
OT-Umgebungen
(nicht nur) für Remote-
Connections einfach und
sicher zugänglich machen

PrivX for OT environments



Business at Risk?

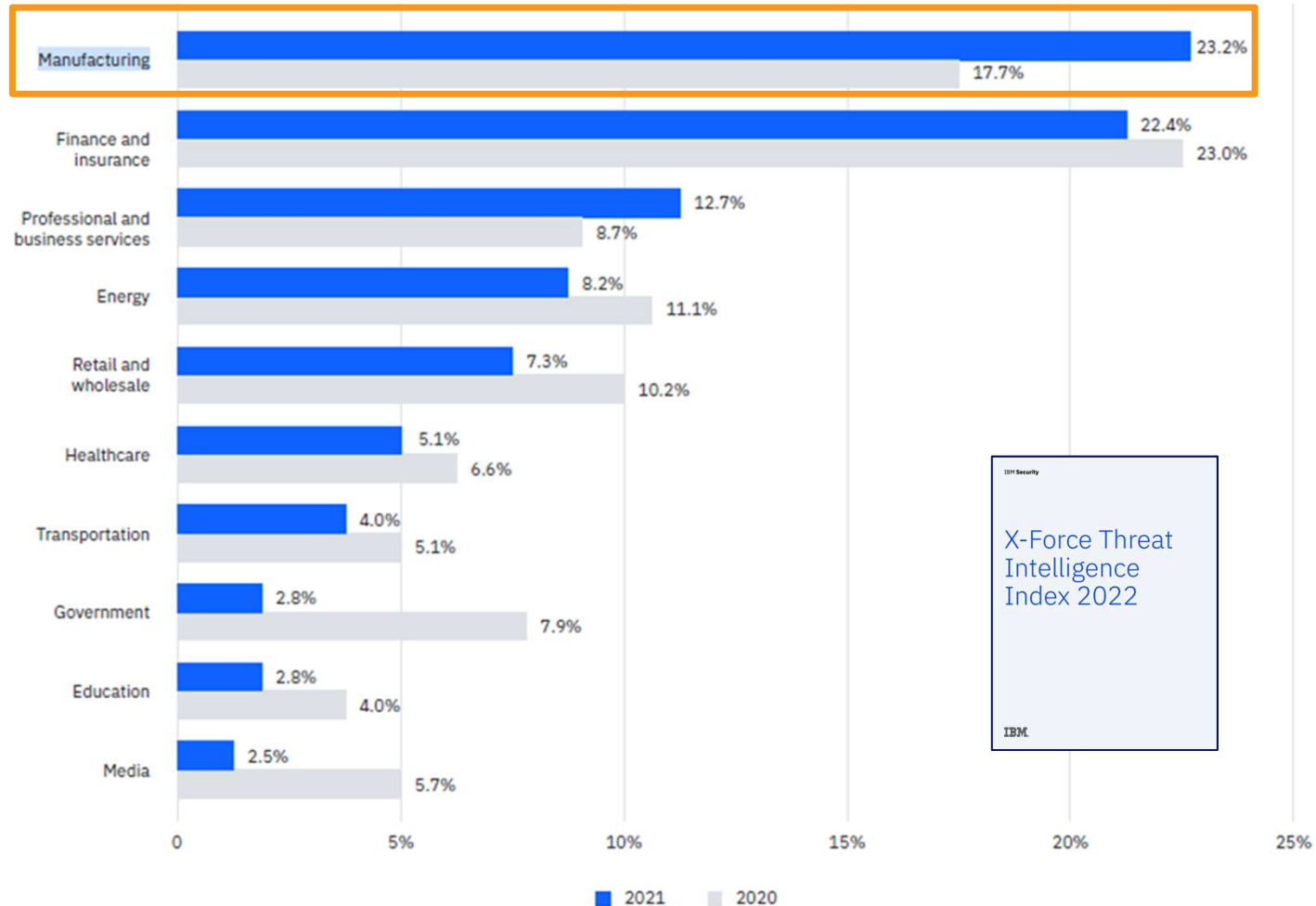
- Attacks are real



Figure 20

Breakdown of attacks on the top 10 industries, 2021 vs. 2020

(Source: IBM Security X-Force)



Typical Use Cases

USERS, APPLICATIONS

Internal users



IT/OT admins

Are responsible of global infrastructure and policies.



