Persistent

WELCOME TO

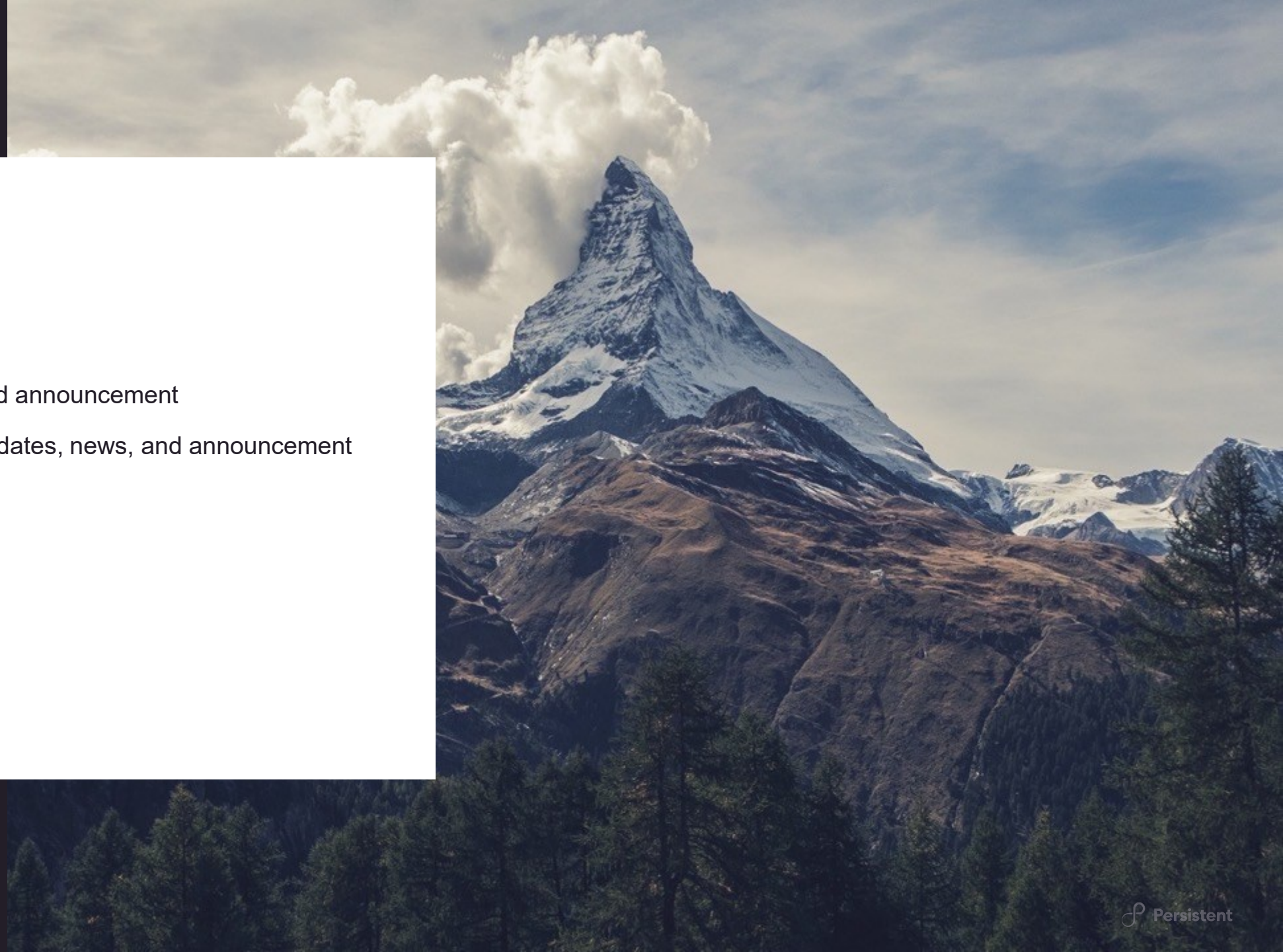
USER GROUP MEETING

Digital Device Management

2nd March 2022

Agenda

1. Open Discussion Forum
2. Product - updates, news, and announcement
3. User Group Community - updates, news, and announcement
4. Q&A/Feedback



