IIoT Security: Managing Identities & Privileges

BY ROB BLACK, CISSP

Table Of Contents

Executive Summary 1

I. IIoT Security Framework 1

II. The Privileged User 3

III. IIoT Architecture 4

IV. IIoT Systems 5

V. IIoT Credentials 6

VI. Recommendations 6

Moving Toward Holistic IIoT Security 7

Appendix: Utilizing BeyondTrust's Privileged Access Management Platform to Enforce IIoT Security 8

Table 1: How Beyondtrust's Solutions Map to Secure IIoT Best Practices 8

Beyondtrust's Privileged Access Management Platform 9

About 10

EXECUTIVE SUMMARY

Armed with only a web browser, a cyber attacker can use a website, such as Shodan, to find vulnerable Industrial Internet of Things (IIoT) devices in your environment. IIoT devices can be a significant entry point for attackers to compromise your infrastructure. While the consequences of traditional cyberattacks typically include loss of confidentiality and perhaps downtime, IIoT attacks can wreak catastrophic damage – including physical harm. With more than 56% of organizations saying IIoT is now mainstream, it's never been more important to ensure end-to-end IIoT security. This white paper provides the framework for IIoT security decision-making and gives you a deep dive into one of centerpieces of IIoT security... **privileged credentials and their associated permissions** for the devices and systems.

I. IIOT SECURITY FRAMEWORK

There are many IIoT security frameworks, such as the Industrial Internet Security Framework, Online Trust Alliance IoT Security & Privacy Trust Framework and NIST Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things. For this paper, we have distilled the most common and important themes into a usable framework for evaluating your IIoT security. The Framework covers:

- Devices
- Supply Chain and Updates
- Identity and Access Management (IAM)
- Cryptography and Communications
- Configuration
- Monitoring
- Incident Handling

The ensuing sections of the paper review each of these Framework elements, with guidance on how to address each in your enterprise.

Devices

The device is the centerpiece of your IIoT security. The device is the "Thing" that puts the "T" in IIoT. Establishing strong device-level security is essential for a successful IIoT program.

If you are a device manufacturer, you need to develop the firmware and applications with a secure Software Development Lifecycle (Secure SDLC), which includes testing device security.

If you are a customer, you can either take the word of your vendor, or you can ask for documentation illustrating the security practices of the device. And if you're a particularly security-minded customer, you could take it upon yourself to perform security testing on the device.

Supply Chain and Updates

Any device that has not been updated with the latest security patches is susceptible to attack. Although this is one of the most important attributes of operating IIoT devices, updating a library is often a low priority for development teams. If you are operating IIoT devices, you must keep them updated. Exploiting known vulnerabilities of IIoT devices is one of the lowest hanging fruits available to cyber attackers.

IIoT systems require a method for updating the firmware and software on the device. If your vendor(s) do not provide such a mechanism, then you should not be using those devices. If you are a vendor, you need to provide a mechanism for updates.

Almost all software today involves a complex supply chain with hundreds or thousands of vendor components embedded within it. IIoT suppliers must have a handle on the supply chain they use. Customers must be diligent to ensure that their vendors know all of the components within their IIoT and have methodologies for keeping the components up-to-date.

These are all non-trivial challenges that few vendors have completely solved today. Not all vendors are created equal. Hold your vendors accountable for successfully managing these challenges.

Identity and Access Management (IAM)

IIoT runs on connections between people, devices, and applications. Creating and managing the identities for these entities is a critical step in securing the IIoT systems. Absent or mismanaged, identity and privileged access control can open your organization to significant risks from external threats.

While it is important for IAM to effectively manage users, management must be extended to end devices and networks. An identity must exist for all the edge devices, gateways, and cloud servers to ensure that all the devices can be secured. Having properly managed identities can enable your organization to reduce the risk of system compromise.

The remaining sections after the IIoT Framework will delve deeper into IAM.

Cryptography & Long- and Short-Haul Communications

An IIoT system typically crosses multiple organizations' networks. A system is only as secure as the weakest element of the solution.

IIoT systems operate by the means of long- and short-haul communications. The gateway and the data center, or cloud, communicate using long-haul communication protocols. The security of long-haul communications is well understood. One just needs to encrypt the traffic. This is the methodology for securing the communication for existing websites and cloud applications.

