Advanced Endpoint Management and Security

Real-time visibility and remediation for today's endpoint assets

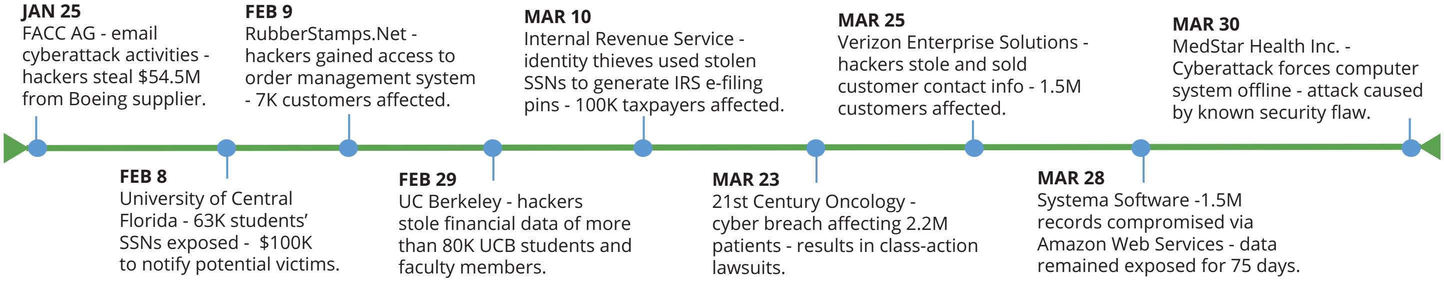
There is a security gap with the way in which we secure today's endpoints. This gap forces IT to work in a reactive manner, putting out the proverbial fires as they break out instead of being able to proactively monitor and manage based on information gathered and synthesized in real-time.

accelerite

Introduction

The pace at which today's business operates puts pressure on IT to deliver faster, and is expected to be in complete control of their environment each minute. IT managers can no longer afford to have a routine IT audit occupy their teams for weeks and months when their business heads expect turnaround times that is measured in hours and minutes. Add to that the challenge of ever-shrinking budgets, and rise in data breaches, disruptions and threats of malware attacks, and what the IT departments have on their hands is a seemingly impossible war to win.

In this landscape, extreme automation in endpoint management remains a critical need. Paradigms such as desired state management remain the cornerstone for lower TCO. IT endpoint management and security remains functional (e.g. patch deployment, configuration, etc.) dealing primarily with actions targeted towards a large set of endpoints as a monolithic activity, and is far removed from the reality of each endpoint's specific state. Of course the problem is that any delay in identifying vulnerabilities and threats due to potential security holes can have damaging financial implications. ***Figure 1*** shows the number of major data breaches and attacks that organizations faced in the first 100 days of 2016!



JAN 25
FACC AG - email cyberattack activities - hackers steal $54.5M from Boeing supplier.

FEB 8
University of Central Florida - 63K students' SSNs exposed - $100K to notify potential victims.

FEB 9
RubberStamps.Net - hackers gained access to order management system - 7K customers affected.

FEB 29
UC Berkeley - hackers stole financial data of more than 80K UCB students and faculty members.

MAR 10
Internal Revenue Service - identity thieves used stolen SSNs to generate IRS e-filing pins - 100K taxpayers affected.

MAR 23
21st Century Oncology - cyber breach affecting 2.2M patients - results in class-action lawsuits.

MAR 25
Verizon Enterprise Solutions - hackers stole and sold customer contact info - 1.5M customers affected.

MAR 28
Systema Software -1.5M records compromised via Amazon Web Services - data remained exposed for 75 days.

MAR 30
MedStar Health Inc. - Cyberattack forces computer system offline - attack caused by known security flaw.

Figure 1: List of major data breach incidents (Q1/2016) - Source: Identity Theft Resource Center (ITRC) Data Breach Report

The IT departments today need a way to find anything across all their assets in real time, and then be able to take corrective action rapidly. Anything less is rolling the dice.

Traditional Endpoint Management and Security Systems

Traditional computing endpoints – primarily PCs and servers – have been only recipients of changes that the IT administrators make on them based on the information they receive from various Information Sources (***Figure 2)***. Supporting Information Sources in the context of endpoint security solutions is a matter of integrating with the right databases and security information brokers who have a list of latest vulnerability, threat and patch information – all valuable to maintaining and enhancing the security posture of any organization.