Launching

We Connect User Group

100k+	2013	50+
Users	Since	Countries

- In-Person User Group Summits
- Product User Group Meeting every month
- Common User Group Meeting bi-yearly
- Webinars, Live Events, Panel discussions

Product UGM

Digital Device Management

Radia Endpoint Management
OTA, IoT Security

Cloud Orchestration Management

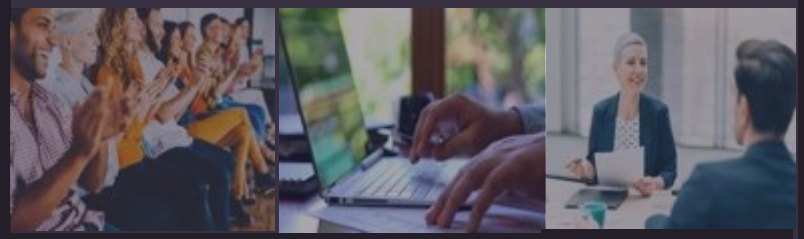
Rovius, MultiCloud, Disaster Recovery, Migration
Cyber Resilience

API Monetization Management

Aepona Marketplace

Bolstering Our Community

Boosting engagement, visibility and a sense of belonging



Experience **Contribute** **Grow**

Be the Champion *of* Community

INFLUENCE & EXPRESS

Community DNA

- Connect
- Learn
- Share
- Collaborate

Perks

STAY UP-TO-DATE	PARTICIPATE	OPEN FORUM
News	Innovate	Build
Market	Showcase	Network
Releases	New Ideas	Advocate
Early Access	Best Practices	Feedback

Persistent

Sentient Endpoint Manager (Radia) – Advanced Patch Manager

User Group Meeting – 02nd March 2022

- Anurag Kumar

86%

of reported vulnerabilities come from third-party applications.

(National Vulnerability Database)

84% of vulnerabilities had patches available on the day of disclosure.

National Vulnerability Database – Dashboard

NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	0	1	0
This Week	0	0	1	0
This Month	1860	1742	898	630
Last Month	2030	2240	800	517
This Year	3890	3982	1606	1147

CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	14245
HIGH	41141
MEDIUM	38099
LOW	1739

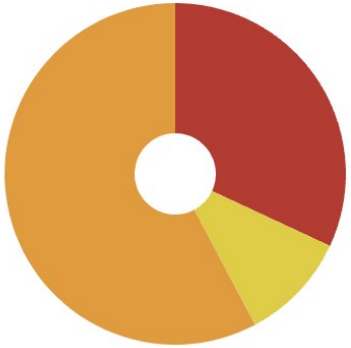
CVE Status Count

Total	181384
Received	58
Awaiting Analysis	321
Undergoing Analysis	1008
Modified	75358
Rejected	10578

NVD Contains

CVE Vulnerabilities	181384
Checklists	573
US-CERT Alerts	249
US-CERT Vuln Notes	4487
OVAL Queries	10286
CPE Names	845832

