jamf

Defense-in-depth:

Closing gaps in security by integrating and layering solutions

Cybersecurity is not important.

It's **critical** to defend your organization from evolving threats and attacks targeting your devices, users, data and resources.

Information security used to be little more than an antivirus solution installed on each computer and a VPN client for the few employees, like traveling sales teams, that worked away from the office.

But times have changed and with it, how we handle cybersecurity.

In this white paper, we cover the:

- Evolution of the threat landscape
- Cruciality of protecting all device types and OS's
- Keys to security that go beyond protecting resources
- Criticality of implementing a defense-in-depth strategy
- Importance of an integrated security approach for enterprise

Evolving threat landscape

The industry has come a long way and advancements in mobile technology signaled to users and organizations that how work was accomplished was ready to change. This evolution didn't stop there. Threat actors too changed their tactics, adapting to changes by evolving threats and attacks. Making them far more sophisticated – which means they are harder to spot for end users and much more difficult to defend against by security professionals.

Simply put: threats now come from every angle. Targeting all device types and operating systems, and being deployed over any network connection.

Why, you ask? Because the perimeter-based, "single solution strategy" that may have once had relative success at ensuring data and endpoint security has been rendered ineffectual. The network perimeter was effectively eroded by the:

- Shift to cloud-based services and apps
- Transition to remote/hybrid work environments
- Inclusion of personally owned devices for work
- Use of untrusted network connections for communication
- Reliance on shared tools for collaboration

Each of these points has no doubt opened up possibilities for users to work from anywhere, at any time, on any device and over any network connection, regardless of physical location or preference in architecture or software. They have also increased potential vectors to exploit by exposing more of a device's attack surface.

Here are some of the different ways in which the threat landscape has evolved to account for the rise in mobile technologies and distributed workforces.

APTs, converged threats and increased attack complexity

The threat landscape has evolved. Any security professional worth their salt knows this statement to be true. But exactly how the landscape has changed, that is the aim of this section. Malicious code is malicious code – whether it's contained in a wrapper posing as an application or executed via a compromised website – the result is and has always been the same: to infect your device and get it to perform tasks that the attacker wants it to execute.

What's being seen is a departure from the 1 + 1 = 2 formula relied upon for so many years. Attacks have grown in complexity, often seeing them combined with other threats or deployed through alternative means, such as compromising a trusted partner of the target, in turn providing backdoor access to the intended target's resources. Examples of some of these sophisticated attacks going back only one to three years are:

- Two attacks in just as many years affected over **100 million** customers by compromising their PII.
- Supply chain attacks tripled in 2023, with **2.1 billion downloads** with known vulnerabilities identified (when fixed versions were available).
- Casino and Hotel experienced a ransomware attack proceeding a social engineering campaign, impacting operations, compromising customer data and leading to financial losses.
- Data exposure linked to **5.4 million users**, alongside an additional **400 million users**' public and private data were sold on the dark web after a social media platform's API was compromised.
- High-risk individuals are continually targeted by nation-states using Pegasus spyware to impact privacy through unauthorized surveillance of personally owned mobile devices.

Converged threats

Also referred to as cyber-physical convergence, it gets its name from the increasingly intertwined nature of our digital and physical domains. Because the line between these two spheres continues to blur as they seemingly enmesh more and more together, impacts on one domain (cyber) have very real effects on the other domain (physical). In addition to disrupting systems, processes and resources physically, knock-on effects are exacerbated by cyber threats that extend attack reach, leading to greater implications triggered by:

- Achieving persistence
- Privilege escalation
- Lateral movements
- Malware deployment
- Data exfiltration

We see this in companies of all industries as their reliance on technology has become so crucial to business continuity that suffering a cyberattack, for example, one that prevents users from accessing email can virtually cease operations until access is restored. Given enough time, the impact on operations could lead to issues of greater significance, such as loss of production and/or revenue, even forcing affected businesses to shut their doors permanently.

Such was the case when the largest pipeline for refined oil products in the U.S., capable of carrying 3 million barrels of fuel per day – was forced to shutdown for five days after being hit with a ransomware attack in 2021. The impact on this critical infrastructure? The most reported was the $5 million ransom that was paid to the threat actors to regain access to encrypted systems and data. In the years since several changes have occurred stemming from the attack. The Department of Justice's more aggressive approach to taking down the infrastructures and criminals behind ransomware attacks is one. Yet, threat actors have also evolved tactics, as "more than 90% of attacks no longer encrypt the victim's devices but simply exfiltrate the data and extort everyone."