The communications between the IIoT sensor, device, and gateway, on the other hand, use short-haul communication protocols. These messages can be sensor updates, telemetry data, commands, alarms, events, logs, status changes, or configuration updates. Whether they are protocols across an OT network or wireless protocols using Zigbee or Bluetooth, often these protocols present significant security challenges. Selecting appropriate protocols and securing the environment that insecure protocols utilize are important steps toward mitigating cybersecurity risk.

Data at rest and in transit between deployed endpoints, gateways, and cloud management servers must be encrypted to reduce the likelihood of compromise. Encrypting data on disk, especially for devices that are deployed in others' environments, is critical. Ensuring that good cryptographic libraries are used is also important so that attackers cannot compromise the encryption via known vulnerabilities.

Configuration

Security misconfigurations can result in IIoT devices being exposed to the Internet, and consequently, vulnerable to attacks. IIoT systems often have insufficient security configurability since many of these connected things are left with default configurations to simplify deployment.

To improve security, operators must harden IIoT systems, such as by closing network ports and turning

off services that are not used. If risky services and ports are used, mitigating controls should be put in place. To mitigate the risk of Internet communication with a malicious server, configuring devices to only communicate with known, good servers is a wise policy.

Additionally, default passwords present a massive risk. While they allow organizations to simplify device deployment at scale, they also can allow hackers to compromise devices at scale. Also, default and embedded passwords should be rotated and brought under active management.

It is important that you evaluate the entire system for vulnerabilities in applications, credentials, networks, security policies, web, cloud and mobile interfaces, and the physical security of the components of the system.

Monitoring

IIoT security can only be effective if the system is actively monitored and managed. Gaining operational insight that comes from monitoring the devices, gateways, and networks of your entire IIoT system should be a security priority.

Device manufacturers and system operators need a way to monitor the device and have an action plan in case something goes wrong.

Monitoring your devices and network for malicious usage patterns, denial of service activities, and unauthorized access can help detect potential attack scenarios and make sure that your devices are being used for their intended purpose. Typically, this type of monitoring would occur in a Security Operations Center (SOC). If your organization doesn't have a SOC, then it can be outsourced to companies, such as MSPs or MSSPs, that specialize in this type of offering.

Incident Handling

Appropriate planning and response to an incident can mean the difference between a resilient organization that can fend off or withstand a cyberattack and one that is severely impacted or crippled. Preparing an incident response plan ahead of time will help you contain an attack, limit the damage, and restore the systems rapidly and effectively.

IIoT is a complex, interconnected environment, and security should be meaningfully addressed with a collective commitment and a mutual obligation from both the vendor and the customer.

II. THE PRIVILEGED USER

Operators of IIoT systems must be able to manage the users who are authorized to log in to the devices in the system. These users may include customers and employees as well as the privileged users who have access to the organization's systems.

Users with administrative privileges have powers significantly greater than those available to a typical user. If these privileges are abused by an insider or obtained by an attacker, they can represent a lethal threat.

Use Case Example – Limiting Insider Privileges to IIoT Devices

Utilities are increasingly adopting smart meters to monitor resource usage. Imagine that one day a utility tried to send out a bill and found that they had no data! This happened for a water company in five cities across three US states. A former employee of the water utility had logged in to the system and turned off the monitoring for many locations. His access to the base stations was not revoked after termination. He simply logged in to the system from his home computer using the same passwords that

he had been using while employed.

Protecting against attacks levelled by former employees requires having good processes and technology. The following controls will help to prevent ex-employees from successfully targeting your organization:

- Monitoring the network and systems actively
- Disabling the ex-employee's accounts as soon as the employee is terminated
- Changing the system passwords after the departure of an employee
- Checking for active employment before authorizing any technical support help
- Auditing the authorized VPN users
- Using Privileged Access Management (PAM) to manage all system level accounts

Ex-employees aren't the only ones capable of inflicting damage. Company insiders, such as the existing employees, vendors, and consultants – also connect to an organization's network and may represent a risk. Typical security tools don't flag when someone is trying to gain inappropriate access using legitimate authentication, and most organizations do not have a streamlined process for managing privileged accounts, which simply increases their risk of being misused.