CVSS V2 Score Distribution



Severity	Number of Vulns
HIGH	54360
MEDIUM	98351
LOW	17536

Isn’t Patching a Solved Problem

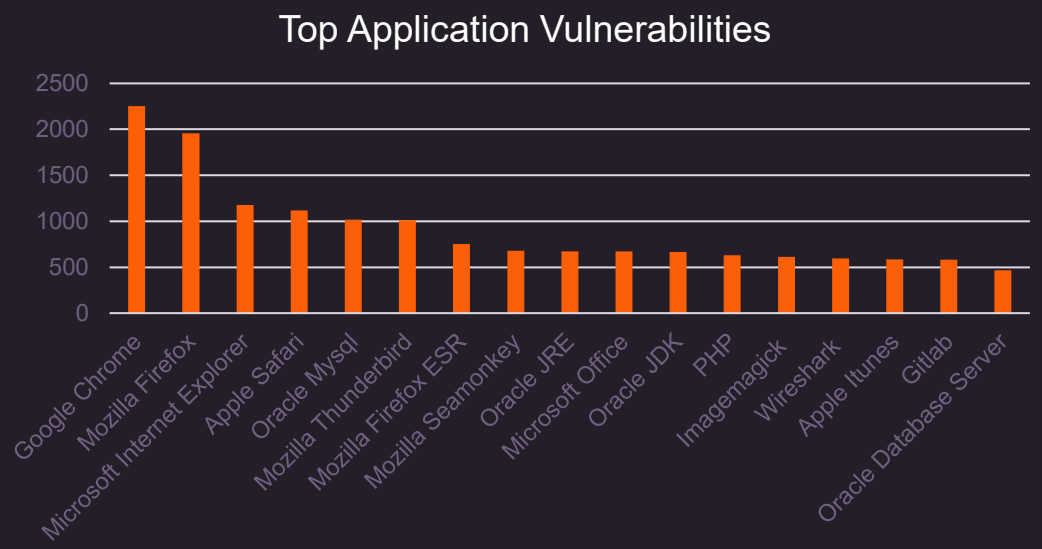
\ Although patching has been “a solved problem” for many years, even decades, a lot of organizations struggle with it today – and struggle mightily.

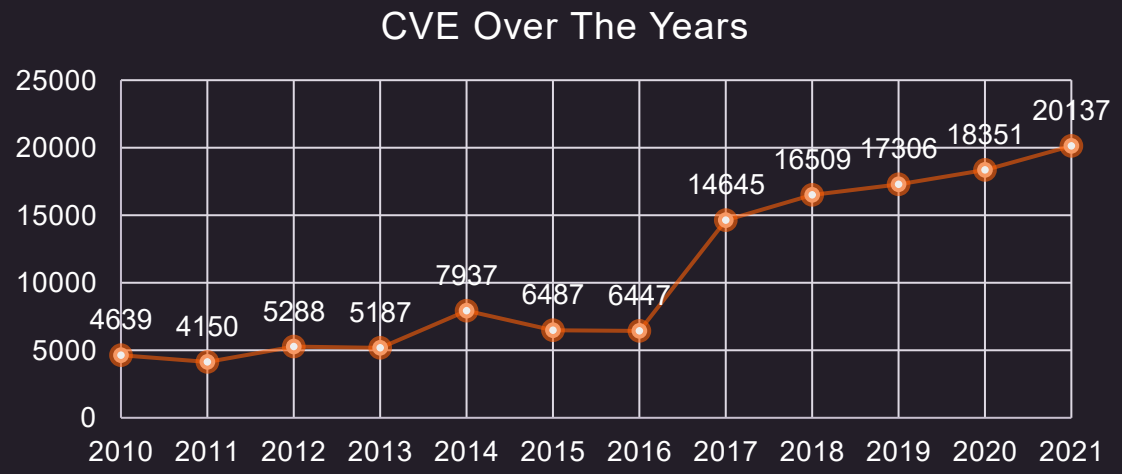
\ “While patching Windows OS (WSUS) on desktops monthly is indeed solved everywhere, but in the darkest woods of IT, patching 3rd party application on a desktop remains a significant challenge for many organizations…

