
ivanti
Stronger Security Through UEM
4 real-world reasons why your endpoint security needs Unified Endpoint Management

Inside you'll learn how your UEM solution helps your Security team:

01 Incentivize good security behaviors

02 Secure a growing hybrid work environment

03 Automatically enforce policies

04 Easily integrate with patching or mobile threat defense solutions

This eBook is part of The Ultimate Guide to Unified Endpoint Management.

ivanti

Introduction

In the Ultimate Guide to UEM we frequently reference both the IT and Security teams – and that's no accident.

Third-party analysts believe that – considering post-pandemic Everywhere Work embracing more remote and hybrid approaches, rather than solely on-premises offices – UEM solutions will shift to incorporate more endpoint security use cases for "proactive and resilient defenses" against modern threat actors. (Cipolla, Wilson and Silva)

It's no surprise, then, that endpoint security remains a top cybersecurity investment priority for organizations worldwide – topped only by cloud security tools and internal user training. (PwC)

(And, if the proposed UEM solution could help secure cloud apps, then that would be a bonus for everyone involved!)

UEM solutions offer a unique starting point for both IT and Security teams to work from the same set of baseline information – their organization's devices, user profiles and network activities – to properly manage, secure and service all endpoints.

1. **Investing in a DEX-focused technology stack** to incentivize good security behaviors from end users.

2. **Securing an organization's rapidly expanding attack surface** means Security teams must address a wider variety of threat vectors from ever before, from IoT devices to unknown Internet connections.

3. **Enforced security policies and monitored user, device and app behavior** can prevent lateral movements in the organization's network from a compromised endpoint, and signal initial intrusions or potential insider threats before damage is done.

4. **Security tools such as patch management or mobile threat defense solutions** easily integrate with modern UEM solutions, providing a simple and speedy method for Security teams to remediate prioritized risks without interfering with regular user – or IT admin – operations.

However, while UEM's device onboarding automations and policy controls offer some basic cyber hygiene protections – and their device and user activity logs offer robust monitoring that can be enthusiastically used by the Security teams – most platforms will require additional controls and tools to reach their complete potential as an organization's single point of truth for all endpoint security. (Verizon)

1 Security's stake in UEM starts with DEX.

More than almost any other department outside of IT itself, Security teams will support investments for a more proactive DEX technology – including UEM solutions, especially as the risks of shadow IT and ever-expanding endpoint attack surfaces keep increasing in a post-pandemic, hybrid workplace.

- CIOs cite shadow IT solutions or products as a top concern for continuity of governments around the world. (NASCIO)
- 12.8% of 2022 cloud-based cyberattacks involved shadow IT. (Shackleford)
- Only 52% of surveyed security professionals report a "high" degree of asset visibility at their organization – and 10% said they don't use any sort of asset discovery tool at all. (Ivanti)

And hackers are already taking advantage of this gap between what the Security team knows they can protect – and what users have done to make their working days easier.

12.8% **of all cloud-based cyberattacks in 2022 involved shadow IT.**

Real-World Repercussions

When Bad DEX Almost Let Hackers Blow Up a Petrochemical Plant

In 2017, threat actors hacked into Saudi Arabian petrochemical plant Triconex. The security team only realized their systems had been breached when six controllers malfunctioned, triggering an alarm.

Incident responders quickly discovered that someone had remotely accessed the systems to insert malware – but that seemed impossible!

After all, the plant's security systems had been designed to foil remote attacks by requiring an employee to insert a physical key at the plant's console to make any configuration changes.

However, the plant's physical layout separated the controller from the control room, requiring operators to walk back and forth from one space to another to implement changes. An employee had kept their physical key in the controller's console to allow for them – and the hackers – to remotely access the code for updates.

Had other redundant security systems not alerted plant employees to the critical failures triggered by the hacker's activities, Triconex's compromised controllers could have turned off all safety systems and killed plant employees, either through chemical leaks or outright explosions.

This cyberattack could have been one of the first hacks resulting in a known human fatality – all because of one tired employee and the security designer's failure to consider human behavior while creating "foolproof" security systems. (Rhysider)

2

Secure more diverse working environments and IoT endpoints via UEM clients.

Remote work conjures images of employees working in a coffee shop, headphones plugged in, blissfully unaware of the fellow “customer” waiting for them to visit the restroom so proprietary files can be downloaded and their unlocked laptop exploited.