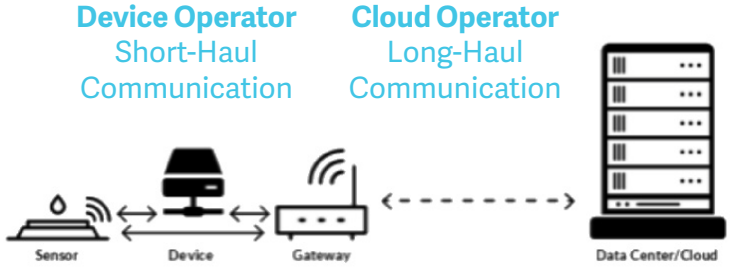
Cybercriminals are aware that an organization must support a variety of technology platforms and will attempt to compromise the credentials of legitimate users to exploit the enterprise system. As an organization, you may support a diverse landscape of users across numerous applications. A centralized platform to manage your privileged accounts helps to exercise tight control over the creation and authorization of privileged credentials. Having a single platform to monitor privileged groups not only improves security and relieves administrators of the burden of managing access controls on many diverse systems, but also reduces long-term costs.

III. IIOT ARCHITECTURE

As more and more devices are connected with the purpose of sharing and gathering data, the IIoT architecture becomes increasingly complicated. This environment looks very different than a cloud application where there are limited entry points. IIoT systems present a broader attack surface due to various types of devices, operating systems, and protocols used.

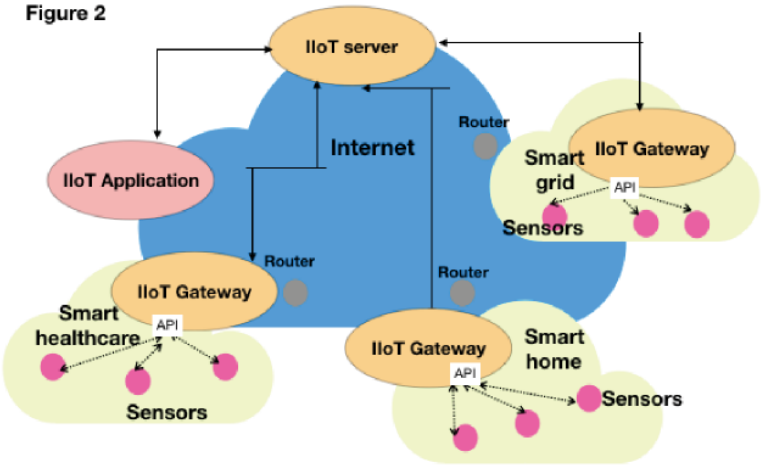
Figure 1 below shows how there are different operators involved in an IIoT system – the device operator, cloud operator, and the communications system. These services could be provided by different entities. What makes this an interesting challenge is that to make the IIoT ecosystem secure, all entities need to be secure.

Figure 1



Most cybersecurity frameworks assume a single network, owned by a single entity. One might think that as long as the infrastructure is secure, all is well. However, as we can see in figure 2, devices and platforms belong to different networks and entities, and several IIoT standalone systems are interconnected. In a traditional cloud setting, access is granted to a specific person for a specific program. On the other hand, in the IIoT architecture, one person exercises control over thousands of things. This makes it possible to infect the entire IIoT system by initially compromising a single entity in any one system. For example, the IIoT server is a single point of failure, and thus, would be an ideal point of attack to cripple the entire system.