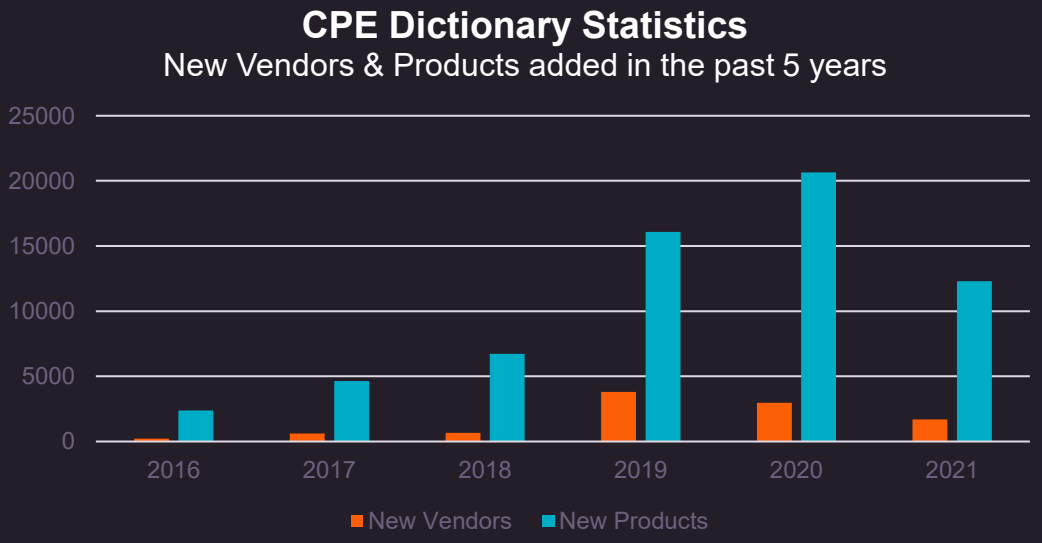
“… And then you have Java … … a security disaster in a league of its own.”

Persistent

Need for Application Patching







- Growing number of security vulnerabilities reported every year.
- Vulnerabilities on software and applications are susceptible to cyber-attacks
- 57% of cyberattack victims stated that applying a patch would have prevented the attack.
- Application patching is required to repair a vulnerability or flaw identified after an application or software is released.
- Application patching has become an important piece in reducing security risk.
- Compliance: Organizations are often mandated by regulatory bodies to maintain a certain level of compliance. Application Patching is necessary for adhering to these compliance standards.

Cannot afford to manually patch 3rd party applications

Difficult To Patch

- **3rd party patching is hard!**
- Every 3rd party application patch is a custom one-off that takes hours to research, setup, test and deploy
- Every 3rd party application has a different deploy mechanism