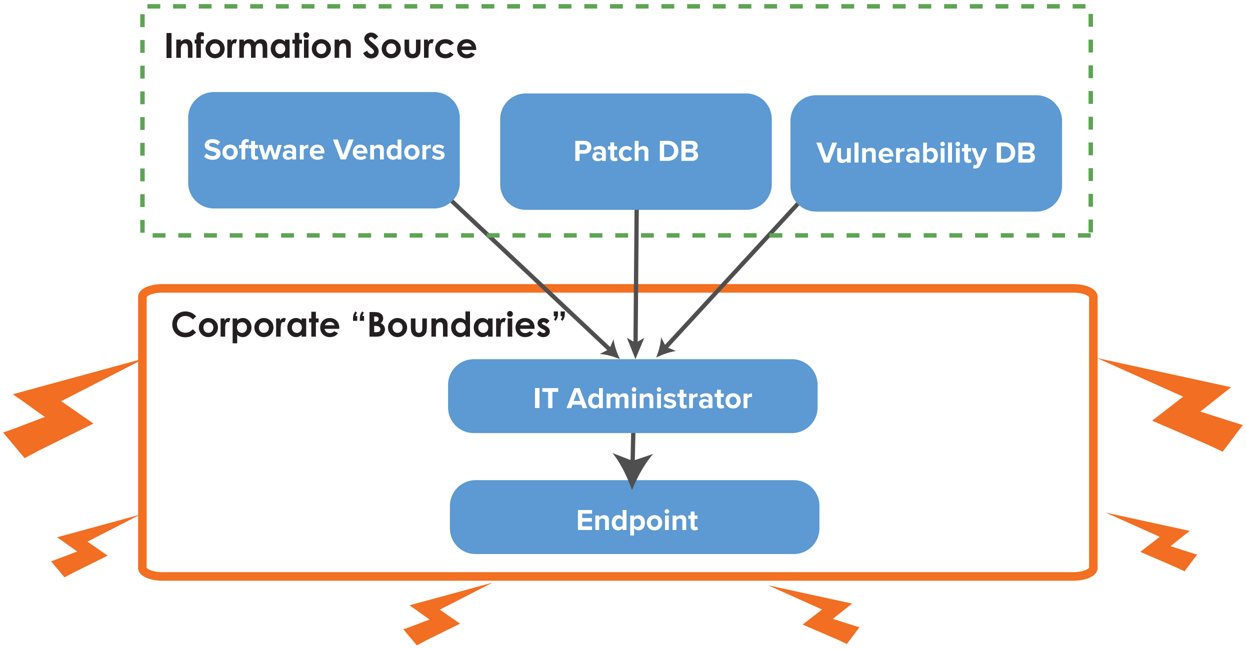


Figure 2: The Trinity of Endpoints, Administrators and Information Sources for Endpoint Security

Traditionally, corporate endpoints within the sheltered corporate "boundaries" – both physical and network boundaries – have been managed and secured using many different tools such as network monitoring and security tools, firewalls, website blockers, and many others. These tools have come together to comprehensively manage and secure client endpoints as well as corporate servers. Endpoint management, endpoint security and OS providers have added further value towards creating a safe and secure environment for endpoints that work in the corporate environment. The Information Source consisted of software vendors, security and vulnerability databases, patch databases and so on.

Same Endpoint But A Widening Security Gap

Endpoints today – even the traditional ones such as laptops – operate in a dramatically different environment. They operate more “out” of physical and network boundaries than their predecessors thanks to better connectivity and a more distributed and mobile workforce operating remotely and from home. They are also more dynamic (i.e. used for varying purposes undergoing significant changes in a short span of time), and are prone to variations due to a more “hostile” local environment.

Approaching the management and security of endpoints today in the same way as earlier leaves a gaping hole in the IT management and security environment. The endpoints today undergo more frequent changes, are more prone to hacking, changes in their software and configuration, malware attacks, theft and other deviations. Apart from periodic checkpoints that can be spread weeks or months apart, IT is essentially “flying blind” against such exigencies!

The problem with the traditional way of managing endpoints is clear – even as IT grapples with a ton of information from its current information sources, it has limited information from the endpoints themselves – and it needs this information at a much faster clip than ever before! There is also the challenge that too much data is not helpful. While reports provide varying degree of detail, they are built for a very different purpose. They are primarily for seeing results of past actions performed on endpoints than gathering fresh information on them (see inset for additional limitations of endpoint reports). IT departments need to be able to pinpoint specific data elements across the network, and bring them back in a matter of seconds.