Figure 2

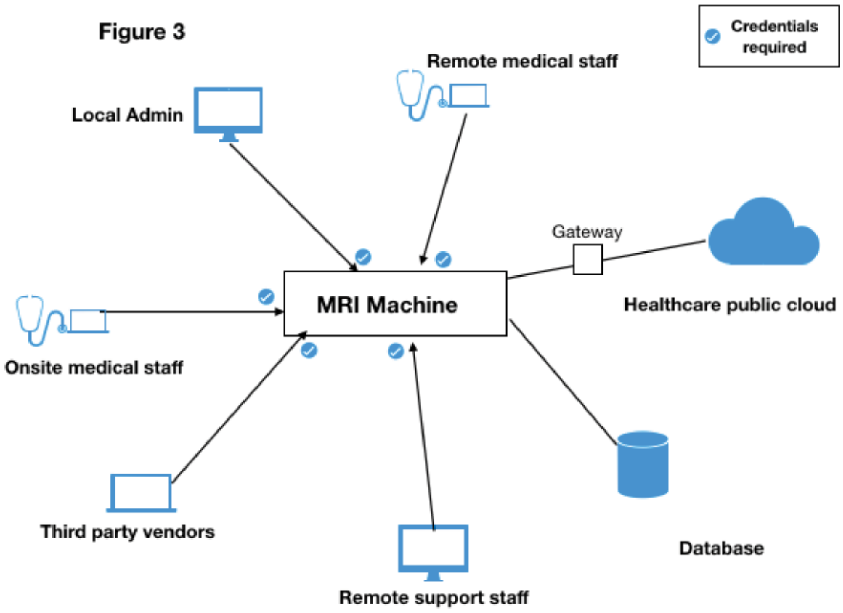


IV. IIOT SYSTEMS

Understanding IIoT systems is critical to mitigating their security risks. The Triton cyber-attack on a Saudi Arabian chemical plant could have resulted in significant loss of life through an explosion. Fortunately, a bug in the malware saved the day, and the equipment shut down instead. This particular cyberattack involved a privilege escalation vulnerability in the firmware that controlled the safety system. Hackers simply reverse-engineered the firmware to exploit this issue.

The expanded use of IIoT in hospitals raises both serious privacy and security issues. And, in healthcare, security vulnerabilities can also have life-threatening implications. Figure 3 below shows an MRI machine connected to its various users.

Figure 3



As shown in the figure above, several users have access to the machine – ranging from the onsite and offsite medical staff, third-party vendors, and local admins, to the remote support staff. A compromise of any one of the users' credentials could shut down operations, potentially jeopardizing a patient's health.

Frequently, weak passwords or built-in passwords provided by the device vendors are used in IoT and IIoT systems. Attackers can readily exploit these easy-to-crack credentials to gain access to the device. They can then control the device, install a backdoor to support their access to the networks, and leverage it to launch more advanced attacks, crippling the entire system.

V. IIOT CREDENTIALS

There are many different types of credentials in an IIoT system apart from the traditional server credentials. Any device and gateway would have credentials for users, local and remote administrative users, certificates, and integration keys. Referring again to figure 3, for the device to connect to other systems in the hospital, it would require a system key for verification. Since IIoT systems are largescale deployments involving services from different providers, they require multiple credentials over separate networks, devices, and applications. Managing the credentials can be a laborious task.

Default usernames and passwords are a persistent problem in IT. To simplify development, deployment, and configuration, many manufacturers use default encryption keys or passwords that are shared across the ecosystem and are unchanged for prolonged periods of time. Using defaults reduces the complexity significantly, but unfortunately, it also means that the attacker will have obtained the secret across the infrastructure from a single deployment. The problem can be compounded if there is no way to change the credentials after they've been compromised.

Compromising an end user's identity and credentials is the easiest way for a cyber-attacker to gain access to devices. The Mirai botnet attack did exactly that. The botnet code is a self-propagating botnet virus that targeted products from IIoT vendors that used weak default passwords, some even hardcoded within the devices. Mirai infected poorly protected Internet devices and launched a massive DDoS attack that blocked access to popular websites and applications.

As a business that uses IIoT products, managing system credentials is imperative. Credential generation, storage, transmission, replacement, and removal should be thoroughly performed to limit the risk of compromise.

VI. RECOMMENDATIONS

To better secure IIoT environments, organizations should focus on six (6) core disciplines, explained below.

1. Better secrets management

Passwords and usernames should never be shared and should be changed on a regular basis. Additionally, secrets should be stored and transferred in an encrypted manner. Ideally, devices should not come with default usernames and passwords and should require users to establish unique, strong credentials during installation.

2. Use Privileged Access Management (PAM)

Privileged credentials for users, processes, applications, and wherever else they exist within devices,

must be routinely monitored and managed. You should audit all the accounts being used and regularly review the access level they require. Implementing multiple factors of authentication could also help provide a greater level of authorization. Ensuring a robust password recovery mechanism would also make it difficult for attackers to compromise the devices or accounts.