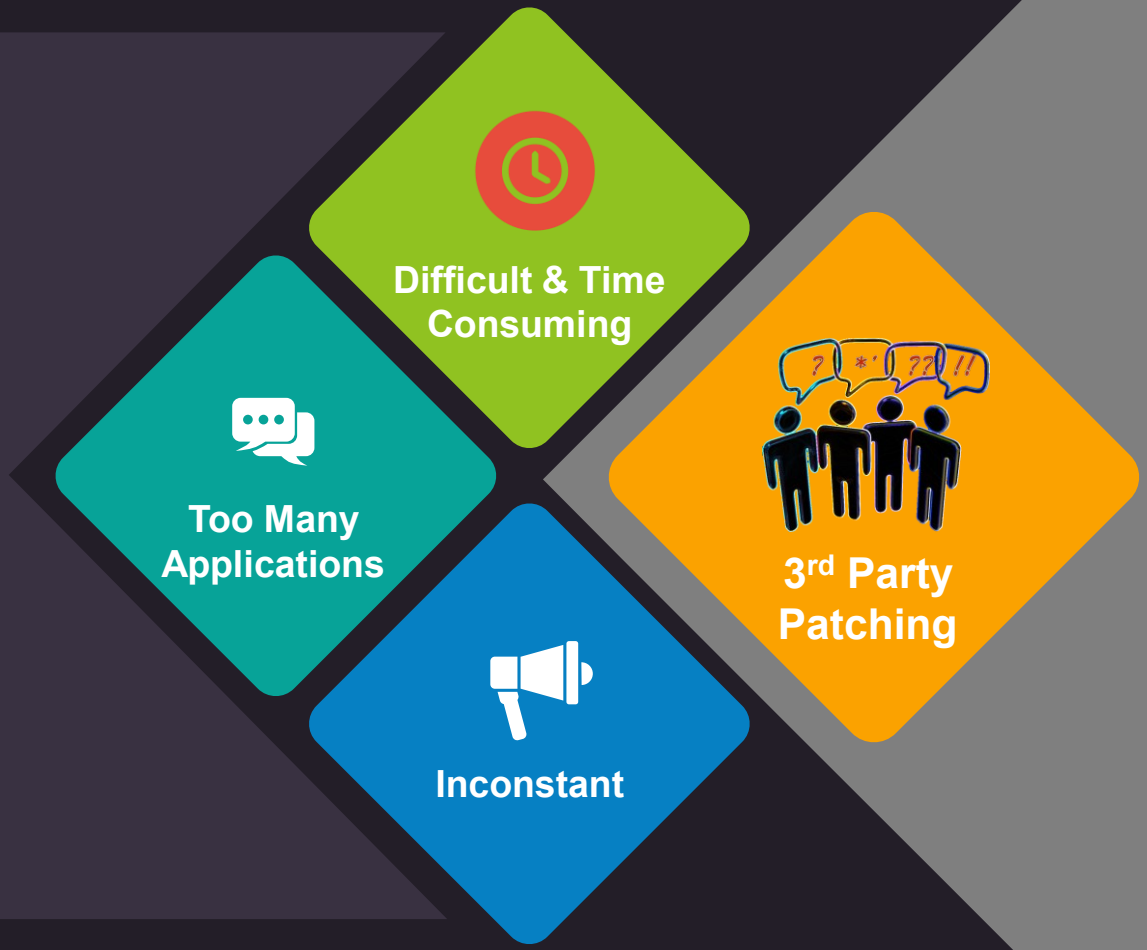
Too Many Applications

There are just too many things to keep up with!

- 3rd party patches out number MS patches
- Multiple vendors
- Multiple versions
- Multiple applications
- Multiple platforms

Inconstant Release Cycles

- Every 3rd party application has a different and not fixed release cycle



Radia Patch Manager Advance

- Extends the patch management capabilities beyond the OS patches
- Drill down reports with filters for audit and compliance purposes.
- Plugs-in into existing Radia deployments, using existing architecture – no new infrastructure investment, no new learning curve
- Existing policy engine
- Download patches and updates directly from OEM approved repositories.
- Decrease security risks and service performance degradation by controlling when and where patches are applied
- Prepare for audits and help demonstrate compliance with out-of-the-box reports and dashboard views
- Scalable and an easy-to-use interface with no scripting or professional services needed

- **Role Based Access Control**
- **Bandwidth throttling and Checkpoint restart capabilities**

- **Support for 100+ third party applications**
- **Support for variety of application types.**

Great Value from Patch Manager Advance

- Increase security to reduce downtime
- Reduce the application patching gap
- Patch hundreds of vulnerable applications
- Delete or re-publish updates
- Zero touch deployments – No need for end-user intervention
- Expand Sentient Configuration Manager to include application patching
- Easy integration into the Sentient console
- Leverage existing Sentient workflows
- Decrease vulnerability to patch windows
- Accelerate patching from months to minutes
- Patch with confidence
- Create and deploy more updates faster
- Automate mundane tasks to maximize administrator productivity
- No additional consulting required

Reduce application security risks

Maximize your investment

Significantly reduce IT effort and cost

Unpatched vulnerabilities were involved in ***60%*** *of data breaches*

(Ponemon Institute Llc)

62% organizations weren't aware of vulnerabilities in their organizations prior to a breach.

Radia Features & Roadmap

Key Modules and Use Cases

Module	Use Cases
Patch Management	\ Support for Windows, Linux and macOS \ **Support for 300+ 3rd party applications.**
Security & Compliance	\ **Monitor and manage security vulnerabilities and configuration compliance** \ **Identify and rectify software security and Identify and rectify software configuration issues of the Sentient-managed endpoint devices**
Device Discovery	\ **Discover unmanaged devices across subnet.** \ **Import devices for management.** \ **OS Hardening, Software and Patch Deployment.**
Wake-On-LAN	\ **Install a critical patch or deploy a mandatory software on a device which is not powered on.** \ **Power on a Remote machine from Radia core console.** \ **Easily manage patch and software deployments on endpoints.**
Realtime Monitoring	\ **Validate the status and health of Radia services across the enterprise.** \ **Health of various processes grouped by server type, location, subnet and so on**

