ivanti

Zero Trust Starts with Ivanti UEM

Table of Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit ivanti.com

Introduction

Today's enterprises are broad and increasingly complex, with many vulnerabilities and pitfalls. This is amplified by frequent mergers and the rapid increase in remote workforces and mobile user bases. Keeping your company secure can feel like a daunting, never-ending task when relying on legacy methods of perimeter-based network security for your users. That's why so many companies are moving toward the Zero Trust (ZT) model to secure their users, endpoints, sensitive data and corporate networks. Ivanti Unified Endpoint Management (UEM) provides a foundation that enables, simplifies and secures users anywhere they connect to your enterprise.

Zero trust is a security framework that assumes bad actors are always on your network. Always-on monitoring and adaptive enforcement deliver continuous protection at the user, device, app, network and data levels.

With threats growing in volume and sophistication, zero trust is the right solution for the Everywhere Workplace. By continuously verifying device and compliance and providing least-privileged access, you can reduce your organization's attack surface and likelihood of data breaches. Plus, zero trust mitigates threats while providing a consistent and more productive security experience for users, wherever they are.

Ivanti's pillars for Zero Trust:

- Verify users
- Manage devices
- Secure workloads and applications
- Protect your network
- Protect your data
- Deliver ongoing visibility and automation for scale

With Ivanti UEM as a foundation for your zero-trust architecture, all our features are built into a single agent. There is no need to install multiple applications, reducing the use of additional resources on the endpoint and accelerating deployment thanks to just one unified agent.

Verify users

Even with best intentions, users continue to be the weakest link, and phishing attacks are more prevalent than ever. Secure your users with strong authentication solutions like multifactor authentication, secure passwordless access, biometrics and privileged access management.

Ivanti UEM integrates with your in-house user directory services to identify and validate users on devices and resources. In addition, UEM can integrate with SaaS directory services like Azure Active Directory. With this integration, UEM policies can set authentication rules based on the user accessing

your company-deployed application, limiting what applications and corresponding data users can access on your enterprise.

In addition, UEM integrates with Ivanti's ZSO to end the pain of passwords by using a combination of mobile devices, biometrics and Fast IDentity Online 2 (FIDO2) keys for multifactor authentication (MFA). Humans can too easily be hacked; the use of the password has become an outdated method of security access control.

Manage devices

Zero trust requires verifying trusted users, trusted devices, trusted apps and trusted networks. This demands a robust endpoint manager that has the breadth for overall policies and is also granular enough to apply to specific users and devices.

Managing endpoints can be a daunting task, especially with the variety of devices available to users, including Android, iOS, IoT, macOS and Windows. With the assortment of devices and their varied use in your enterprise, having a unified management interface increase IT productivity, reducing the need and cost of having to manage different types of endpoints and devices. A UEM unified interface provides simplified policy templates while still delivering granularity for modifying policy at the user and device level.

Managing the device is only half the equation to enhance user productivity. Another big element is managing the experience on that device. This demands simplified desktop configurations, improved logon times, and an optimized user experience. Ivanti's UEM Environment Manager Policy replaces the slow and complex logon scripts and group policy objects to deliver fast logon times for users with minimal effort from IT.

Within UEM, a custom-tiered compliance policy can be enforced. This entails setting a time limit for the user to update an application or operating system using time-based push notifications, blocking: a) access to work resources; b) removal of applications; and/or c) work network resources including VPN connection settings. This policy can include a final action of wiping all UEM-provisioned corporate management settings, plus applications with corresponding application data, and finally retiring the device from UEM.

Secure workloads and applications

Whether your workloads are in the cloud or on-premises, a zero-trust approach can support secure development practices, least privileged access, secure app-to-app communication and container security.

