuring individual passwords.
Credential hygiene	A set of practices designed to keep passwords and access keys secure and clean. This includes automated password rotation after each session, eliminating static credentials, and ensuring that high-privilege accounts are never shared between multiple users.
Cyber resilience	The ability of an organization to maintain continuous operations despite experiencing a cyberattack. Unlike traditional defense, resilience assumes a breach will occur and concentrates on minimizing impact and ensuring rapid recovery.
Digital accountability	The principle that every action within a system must be uniquely attributable to an individual. This aligns with frameworks like NIS2 and DORA, where the Board of Directors is held legally responsible for the organization's security posture.
Lateral movement	A technique used by attackers to navigate through a network after gaining an initial foothold. Once inside, they attempt to hop from one server to another to reach high-value data. PAM systems are designed to block these unauthorized transitions.
Mutual authentication	A security standard where both parties in a connection must prove their identity. Not only does the system verify the user, but the user’s device also verifies the legitimacy of the gateway, protecting against impersonation attacks.

Glossary

Reverse Proxy

A Fudo Enterprise feature that uses a reverse SSH tunnel to make selected internal services available through an external SSH server or DMZ host.

The external SSH server/container serves as the access point for users connecting through the Reverse Proxy. Instead of connecting directly to Fudo, clients establish their connection to this external server, which then forwards traffic through the reverse SSH tunnel into the internal environment.

Reverse SSH

An SSH tunneling method where the connection is initiated from the inside to an external host, allowing authorized users to reach internal services through a secure intermediary endpoint.

Supply chain risk

The vulnerability arising from dependence on third-party vendors. If a supplier's remote access is breached, attackers can pivot into your network. Managing this requires strict auditing and recording of every external session.

Zero Trust

A security model based on the principle of "never trust, always verify." Regardless of the user's location, the system treats every access request as a potential threat, requiring continuous identity verification at every step.



Fudo Security HQ
Fudo Security Sp. z o. o.
Al. Jerozolimskie 178
02-486 Warsaw, Poland
+48 22 100 67 00

Sales contact
sales@fudosecurity.com