Site admins

Are responsible of site safety and granting access only to authorized users. Want see what is going on and what was done?.



Service engineer
(user, admin, root)

Needs to connect systems in test and production environments using different types of applications.

External users



Service engineer

Needs to connect systems in test and production environments using different types of applications.



System Vendors,
Integrators

SYSTEMS, RESOURCES

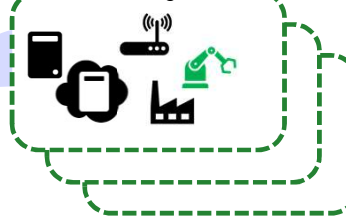
R&D site



Development, Testing

Digital twins

Manufacturing site(s)



Remote access and control

Emergency fixes

Maintenance
Patching/upgrading

Monitoring/stats

Optimization

Servers, network appliances, applications,
HMI's, PLC, etc.

Challenges for Easy and Safe Access Interactive & M2M

Risks

- Safety hazards
- Quality issues & machinery break down
- Operational service downtime
- Intellectual property and customer data theft & Loosing reputation as a company



Compliance

- Security audit failure related to Industry regulations
- Lacking up-to-date security audit reports
- Incomplete access governance



Productivity

- Security slows down operations
- Time and labour intensive access provisioning processes
- Too many different systems to maintain
- Secure remote & 3rd party access



Security

- Shared Credentials in the wrong hands
- No visibility: Who/what has access to what & when?
- Passwords and secrets are "leaking" outside
- Security system by-pass

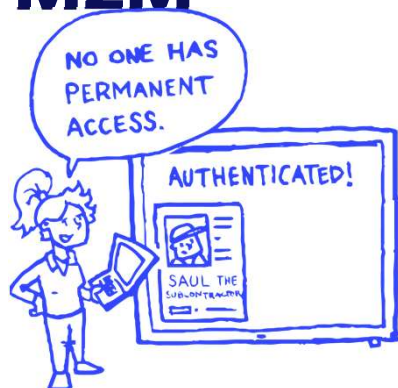


Challenges for Easy and Safe Access Interactive & M2M



Reduce risks

- Prevent unauthorized access
- Uniform, single point of control to all machine and human access
- Prevent harmful consequences with incorrect access rights



Ensure compliance

- Comply with industry regulations
- Monitor, audit and record sessions for forensics and integrate with SIEM
- Integrations to HR and IT solutions



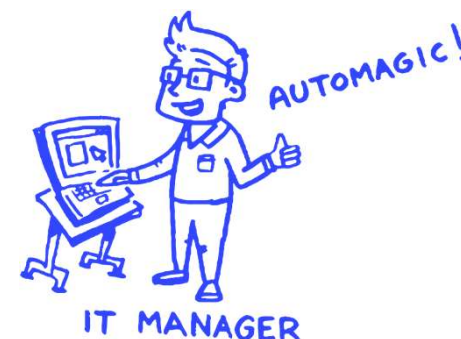
Increase productivity

- Reduce the overhead of managing secrets by eliminating rotation and vaulting
- Single Sign On to all resources from one system



Improve security

- Right identity with the level of right access to the right target for the right duration
- Session monitoring and recording. SIEM integration
- Monitor/prevent by-passes