Reports: Looking backward, not acting forward

- Oriented towards results and outcomes of past actions on endpoints rather than future actions that need to be taken
- Appear without any context of changes that might have happened anywhere in the endpoint universe – from the information source to corporate IT environment to the endpoint themselves
- Viewed infrequently with information in them often days and weeks old
- Not in the clear line of sight of the administrators while they are “acting forward” on the endpoints

This gap in endpoint management trinity of Information Source, Administrator and Endpoint is illustrated in ***Figure 3***.

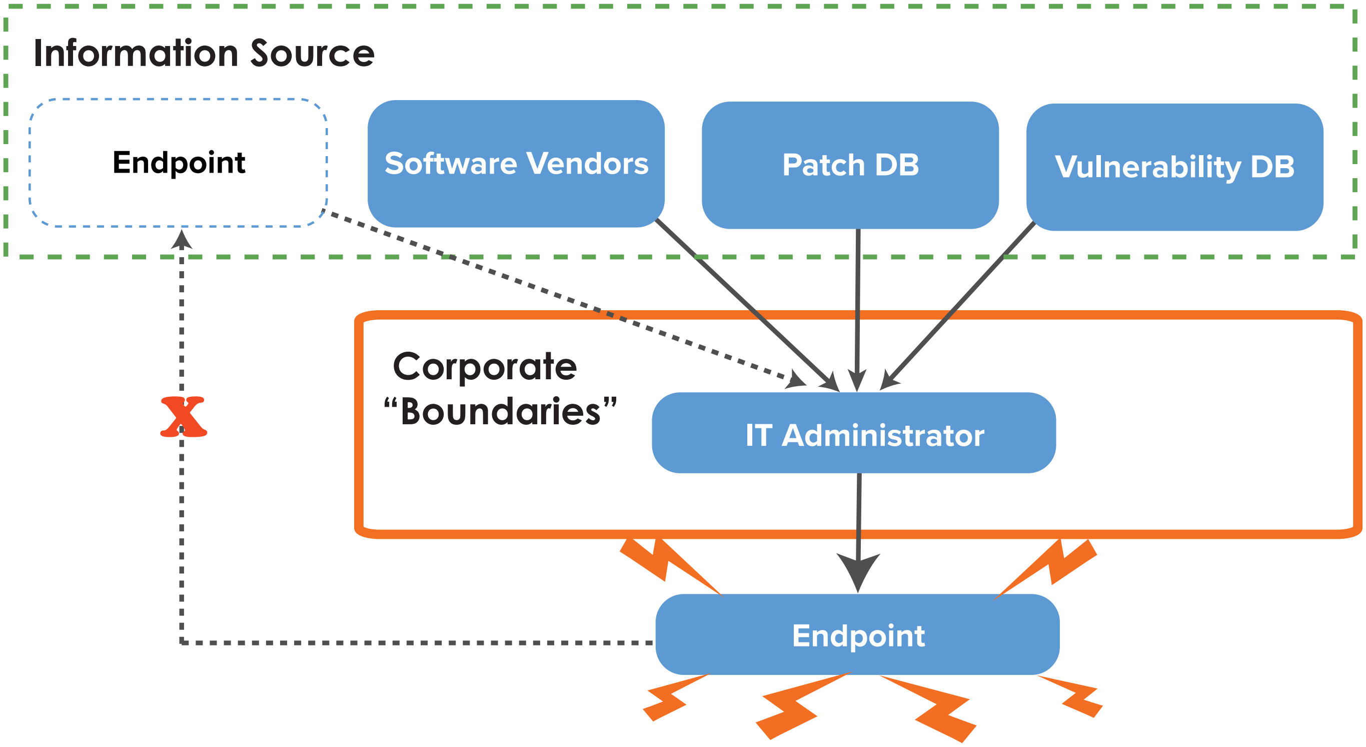


Figure 3: Modern Endpoint Environment

As these endpoints proliferate through the organization and workforce becomes more mobile with them, this gap will only widen further. Without using endpoints themselves as an active source of information, IT will miss a critical piece of information that can help them make informed and timely decisions.

Following are the four key characteristics of information they additionally need in today's environment:

1. **Information Straight from the Source** - According to a recent report from Hewlett Packard Enterprise called the HPE Cyber Risk Report 2016, "Attackers have shifted their efforts to directly attack applications". The report goes on to say that they have "shifted their focus from servers and operating systems to applications" – meaning, your endpoints. It is clearly not enough to monitor and secure the network and data from one end while the attacker is attacking the other! There is a need to bring endpoints into the realm of information source and work with them directly instead of intermediate caches or databases.