While human error will always remain in some capacity, endpoint security solutions and policies – enforced by the IT team’s UEM platform – will help to remediate some of the risks invited by a more geographically diverse workplace.

Let’s discuss two of the more common risks for endpoint security: the proliferation of the Internet of Things (IoT) and man-in-the-middle attacks in public network settings.

(Spoiler alert: both scenarios can be remediated through proper asset discovery, network segmentation and device monitoring – all of which can be executed through UEM solutions with the proper security-focused configurations and supporting features.)

Real-World Repercussions

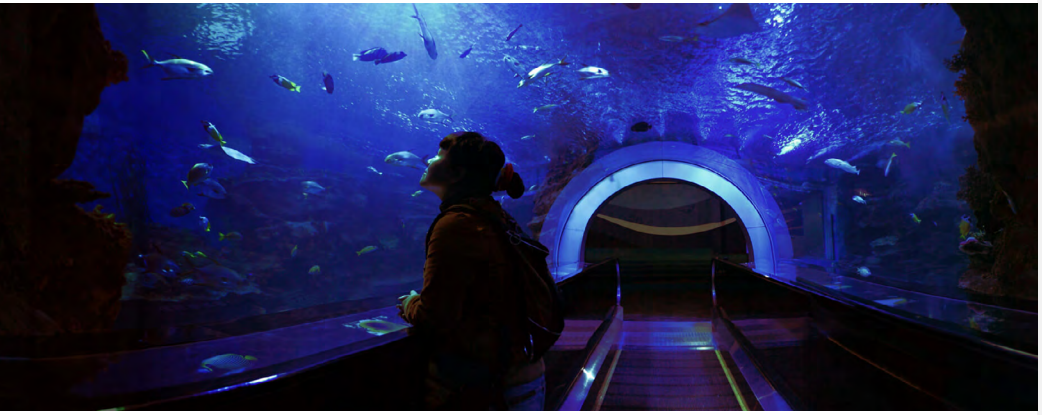
Unexpected Internet of Things (IoT) Attacks

IoT attacks made up more than 12% of all global malware attacks in 2021 – up from less than 1% of all malware attacks in 2019. (IBM Security)

Yet, 47% of surveyed IT professionals reported that their organization had no IoT compliance policy. (SAM)

IoT-enabled devices in both corporate and remote workplaces can be remediated through relatively simply network segmentation and active scanning capabilities.

However, many of these devices are ones that organizations and end users alike wouldn't necessarily consider in their risk analysis until it's too late – as these organizations discovered.



Fish tank thermometers

One North American casino discovered what havoc unmanaged IoT could wreak on their operations, as hackers exploited a vulnerability in their casino lobby's fish tank thermometer. Since this IOT-enabled tank was improperly segmented on the casino's network, the hackers could move laterally into the casino's cloud infrastructure and continue their attack. (Wei)

Medical devices

The WannaCry ransomware attack in 2017 prompted manufacturers and government agencies to reconsider vulnerabilities of internet-connected medical devices – including insulin pumps and pacemakers. (Chase, Coley and Connolly)

Vehicles

2015: Hackers hijacked a Jeep Cherokee, shutting down its engine mid-drive on the highway. (Greenburg)

2023: A Tesla driver discovered that the official Tesla mobile app allowed them to enter – and drive – a vehicle they did not own. (Day)

Post-2023: Government officials warn that "there is currently no comprehensive [...] cybersecurity approach" for either electric vehicles or their chargers (SANDIA) – vehicles which organizations' employees will drive to offices or offsite meetings, and to which they'll Bluetooth-connect their corporate devices.

3

Enforced security policies and device records prevent hackers from gaining a foothold in organization networks.

Proactive cybersecurity strategies not only try to stop hackers from breaking into organization networks, but also account for what happens if bad actors manage to enter.

Take the humble USB drive. A mainstay of salespeople everywhere, it can hold large files such as presentations, videos and music to use in new computers without having to wait for a network connection to upload or download material.

Of course, if USB drives can carry large files for legitimate purposes, then they can also carry malware, too.

UEM solutions can automatically deploy and enforce removable media policies by default. Through such policies, your organization's end users must request special permission to use memory-carrying devices with their company-owned machines, rather than leaving every device and endpoint automatically exposed to these attacks.