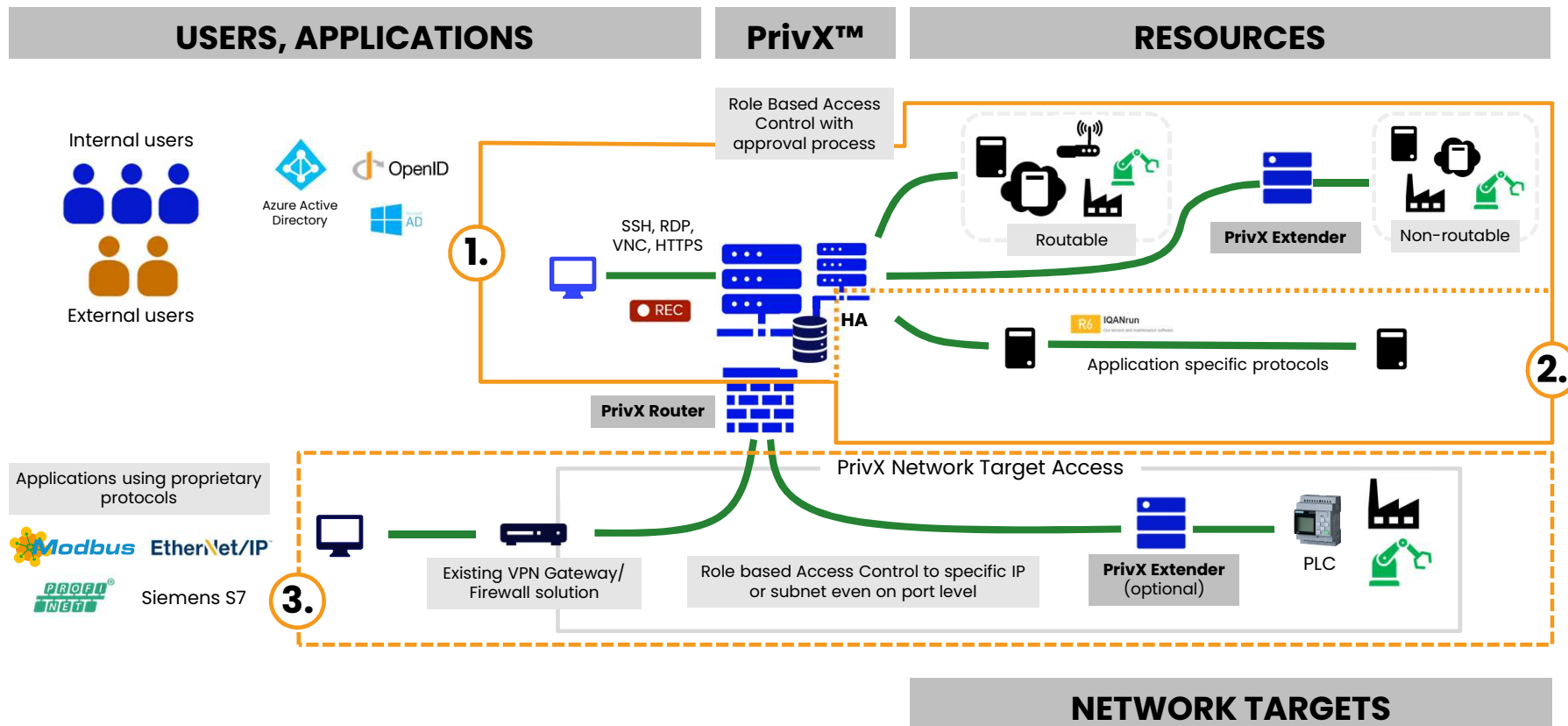
NIS 2.0 Tightens EU Requirements and Sanctions

- Cybersecurity **risk management** policies
- **Incident response**
- **Supply chain security**
- **Encryption**
- **Vulnerability disclosure**
- **Swift reporting** in order to avoid the potential spread of incidents
- **In-depth reporting** to draw valuable lessons learned from individual incidents

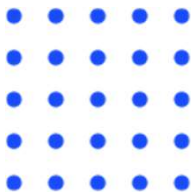


- **Modern Security Tools** and comprehensive **processes** are needed to help companies and public entities comply with regulation, adding minimum TCO and personnel overhead