Social engineering

There is seemingly no end to the number of social engineering-based threats across the modern threat landscape. At one time, the only common concerns were an occasional impersonator trying to pass themselves off as a company employee or that email from a generous yet worried prince who so desperately needed your bank account to hold on to his millions.

Oh, how times have changed.

Social engineering exists today as an almost hierarchical flowchart, detailing a never-ending list of attack types too numerous to list entirely. One that sees new additions made almost lockstep with the release of each new technology. No doubt, the "one ring to rule them all" is phishing and all the variants that spring from its well.

And while each new iteration, like QR code phishing, or "quishing" as it is affectionately named polymorphs its way into our security vocabulary, there are two levels of evolution happening within social engineering – one that's at the surface level and another that sits below the surface. The former is easy to spot. It's the top five impersonation threats that see phishing adapted to target the way we work:

1. Email phishing
2. Spear phishing
3. Whaling
4. Smishing and Vishing
5. Angler phishing

The latter, however, doesn't have a clever name attached to it per se. That serves to make these novel threats all the more dangerous...and difficult to detect by end users, IT and Security teams alike.

Two examples of these tampering techniques were recently discovered by Jamf Threat Labs and their proof of concepts (PoC) pose startling impacts for mobile security – currently and in the future:

Fake Airplane Mode

A post-exploit persistence technique that shows a functional Airplane Mode. However, look below the surface and you'll find that after a successful device exploit, threat actors have edited system files that control the UI to display Airplane Mode icons while simultaneously disabling internet access to all apps except the attacker's application. Doing so enables the attacker to maintain access to the device (persistence) even when the user believes they have successfully placed the device offline.

Fake Lockdown Mode

Previously, we mentioned the Pegasus spyware and how nation-states rely on that exploit to track high-risk individuals. While we go into nation-state/sponsored threats in the next section, an important tool to reduce the attack surface is Apple's Lockdown Mode.

Consider for a moment that, believing your mobile device to have been compromised, you enable Lockdown Mode to protect yourself from further exposure. Only to realize that your device remains every bit as vulnerable because threat actors have effectively bypassed this protection of last resort.

These are exactly the types of social engineering threats that trick users into believing they are protected, when in fact they have been misled into this false sense of security while threat actors maintain access to and control over their mobile devices.

Nation-state/targeted attacks

In the digital age, feelings of paranoia related to every action taken, word spoken, and message replied to – in public, at the office or in the privacy of your own home – are justified given just how pervasive technology has permeated into seemingly every facet of our existence.

Even if you, like Christopher Walken, have adopted a policy of not owning a computer or smartphone, you are still at risk of having your privacy impacted by those using mobile devices around you.

Nation-state/sponsored, or Advanced Persistent Threat (APT) groups don't only pose a threat to businesses in certain industries. The modern threat landscape sees APTs expanding their scope of attack beyond critical infrastructure to target any persons, organizations and/or regions that further the nation-state's interests.

Here are some nation-state data points by the numbers:

90% of security alerts originated from sectors outside of critical infrastructure

Top 3 most targeted sectors globally are:
Education **16%**

Government **12%**

Think tanks/NGOs and IT tied at **11%** each

9 in 10 organizations believe they've been targeted by state-affiliated threat actors

The cost to organizations averages **$1.6 million per incident**

5 APTs (so far) have been observed weaponizing AI to enhance threat capabilities

While financial gain certainly ranks among the top motivators for any threat actor, nation-state and state-affiliated threat actors' primary objective is data theft. This is not to say that espionage and disruption of networked systems and services are less significant objectives by any means. The modern threat landscape finds APTs increasingly prioritizing the exfiltration of sensitive and confidential data as a means to gather intelligence, carry out other malicious attacks and impact social and political activity.

In the case of the latter, espionage, particularly the proliferation of mobile malware used to spy on high-risk individuals has merged with privacy concerns over unauthorized surveillance via the myriad sensors included in mobile devices to monitor users. And it doesn't end there, with nation-states utilizing the data gathered to further target victims, such as journalists, politicians and executives – without their consent and without knowledge that their devices have been compromised. Thanks to their stealth-like features, this type of spyware is designed for remote deployment and extraction of any data type from a victim's mobile device, often relying on zero-click installation and zero-day exploits to infect target devices.