Focus on Security and overall compliance

Module	Use Cases
Secure Remote Control	\ **Approval based remote control** \ **No inbound port on devices for added security** \ **Detailed reporting of each session**
Inventory & Insights	\ **Detailed hardware information** \ **Detailed software inventory with software title recognition library** \ **Real time reporting of key metrics**
Software Usage Metering	\ **Software Utilization and License Compliance** \ **Identify which software applications are installed but not in use** \ **Reclaim unused licenses, resulting in cost optimization**
Software Management	\ **Policy driven Software Management (deploy, change, update, remove)** \ **Ongoing software update, verification and repair** \ **Support for package creation, deployment and execution**
Operating System Management	\ **Bare-metal Deployment, OS Migration, Disaster Recovery** \ **Deploy OSes based on machine make/model, user role or network location** \ **Easy settings migrations and in-place upgrade**

Managing the entire device stack

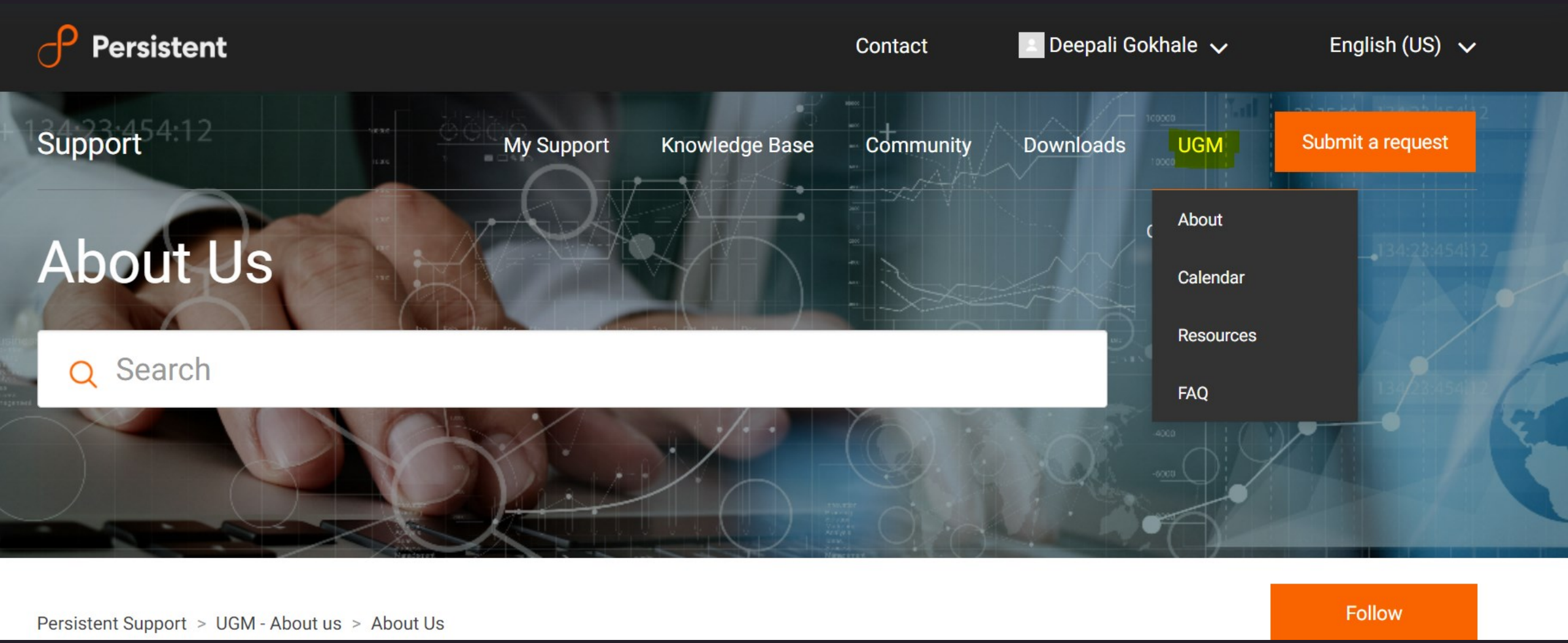
RELEASE TIMELINES

	10.0 CP5 – July 2021	11.0 – May 2022	11.1 CP1 – November 2022
S Security	\ Security & Compliance Updates \ Dual Factor Authentication \ Device Discovery - **Technology Preview*	\ Advance Patch Manager – Windows 3rd Party Application Patching \ Support for Radia on Cloud – (Public/Private) with Added Security	\ Radia Agent Support for Certificate Store
I Insights	\ Infrastructure Monitoring \ Remote Control (Version 1.0)	\ Remote Control (Version 2.0)	\ Radia Agent Monitoring \ Remote Control (Linux Support)
A Automation	\ Smart Agents (Version 1.2) \ Support for MS-Autopilot \ WakeOnLan	\ Smart Agents (Version 2.0) \ Added Analytics \ OMA/DM Support	\ Smart Agents (Version 2.1) \ Approval Workflow \ Policy Assignment, Job Creation \ Dynamic grouping of devices
C Continuity	\ Office 365 Standalone Support \ Reporting enhancement using ELK stack – Phase 1 \ Agent 64-bit transformation - macOS	\ Radia 64-bit transformation - Phase 1 (RCS, Apache, Java components) \ Agent 64-bit transformation - Windows	\ Radia Servers 64-bit transformation - Phase 2 (Final) \ Reporting enhancement using ELK stack - Final