Real-World Repercussions

Stuxnet: The World's Most Famous USB Drive Malware

Stuxnet is the name given to a computer virus allegedly crafted by certain intelligence agencies to bring down Iran's nuclear enrichment program.

The facility operated under the tightest security – which meant that it was air-gapped from any Internet or outside network access. The only way malware could make it inside the facility was if an already trusted insider personally plugged it into a computer on the facility's network.

So, the attackers made a computer virus that only attacked the industrial control systems the Iranian facility used for the centrifuges and loaded up the entire malware package on USB drives.

The tainted drives were distributed throughout the region for the nuclear scientists to find – perhaps at conferences, perhaps just handed out by trusted colleagues in the region.

Eventually, a scientist made the fatal mistake and plugged in a USB drive laced with the Stuxnet malware… and the program lost an estimated 1,000 centrifuges and wasted material, helping to pressure Iranian leadership into signing the 2015 Iranian Nuclear Deal.

To learn more about Stuxnet, check out these resources:

- "Ep 29: Stuxnet" by Jack Rhysider
- "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" by Kim Zetter

The device and user logs that a UEM platform records can be used for security purposes, too.

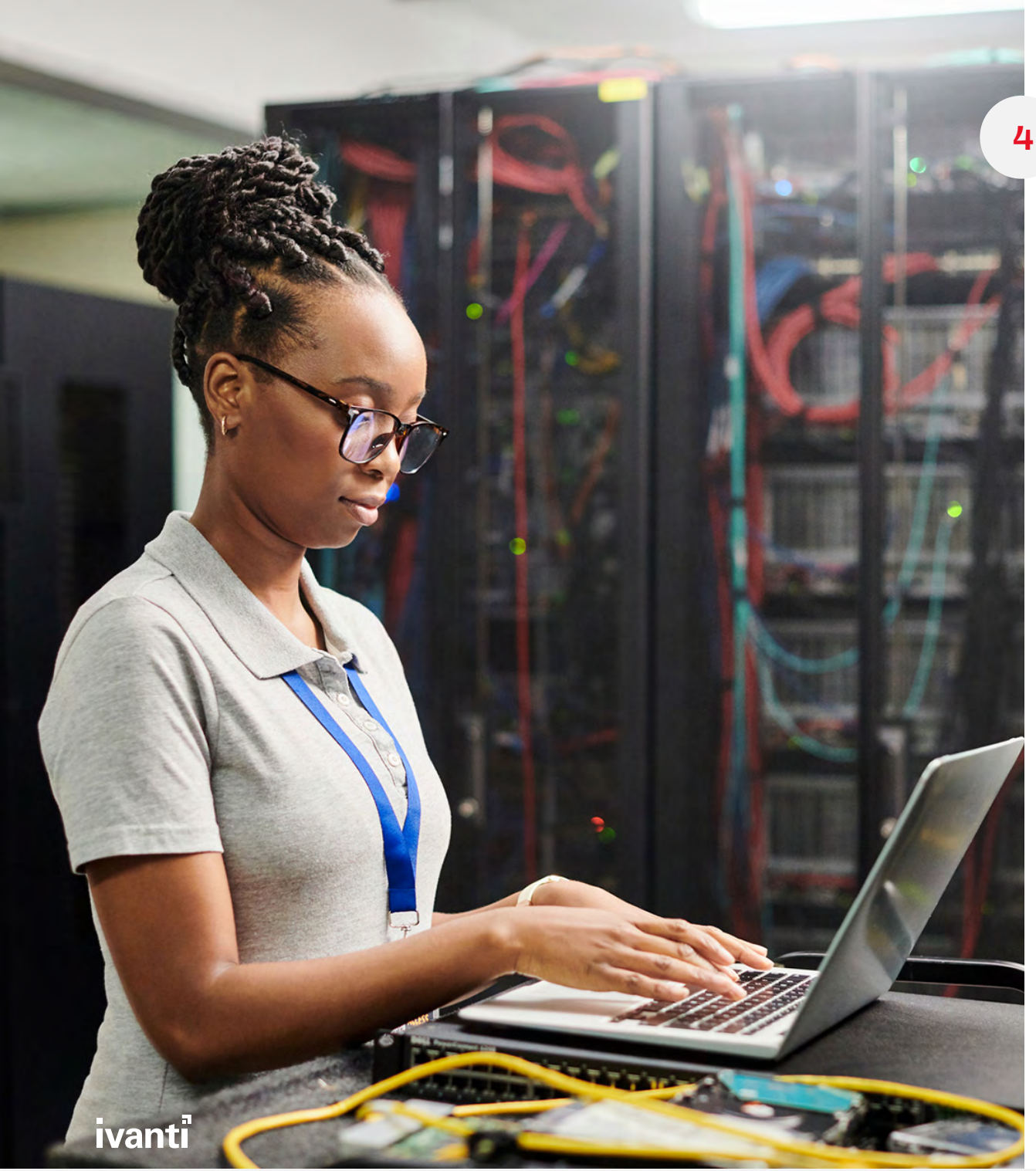
If the organization has reason to believe an employee may present an insider threat, then the Security teams can check a device's records for signs that sysadmin-level tools such as PowerShell were illegally installed and used on a user's device.