One size does not fit all

In addition to the evolving nature of cyber threats we discussed in the first section, each of these points has had a hand in leading us to where we currently are. A tipping point where legacy solutions, procedures and workflows designed to protect a:

- Company-owned desktop computer
- Running one supported OS

That is locked down by IT to:

- Only run limited software applications
- Restrict performing any tasks not in scope with business objectives
- Sit within the relative security of the company's network perimeter
- Route network traffic through the corporate Firewall
- Protect data with antimalware solutions
- Securely tunnel remote access by a VPN

Legacy solutions developed to secure static endpoints are not enough to ensure a computer's security posture in today's threat landscape let alone in modern enterprises that encompass all the impactful changes that represent dynamic work environments.

Modern security strategies benefit from being strong yet flexible. Simply invoking an administrative policy that bars the use of mobile devices, a particular OS type or personal devices will not mitigate risks associated with that hardware or software. The fact is, such a policy wouldn't even prevent users from trying to access enterprise resources from "restricted endpoints." The possibility of them introducing risks into your network is very real – and worse yet – administrators wouldn't be aware of this until after an incident occurs.

What is the best course of action then?

IT and Security teams are able to best manage endpoints and their security by relying on best-of-breed solutions. The management and security solutions are designed to support their respective device type(s) and OS's natively. This not only ensures the greatest level of compatibility with hardware and software but also provides IT and Security teams with the tooling needed to best manage and secure the endpoints in their infrastructure.

macOS in the enterprise

Consider your enterprise environment. Chances are that you manage Windows-based devices for work, but what's your stance on macOS computers and laptops? According to a recent survey of small and medium-sized enterprises, "**55%** of businesses use Mac devices themselves or explicitly approve of their use within the company.", regardless of the industry.

Before we go further, let's examine macOS market shares (as of February 2024):

Globally:	U.S.:
15.46%	**25.02%**

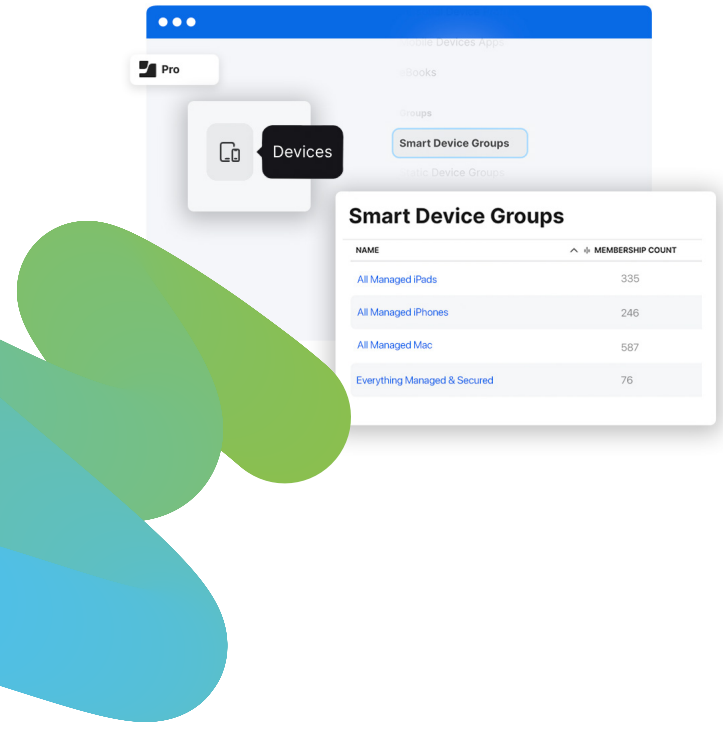
In the U.S. alone, macOS commands a quarter of the market; with just over half of that number being used in business. So, a better question to ask may be how do you secure macOS endpoints when (not if) they're used in your enterprise? Because – like it or not – macOS is likely being used to some degree or another by your end users to perform work-related tasks. Whether it's sanctioned by the company, as a corporate-issued device, part of an employee choice program, or BYOD/COPE initiative or a personal device that a user utilizes even though it is unsanctioned.