** HPE Cyber Risk Report 2016, http://techbeacon.com/resources/2016-cyber-risk-report-hpe-security*

2. **Information in Real-Time** - Endpoint information is much more dynamic than the other sources. It changes on a daily and sometimes even hourly basis. Not getting timely information from them can give a false sense of security, which only worsens as precious days and weeks go by since the “last scan” was performed! Given the fast-changing and dynamic nature of endpoints and pace of corporate working today, it is important for IT to have the most current information on their endpoints.
3. **Information When They Want It** - IT operations and security teams use multiple tools for managing and securing their network and endpoints, such as DLP, disk encryption tools, endpoint management solutions, anti-virus, firewall and many others, all of which have a specific cadence and purpose. IT needs to have an integrated view of all their endpoints, and be able to run queries “out-of-cycle” from current operations, as and when they need.
4. **Information That is Specific** - While the attackers are sharpening their attacks on individual endpoints and applications, IT’s remediation and fixes turn out to be blunt at best, and off-the-mark at worst. The current information available today is trapped in multiple databases as systems of record, and covering all the endpoints to instantly gather information on their most current state as recorded by each of these tools presents a formidable challenge for IT teams. IT needs to have a way to quickly zero in on specific configuration items and attributes that are critical, identify patterns in them, and be able to visually view the results to ease their actions.

Accelerite Sentient – A New Paradigm for Endpoint Management and Security

Due to the above gap in the current enterprise architecture, IT is forced to work in a reactive manner, putting out the proverbial fires as they break out instead of being able to proactively monitor and manage based on information gathered and synthesized in real-time. Plugging this gap is only possible if the endpoint itself is capable of being an information source for IT administrators. But how do you go about fixing the enterprise architecture to incorporate a change of this nature? What are the key considerations and parameters that one needs to keep in mind when incorporating this change?

Accelerite Sentient fills this gap, and provides IT administrators a way to query endpoints for their current status – including applications installed on them and their versions, software they are running, existence/absence of files in them, their available disk space and many other critical parameters. Sentient has the following key characteristics that are critical to managing and securing endpoints:

1. **Real-time Information for Immediate Action** - Sentient empowers IT administrators to pull in real-time information from enterprise endpoints in order to quickly identify critical pieces of information, security threats, vulnerabilities, and address compliance and configuration issues in their endpoint network within seconds and minutes.

2. **Proactive Oversight and Management** - Sentient allows administrators to proactively query the current status and existence/non-existence of configurations and files from the point of view of actively unearthing issues in real-time, in contrast to reporting queries that are targeted towards analyzing outcomes of actions that administrators have previously taken. With Sentient, IT admins can now get ahead of the problem and be able to proactively address their endpoint configuration and security.

3. **Targeted Operations Across Diverse Endpoints** - With Sentient agent residing in each endpoint and responding in real-time, administrators can take more targeted actions that effect a narrower set of relevant endpoints and query them for specific attributes instead of casting a wide net every time and putting undue pressure on their network and many endpoints at the same time.

4. **Insights-Driven for Maximum Impact** - Sentient classifies and presents the information gathered in visual format with drilldown information, and makes it easy for IT to locate problem areas in their network of endpoints quickly. The search queries in Sentient are in freeform text format, which enables IT to easily query their endpoints using natural language phrases.

Sentient integrates with other endpoint management and security tools, and allows for IT departments to have in-place remediation. It complements the current IT endpoint management and security operations infrastructure, additionally providing real-time information, and works as a gateway security solution.

Conclusion

As workforce becomes increasingly mobile, working from home, working remotely, and attackers attacking more applications than servers, endpoints need to be more proactively involved in the decision-making processes such as patching them, updating software versions, changing configurations, installing and uninstalling files or software, and so on. It is no longer enough for them to be just "managed" as a reactive measure based on information that is only external to them. They need to be made smarter and be included in information gathering for compliance, security, audits, asset utilization, etc. Accelerite Sentient provides IT departments the means to gather information from endpoints in real-time for proactive management and security of endpoints.

accelerite

Accelerite delivers business-critical secure infrastructure software for Fortune 500s, telecom operators and SMEs around the globe. Accelerite's product suite includes solutions for cloud life cycle management, endpoint security, enterprise mobility management, and the Internet of Things. Headquartered in Santa Clara, CA, Accelerite serves as the products business of Persistent Systems (BSE & NSE: PERSISTENT), a global leader in software product development and technology services, with 9,000 team members worldwide.

Interested in seeing Accelerite Sentient in action? For more information, please visit accelerite.com/site/real-time-security or contact sales at +1-800-787-9540 or sales@accelerite.com.