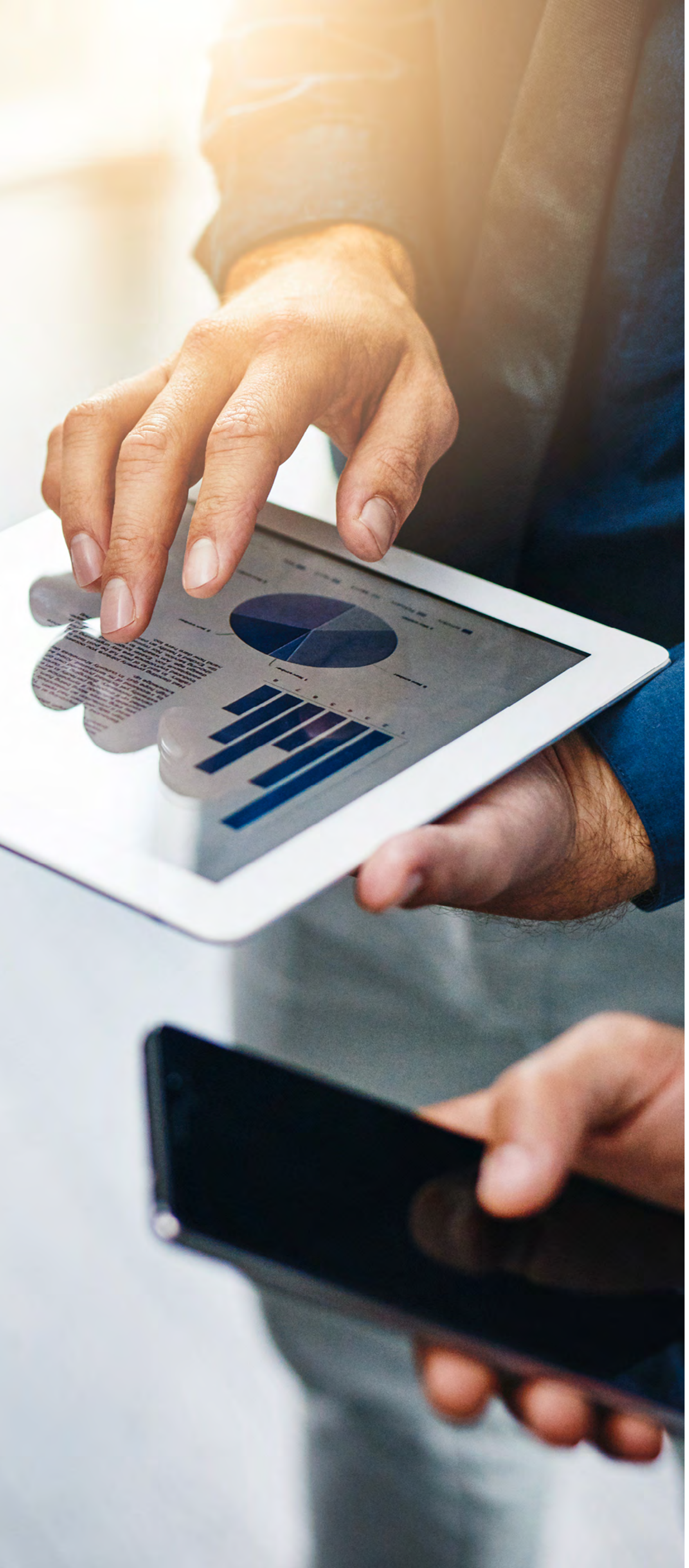
With Ivanti UEM, policies can be created to secure applications on devices. UEM policies can control third-party applications using the device's operating system store. UEM also provides protection for data at rest, data in use and data in motion. For data at rest, you can configure the application data for an additional layer of encryption. Based on policy, if the device becomes compromised or does not meet specified security-device policy requirements, the data can be automatically wiped from the device. Policies can also be established where if the device has not synced with UEM for a certain time period, the data would be automatically wiped. With data in use, data loss protection (DLP) policies can be implemented to prevent copying and pasting between the specified applications. For data in motion, applications can be given a separate, secure tunnel.

Ivanti Docs@Work creates a secure content environment on-device for the end user to access and manage corporate documents and data. End users can securely view and store files on the device, which can also be selectively wiped if the device is ever lost or falls out of compliance.

Protect your network

Context is key for zero trust network access. Organizations must go beyond traditional VPNs and design micro-segmented networks that can make intelligent access-control decisions based on user attributes, device posture and application type.

Ivanti Sentry can protect your on-premises intranet applications and Ivanti Tunnel can protect your third-party Software as a Service (SaaS) external internet-based applications.



Ivanti Sentry is an intelligent security gateway that creates a secure VPN tunnel from your device to your on-premises enterprise applications. With UEM policies, you can specify users and/or devices that will provide secure, encrypted tunnel access to your on-premises applications. You can also prevent non-compliant, jailbroken, rooted or other compromised devices from connecting to your internal intranet.