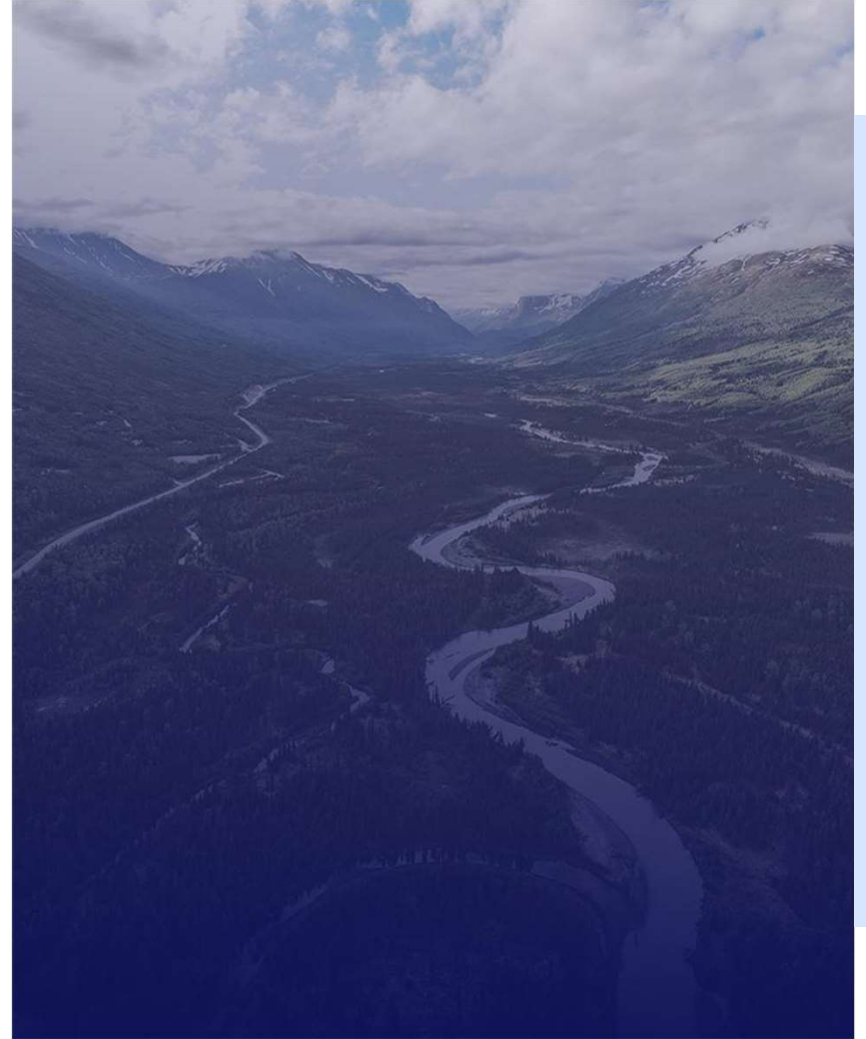
Accessing Resources and Network Targets



Customer Use Cases



SSH.COM



Use Cases for PrivX Secure OT Access

IoT & Automation system vendors; Device & sensor access & data collection



Intelligent household device service access

- Protect service business
- No shared secrets for authentication



Sea-port infrastructure engineering remote access

- Connectivity to remote terminals running PLC systems
- Role-based access , regional limitations

What Makes Us Different for OT and IIoT?

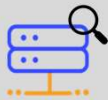
Various point solutions are **limited** and **complex** to maintain



Remote access (SRA) is not enough



Firewalls and VPNs are revolving doors



Network and IP monitoring is contentless



Traditional PAM systems are designed for IT admins, not OT

74%

of data breaches start with digital keys in the wrong hands

83%

of organizations don't have robust processes to control their digital keys

95%

of cloud breaches in 2020 were predicted to be due to customer vulnerabilities

SSH.COM offers a full stack of layered security tunnelling, encryption, and access management solutions. **PrivX OT Edition** offers:



Just-enough-access (JEA)

Just enough access to get the job done with **role-based** access control and approval workflow.



Workflows and approvals

Build in workflow engine for creating approval processes and granting role permissions



REC

Auditing and session recording

Send audit events to external systems (e.g., SIEM). Full transparency for shared accounts.



Access resources just-in-time (JIT)

"never trust, verify real-time all the time". Always synchronized with Identity Management Systems.



Move to ephemeral certificates

Gradually get rid of passwords and keys and move to short lived certificate-based authentication.



Safeguarding and **Protecting**
businesses in changing, complex, and
increasingly unsafe **digital world.**

Dietmar.Wyhs@ssh.com +49 160 8891247