ROADMAP & FEATURES

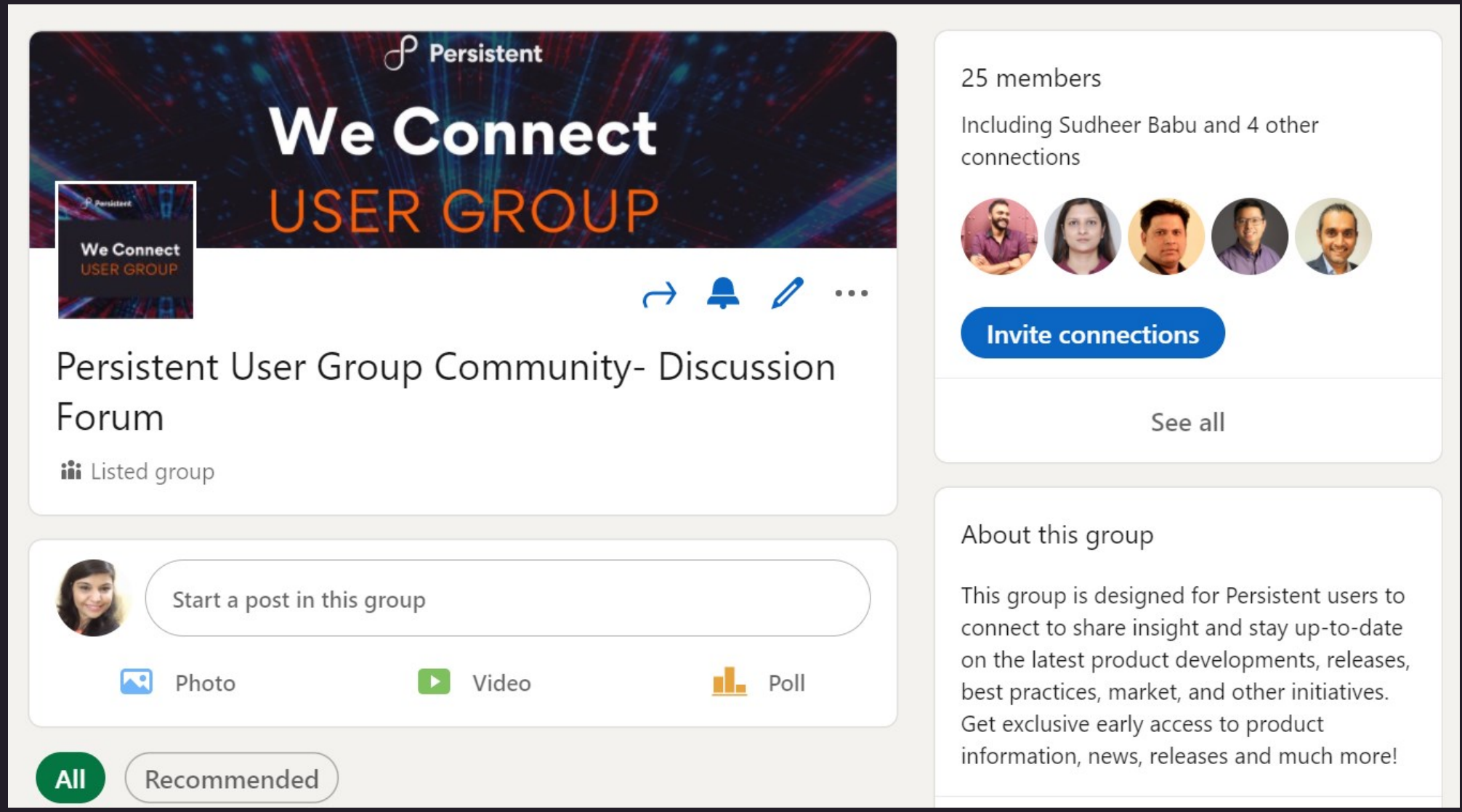
	2022	2023 & BEYOND
S Security	• PATCH MANAGEMENT UPDATES • 3RD PARTY PATCHING • VULNERABILITY MANAGEMENT FOR ENDPOINTS • EVENT DETECTION AND REMEDIATION (SEE & FIX) • REAL TIME MONITORING, REPORTING AND SELF HEALING OF END USER COMPUTING DEVICES.	• SIEM COMPLIANCE • DEVICE LOCKDOWN/QUARANTINE (FOR NON-COMPLIANT DEVICES) • VULNERABILITY MANAGEMENT FOR ALL CONNECTED DEVICES. • EVENT DETECTION AND REMEDIATION (SEE & FIX) - PHASE 2/FINAL • REAL TIME MONITORING (AND MANAGEMENT) OF ALL CONNECTED DEVICES (NETWORK DEVICES, HUBS, SENSORS ETC.)
I Insights	• SENTIENT INFRASTRUCTURE MONITORING • COMPLIANCE CHECKS AND REMEDIATION • SECURE REMOTE CONTROL	• COMPLIANCE CHECKS AND REMEDIATION • SECURE REMOTE CONTROL - EXTENTION FOR LINUX
A Automation	• INTEGRATION FRAMEWORK • APPROVAL WORKFLOW (FOR JOB CREATION /DEPLOYMENTS) • SCALABLE COMMAND EXECUTION FRAMEWORK • DYNAMIC DEVICE GROUPING • SMART AGENT	• INTEGRATION FRAMEWORK - EXTENTIONS • APPROVAL WORKFLOW (EXTENTIONS)
C Continuity	• PLATFORM SUPPORT FOR NEW OS, HARDWARE AND SOFTWARE • CUSTOMER RFE • PATCHES & HOTFIXES • CLOUD READINESS	• PLATFORM SUPPORT FOR NEW OS, HARDWARE AND SOFTWARE • CUSTOMER RFE • PATCHES & HOTFIXES
M Modernizat	• RADIA 64 BIT RELEASE • INFRASTRUCTURE OPTIMIZATION - MICROSERVICES AND CONTAINER READY - PHASE 2 • OMA/DM - MODERN MANAGEMENT SUPPORT	• AI/ML - FOR BETTER OUTCOMES, ISSUE DETECTION • INFRASTRUCTURE OPTIMIZATION - MICROSERVICES AND CONTAINER READY - PHASE 2/FINAL • IMPROVED UI, DASHBOARD AND REPORTING

User Group Resources



Link

Join our Discussion Forum



Link

Next user group meeting

4th April 2022

Digital Device Management

Radia - Endpoint Management

OTA, IoT

Security

Calendar Link

You will receive invitation for Product specific User Group Meetings shortly, if you have not received it, please write to pugm@persistent.com

Question & Answer

Let the discussion begin

Persistent

See Beyond, Rise Above

Persistent