Or, perhaps an organization's system alerts to an ordinary "user's" activity, which shows the user suddenly performing advanced networking techniques on their organization's managed device.

Such activities may be a sign that it's not actually the authorized user at all, but rather a hacker hiding behind that user's authentic (but compromised) credentials, attempting to escalate privileges within the corporate network.

With the right configurations, alerts and security tools, these activities could be detected on an endpoint or mobile device long before the hacker ever moved laterally in the organization's network or gained admin-level permissions.

And – as rising cyberinsurance rates place new pressure on already strained organization finances – both IT and Security teams may find it quite economical to enforce stricter removeable media policies and user activity alerts for both proactive risk remediation and lower insurance premiums. (Breg)



4

Easy integrations offer simple, one-and-done security implementations.

While a well-integrated UEM platform offers basic cyber hygiene opportunities, it cannot be the end-all of your endpoint security solutions.

However, UEM solutions offer a supremely well-positioned launch pad for other tools – such as patch management or mobile threat defense solutions. After all, the UEM itself has a client directly installed onto every owned and managed organization device.

It's basically a few clicks away for other security tools to be hooked into that same device via the UEM client, immediately augmenting your endpoint security defenses while not detracting from your organization's DEX or end user productivity.

UEM + Risk-Based Patch Management

For example, UEMs can be combined with risk-based patch and vulnerability management solutions for a seamlessly proactive risk response to remediate actively exploited vulnerabilities in your current environment.

1 **The Security team analyzes current threat intelligence data,** running currently exploited vulnerabilities against your organization's currently used devices and applications.

- The UEM's active scanning capabilities ensure no device or application is missed during this initial assessment!

2 **The Security team deprioritizes or expedites current unpatched vulnerabilities,** depending on your organization's risk environment and priorities. They may consider:

- Priority level of potentially impacted devices, users, OS and organization-critical functions.
- Whether a vulnerability has been actively exploited by known threat actors in the wild.
- What sort of access or permissions an exploit could grant a threat actor.
- How often potentially impacted devices or applications are used by the organization, either passively or actively.
- How difficult a patch will be to apply, or if other remediation will need to occur (quarantine, segmentation, etc.).

3 **The IT team receives a list of prioritized patches,** along with:

- Information on why these patches should be implemented, based on the organization's unique risk factors – which reassures the IT team that Security isn't asking them to just patch all possible vulnerabilities!
- Specific devices or users for patch rollout, per predetermined cadences.
- Known possible interferences with current software suites or workflows.

4 **The IT team automatically rolls out patches to identified devices and endpoints via the UEM platform,** scheduling updates for least possible impact to end user productivity and keeping an eye out for any odd activities indicating a patch has interfered with regular workflows.

For more on risk-based patching and remediation strategies, please consult *The Ultimate Guide to Risk-Based Patch Management.*

UEM + Mobile Threat Defense

Everyone is vulnerable to phishing – even the pros!

