infinipoint

SOLUTION BRIEF

Accelerate Critical Vulnerability Protection

Reduce MTTR and IT operations overhead for applying patches

Making sure your end user devices are patched and updated is an important part of any security program. Yet it remains one of the most tedious and exhaustive tasks an IT operations team can undertake. Infinipoint helps organizations accelerate the deployment of critical updates to end user devices by automating compliance checks and enabling 1-click, end user remediation without negatively impacting end user productivity.

Patching vulnerabilities and updating devices is still a problem

Despite an unprecedented wave of threats over the last year, many organizations still aren't patching vulnerabilities in a timely manner. Challenges include limited resources, manual remediation processes, end user disruption, and more. Research by Dark Reading reported 60 percent of organizations that experienced a data breach cited a known, unpatched vulnerability as the cause. And over 80 percent of security professionals forgo patching to avoid disrupting the workforce. The consequences of this can be costly, from the high cost of a data breach (average cost $4.24 million in 2021)[1], inflated IT operations costs and industry-specific compliance sanctions for failure to apply software patches in a timely manner when associated with a data breach.

Benefits

Infinipoint enables you to:

- **Reduce mean time to remediation (MTTR) to as little as 1 day**
- **Gain visibility into what patches have been deployed on what devices**
- **Automate manual process and reduce IT operational costs**
- **Reduce risk associated with compromised and vulnerable devices**

Enable a Zero Trust device posture and improve end user productivity

Infinipoint assesses the security posture of all end user devices upon accessing corporate resources. This includes critical updates needed for browsers, operating systems and other software. Once identified, Infinpoint initiates a 1-click remediation step to apply the update. This enables critical updates to be deployed in an automated fashion with no end user disruption and no additional overhead for IT. Updates are enabled via the Infinipoint Self-Service Portal which is updated regularly with the most recent updates and patches. Infinipoint also provides flexible options for remediation. End users can be granted grace periods for applying updates, striking an optimal balance between risk mitigation and business productivity. Lastly, Infinipoint can be configured to only enforce updates for critical vulnerabilities, such as for browsers, which often have many updates that are not critical enough to enforce an end user remediation action.

Infinipoint Highlights

Any Access Method

Integrates posture check and critical updates using any access provider.

Self-Service Portal

Continuously updated with the most recent critical updates, offloading IT.

1-click Remediation

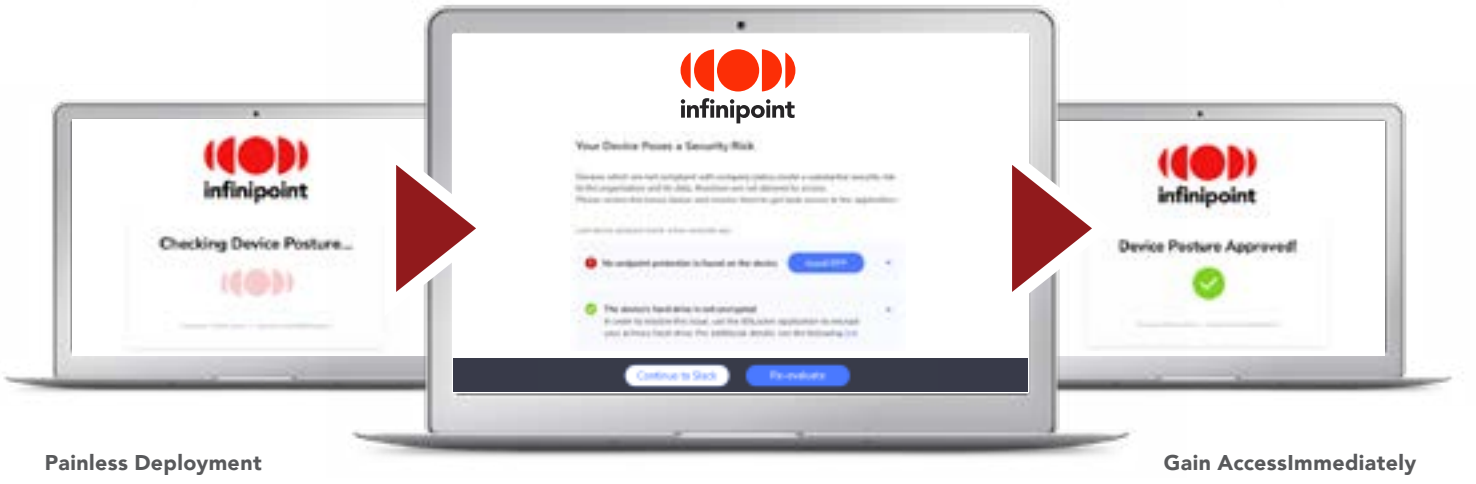
Offloads IT from pushing patches and automates critical updates.

[1] Cost of a Data Breach Report 2021

infinipoint

Productive & Secure Device-Trust

This is where adoption begins…



Painless Deployment **Gain AccessImmediately**

Advanced Policy Checks &
Self-service 1-Click-Remediation

Infinipoint automates the process of applying updates to critical vulnerabilities by conducting a security assessment upon access, identifying out of date software and enabling automated or end-user driven remediation. All without disrupting end user access or productivity.

Apply critical updates faster and minimize IT burden

- **Reduce mean time to remediation** - Accelerate updates for critical vulnerabilities by leveraging Infinipoint Self-Service Portal and 1-click recommendation options. Provide flexible remediation options including only applying updates to critical vulnerabilities, enabling end user grace periods for compliance, creating a frictionless experience for end users.
- **Validate critical updates are successful** - Avoid patch failure such as the update has been installed, but the browser has not been restarted or the system has not been rebooted. Infinipoint can help avoid these issues by enforcing the relaunch of the browser to ensure that not only the patch has been installed, but it has been applied with a required restart of the application.
- **Minimize IT operational burden** - Limit use of enterprise device management and patching systems to select corporate devices. Provide easy-to-use self-service remediation capabilities that address device vulnerabilities and security risks without putting an unnecessary burden on IT teams or users..

infinipoint

About Infinipoint

Infinipoint is the pioneer in the Device-Identity-as-as-Service security category to extend a true Zero Trust security posture to devices. Infinipoint is the only solution that provides Single Sign- On (SSO) authorization integrated with risk-based policies and one-click remediation for non- compliant and vulnerable devices. This reduces risk by protecting access to an organization's data and services while transforming devices to support a world-class security posture.

To Learn More Visit, infinipoint.io, or Contact us at Info@Infinipoint.io