3. Keep your devices updated

Devices need to be assessed regularly to determine the level of access they should have, to keep them fully patched and up to date, and to protect data end-to-end. An automatic update service would simplify this process, but in implementing this capability, ensure that the update files are encrypted, signed, and verified before they are uploaded and applied.

4. Use encrypted communications

It is crucial for IIoT devices to maintain integrity and confidentiality. Long-haul communications are easy to encrypt by simply using SSL/TLS encrypted connection. For short-haul communications, it is important to pick an appropriate protocol and use a diversified key. If that is not possible, use encryption for the entire network to help achieve secure and encrypted communications.

5. Segment networks

IIoT devices are often some of the least secure devices you could have attached to your home/office network. Having separate networks for questionable IIoT devices – like a guest network to segregate IIoT devices from other computers on your network – would help contain any potential damage. Then, if any device is hacked, at worst, it will be able to affect only the other IIoT devices in the network and not the important devices like your desktop computer or backup server.

6. Exercise caution while bootstrapping trust in devices

While bootstrapping trust in a device is time and cost-effective, it is a security hazard. If a hacker manages to extract the key from a particular device, he would be able to use that key to decrypt the secrets of other devices. So rather than hard-coding a secret in a mobile application, allow the application to generate a secret when it is first run. It would also be helpful if the device generated its own certificate when first provisioned and pinned a server-side certificate. Ensure that the secret is stored securely by using the native OS functionality.

MOVING TOWARD HOLISTIC IIOT SECURITY

Despite the growing threat associated with the Industrial Internet of Things, a majority of organizations have adopted or are planning to adopt IIoT. As IIoT transforms previously isolated systems to a connected network that is intertwined with our day-to-day lives and businesses, it creates new, critical dependencies on the robust functionality of that infrastructure. Getting IIoT security right depends on the manufacturer, operator, and the end customer working together. Security cannot be fully implemented by the device manufacturer or just by installing a security-based software program. Successful IIoT security requires a combination of technologies, frameworks, and processes adopted by all of the constituents of the IIoT solution.

APPENDIX: UTILIZING BEYONDTRUST'S PRIVILEGED ACCESS MANAGEMENT PLATFORM TO ENFORCE IIOT SECURITY

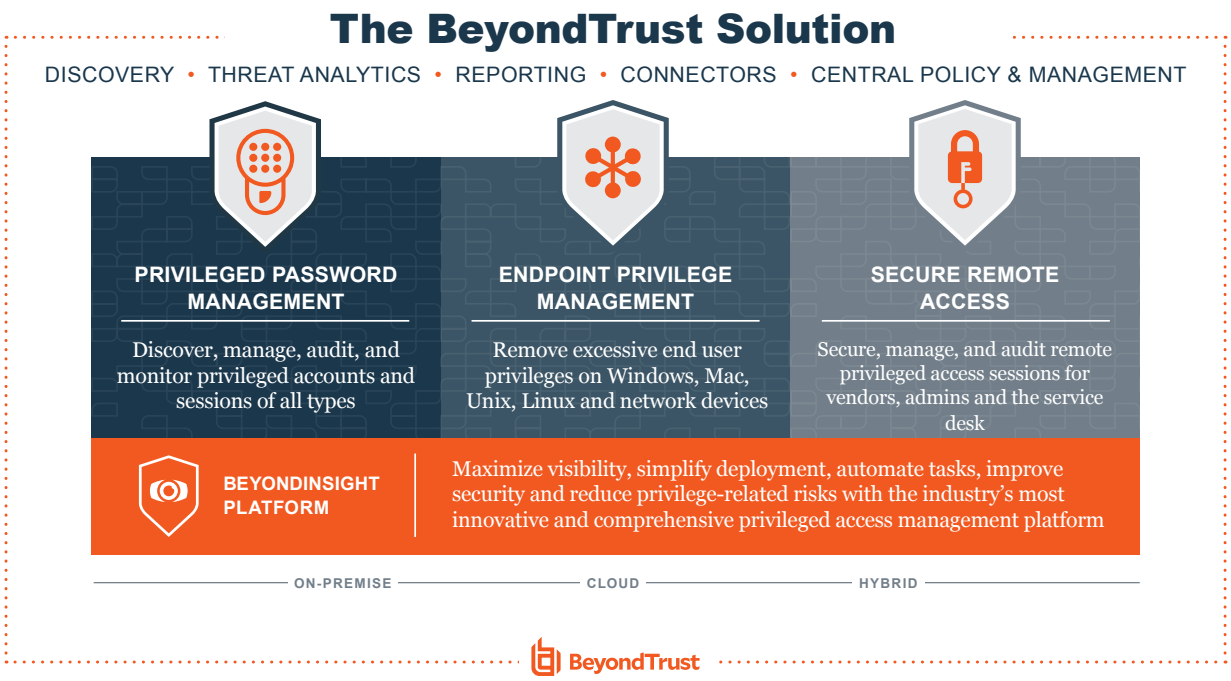
The BeyondTrust solution for secure IIoT discovers all IIoT devices in the environment, groups IIoT assets for consistent privilege management, and scans for security vulnerabilities and privilege-related risks. By delivering a single platform that unifies policy, management, reporting, and analytics across all devices and endpoints, organizations can meet stringent security and compliance controls, while achieving business goals. The figure on page 14 depicts an eight-step best-practices approach for securing IIoT devices.