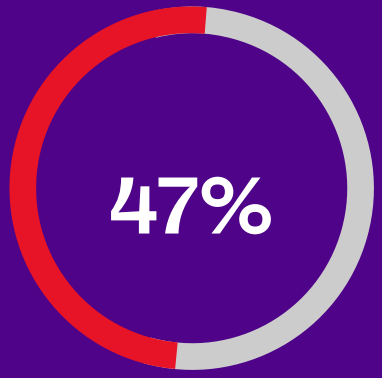
Phishing campaigns are a known entry point for ransomware gangs in particular, making up 54% of all ransomware delivery methods as of 2020. (Datto)

Specialized “whaling” phishing attacks – hacker-crafted email campaigns specifically targeting executive leaders in major corporations – resulted in American companies losing an estimated $2.4 billion USD in 2021. (Verizon)

New research has shown:

- 47% of IT professionals admit to falling for a phishing attack. (Ivanti)
- Only 43% of security professionals say their organizations have experienced a phishing attack in the last 24 months (Ivanti) – even as other industry reports find that 83% of organizations experienced a successful phishing attack in 2021 (Verizon).
- Over a third of senior leaders admit to clicking on a phishing link – which is four times the rate of other office employees. (Ivanti)

There’s a 40-point gap between how many phishing attacks Security teams believe their organizations experience – and how many phishing attacks occur.



of IT professionals have fallen victim to phishing attacks.

So, if:

- IT specialists fall for phishing emails
- Security specialists don't realize their organizations are receiving phishing attacks
- Senior executives are getting targeted at higher rates – and falling for those attacks at higher rates

… then security training and spam filters on organization inboxes aren't enough to stop users from compromising organizations' security through phishing campaigns.

While a UEM's configurations and settings may help limit the initial damage caused by a phishing link click – particularly if it's been paired with a patching solution, severely hampering hackers' ability to escalate their privileges or move in the network – it will not be nearly as effective if not paired with a specialized mobile threat defense (MTD) solution.

The best MTD solutions can run through an enrolled device's UEM client – either owned by the company or as part of a BYOD program – not interfering with any regular user activities or eating up any additional memory.

If the MTD solution detects:

- **An incoming phishing link:** the system immediately blocks the movement and ensure the action isn't completed by the user.
- **Potentially malicious activity:** the MTD and UEM solutions then automatically proceed with various levels of remediation, depending on the specific activity and potential threat level – up to and including removing user access to any organization applications, even on a personally owned device! – until the user has removed the app or otherwise fixed the issue.
- **An uninstalled OS update:** the system politely offers a push notification to the user, encouraging them to install the update. Increasingly levels of remediation are implemented if the user continues to not update their device — up to and including quarantine of any organization apps or access from the out-of-date device.

References

1. Breg, David. Quarterly Cyber Insurance Update. 10 February 2023. https://www.wsj.com/articles/quarterly-cyber-insurance-update-february-2023-62141c19.
2. Chase, Melissa, et al. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. 14 November 2022. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
3. Cipolla, Tom, et al. Magic Quadrant for Unified Endpoint Management Tools. 1 August 2022. https://www.gartner.com/doc/reprints?id=1-2AQEK9FU&ct=220802&st=sb.
4. Datto. Datto's Global State of the Channel Ransomware Report. November 2020. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.
5. Decime, Jerry. Settling the score: taking down the Equifax mobile application. n.d. https://www.linkedin.com/pulse/settling-score-taking-down-equifax-mobile-application-jerry-decime/.
6. Greenburg, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. 21 July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
7. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
8. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
9. —Khandelwal, Swati. Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw. 14 September 2017. https://thehackernews.com/2017/09/equifax-apache-struts.html.
10. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.
11. PwC. 2022 Global Digital Trust Insights. December 2021. https://www.pwc.se/sv/pdf-reports/cybersecurity/cyber-global-digital-trust-insights-2022.pdf.
12. Rhysider, Jack. Darknet Diaries, Episode 68: Triton. June 2020. https://darknetdiaries.com/transcript/68/.
13. SAM. IoT Security Landscape Report. July 2022. https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf.
14. SANDIA. Cybersecurity for Electric Vehicles Charging Infrastructure. July 2022. https://www.osti.gov/servlets/purl/1877784/.
15. Shackleford, Dave. SANS 2022 Cloud Security Survey. March 2022. https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security-survey.pdf.
16. Verizon. Mobile Security Index 2022. 2022 August 2. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf.
17. Wei, Wang. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. 16 April 2018. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.
18. Weissman, Cale Guthrie. Here's Why Equifax Yanked Its Apps From Apple And Google Last Week. 15 September 2017. https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week.

Explore more in the full Ultimate Guide to Unified Endpoint Management.

Access your Guide

ivanti

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