Your IT administrators can easily configure Ivanti Tunnel to provide an identity certificate on a per-application basis. This ensures business apps are protected while personal apps are not, so personal app data will not be viewable by your IT. This keeps private, personal user data protected while also securing business data.

Defend your data

We know how hard it is to achieve data mapping, classification and loss prevention at scale in the modern work environment. Still, data hygiene is critical for continuity, compliance and privacy.

Ivanti UEM provides protection for data at rest, data in use and data in motion. UEM policies can wipe data off devices if contact time reaches their policy limit while providing a secure workspace on devices. DLP policies can be applied on an app-per-app basis, preventing users from copying and pasting data. And application traffic can be encrypted based on your app policies.

In addition, third-party application controls allow you to validate applications before deploying to your user base.

Ongoing visibility and automation for scale

You can't secure what you can't see. Stay in the know with robust reporting across all your IT infrastructure — and react seamlessly with automated threat response. This is the only way to scale your IT teams to meet the challenge of securing the Everywhere Workplace.

Ivanti UEM Data Analytics provides discovery on detailed asset data, extending data using connectors for vendors' warranty information, and normalizing data for better data consistency and reporting. This increases visibility into the health of your endpoints and devices, while reducing loss of productivity due to hardware issues.

UEM provides robust and granular reporting, plus notifications when users violate your security policies. While UEM can integrate with third-party SIEMs for logging, UEM can also integrate with Ivanti Neurons for UEM and Mobile Threat Protection (MTP) to automate with patching, device quarantine and application vulnerabilities, including zero-day threats.

UEM increases IT productivity by helping gather detailed device data, automating software and OS deployments and personalizing workspaces while quickly fixing user issues. Our endpoint manager manages multiple devices — physical and virtual — including Windows, MacOS, Linux, iOS, Android, Apple TV, Raspberry Pi and other IoT devices.

Features to Mature your Zero Trust Architecture

As with any security architecture, there are additional features you can implement to help monitor and protect your users. Ivanti's Zero Sign-On removes the use of passwords and relies on biometrics, mobile ID and FIDO2 keys to reduce the need to have users memorize a new password for your MFA. Mobile devices are now more heavily targeted for phishing and malicious software. Therefore, Ivanti's Mobile Threat Defense enables your enterprise to monitor, manage and secure devices against attacks that occur at the device, network and application level, as well as preventing mobile phishing attacks. Ivanti Neurons fuels your IT with real-time intelligence you can act on, enables devices to self-heal and self-secure, and provides users with a personalized self-service experience. Enabling these features with automated self-healing and self-services will reduce user downtime and TCO.

Conclusion

The Everywhere Workplace is here — and with it, a necessary shift to a zero-trust security framework. The decentralized workforce has created opportunity, while exposing and amplifying significant threats. These threats include user error and unintentional disclosure stemming from an increasingly muddied delineation between corporate and personal devices. Another threat is a rapid rise in ransomware and phishing from bad actors capitalizing on an abrupt shift to a perimeterless landscape.

To thrive in — not just survive — the permanent shift to the Everywhere Workplace, businesses must act quickly to adopt strategies designed to identify and secure all users, devices, applications and data. A powerful Unified Endpoint Management capability is an essential component of this effort. At Ivanti, UEM blends seamlessly with other elements including Mobile Threat Defense and Zero Sign-On to create a zero-trust framework that is perfectly tuned into today's threats — and perfectly positioned to handle what comes next. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Zero Trust Architecture
https://csrc.nist.gov/publications/detail/sp/800-207/final
2. Ivanti Unified Endpoint Management:
Everything You Need to Know
https://www.ivanti.com/blog/ivanti-unified-endpoint-management
3. Delight your users with a personalized,
secure work experience—everywhere
https://www.ivanti.com/solutions/unified-endpoint-management
4. Humans Can be Hacked.
So Stop Using Passwords, Already!
https://www.ivanti.ru/en-us/blog/humans-can-be-hacked-so-stop-using-passwords-already
5. Ivanti Device and Application Control 5.2
Is Now Available
https://www.ivanti.com/blog/ivanti-device-application-control-5-2