TABLE 1: HOW BEYONDTRUST'S SOLUTIONS MAP TO SECURE IIOT BEST PRACTICES

Secure IIoT Best Practice	How BeyondTrust Solutions Help
1. Scan for Vulnerabilities	Network Security Scanner provides continuous vulnerability assessment and remediation guidance of the infrastructure across physical, virtual, and cloud environments.
2. Scan for Configuration Compliance	Network Security Scanner performs continuous configuration and baseline scanning against industry configuration guidelines and best practices from NIST, STIGS, USGCB, CIS, and Microsoft, across physical, virtual, and cloud-deployed assets and devices.
3. Gain Accountability Over Shared Accounts	Password Safe controls and audits access to shared accounts and improves accountability by ensuring that all credentials are properly managed and rotated across the environment, and that all audited activity is associated with a unique identity.
4. Eliminate Hard-Coded Passwords	Password Safe controls access to scripts, files, code, embedded application credentials, and hardcoded passwords, including removing hardcoded passwords in IIoT devices. Here, Password Safe reduces risk by closing backdoors to critical systems.
5. Enforce Appropriate Credential Usage	Password Safe eliminates administrator privileges on end-user machines, securely stores privileged account credentials, requires a simple workflow process for credential check-out, and monitors privileged sessions. This reduces risk by limiting lateral movement in the case of a compromise and by providing a secure audit trail for forensic purposes.
6. Segment Networks	Password Safe utilizes a secured jump server with multi-factor authentication, adaptive access authorization, and session-monitoring for access that needs to cross trust zones. This enables IT teams to segment access based on the context of the user, role, application, and data being requested, and reduces risk by minimizing the "line of sight" access that attackers have into internal systems.
7. Restrict Privileges	Endpoint Privilege Management solutions can grant only required permissions to appropriately access devices, restrict the commands that can be run on those devices, and provide a full audit trail of user activity for forensic purposes.

BEYONDTRUST'S PRIVILEGED ACCESS MANAGEMENT PLATFORM

BeyondTrust's integrated PAM solutions help to secure IIoT to provide control and visibility over all privileged accounts and users. By uniting best-of-breed capabilities across on-premise, virtual, and cloud platforms that many alternative providers offer as disjointed tools, the Privilege Management platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks.



To learn more about BeyondTrust solutions for securing IIoT devices, visit beyondtrust.com.

ABOUT ROB BLACK

Rob Black, CISSP, is the "IoT Security Guy." He is the Founder and Managing Principal of Fractional CISO. Besides IoT and cybersecurity, Rob has extensive web services and cloud solutions experience. He has held product and corporate security leadership positions at PTC ThingWorx, Axeda and RSA Security. Rob received his MBA from the Kellogg School of Management at Northwestern University. He holds two Bachelor of Science degrees from Washington University in St. Louis. One is in Computer Science and the other is System Science and Engineering. He is also a Certified Information Systems Security Professional

(CISSP). Rob is the inventor of three security patents. He speaks at conferences and blogs about IoT security.

You can follow him on Twitter @IoTSecurityGuy.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 78 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.