Not only is Mac growth accelerating but it impacts adoption for work and will have critical consequences for enterprise security – as would any piece of hardware or software – if not addressed by IT and Security teams using native management and security tooling that are designed to meet the unique needs of Macs, just like they do with Windows-based devices.

Mobile devices: Unchecked risk

The average user has one computer to use, but often utilizes multiple types of mobile devices, such as a smartphone, tablet and smartwatch. In fact, according to a Statista survey, the average global number of devices per user rose to 3.6 in 2023.

That's four times the attack vectors per user. It's a "no-brainer" for organizations to secure desktop OS-based devices, but if mobile devices go unchecked in the enterprise that means they're likely allowed to connect to corporate networks and access business data and resources as part of the employee's productivity workflow without protection.



What types of mobile threats exist?

Many of the same ones that exist for desktop computers, only without specialized endpoint security software to provide visibility into the unique filesystems of mobile devices.

Below is a look at how common types of mobile risk can impact the enterprise:

- **Unauthorized access:** Social engineering campaigns gather credentials from victims through SMS and social media, allowing threat actors to gain access to business services.
- **Malware introduction:** Apps downloaded from unsupported app stores or sideloaded execute malicious code when launched, affecting business and personal data.
- **Non-compliance:** Lack of policy-based enforcement leaves organizations open to liability when devices fall out of compliance, increasing consequences in regulated industries.
- **Data exfiltration:** Theft of business, personal and privacy data places sensitive and confidential information directly in the hands of threat actors.
- **Lateral movement:** Network-based attacks leverage compromised credentials to extend attacks across the infrastructure, increasing the size of data breaches.
- **Bypass protections:** Misconfigured security and app settings lead to increased attack surfaces, making it easier for threats to execute payloads on devices without mitigation.
- **Privilege escalation:** Vulnerabilities found in out-of-date software can be exploited, giving threat actors a way to gain a foothold into devices, and by extension, your network.

Going beyond simply protecting resources

When speaking of closing security gaps, there's a natural progression of thinking that occurs among security professionals envisioning the different ways to mitigate risks. Refining patch management processes so software and operating systems remain up to date and protected against known threats is one common thought. Another might be to embrace recent artificial intelligence (AI) trends to incorporate machine learning (ML) technology into your security stack to respond to incidents more quickly or streamline threat hunting through automation.

While these are all excellent ways to shore up security gaps, there are other elements to this that go beyond implementing updated controls to better secure devices, users and data. Underlying elements that, while maybe not as flashy or "fun" to work with as technical or logical controls, add value to your organization by streamlining, automating and consolidating the procedures, processes, tooling and workflows that make up your overall security strategy. Furthermore, it brings all of them together alongside the IT and Security teams responsible for ensuring devices, users and data are compliant, and operate efficiently.

In this section, we delve into these elements, dubbing them "the four C's" to highlight how they work together to maximize efficacy while minimizing challenges to your organization's overall security posture.

Consistency

Organizations should treat all device types that are used for work and connect to business resources – alongside the various OS's running on them – in the same regard when it comes to enterprise security. After all, a company that issues Windows computers to its employees and deploys endpoint security controls to ensure they remain managed and secured but does not implement mobile threat defense to safeguard business data from unsanctioned mobile devices used by the same employees effectively leaves them open/unsecured to mobile risks that may precipitate a data breach.

Despite being secure by design and Apple's doubling down on security and privacy, threat actors routinely attack Apple devices (macOS, iOS and iPadOS) just as they do Windows or Android devices. The problem with consistency is not focusing exclusively on how each OS is different from the next, but rather on how they're alike. After all, desktops, laptops, tablets or smartphones – despite differing footprints – are still examples of computing tools that share more in common at their operational core than the sum of their visual differences.

That is the crux of consistency: treating all endpoints that access enterprise resources the same – regardless of:

- Device type
- Form factor
- Operating system
- Apps and services

Compliance

The definition of compliance is the act or process of yielding to a desire, demand, proposal, regimen or coercion.

Compliance may hold a different meaning depending on the industry your business operates. For regulated industries, there are specific laws that govern how data, processes and workflows should be secured to prevent leaking of protected data types. For non-regulated industries, organizations may have a level of compliance they seek to maintain. One that may be aligned to internal business policies and/or tied to standards or frameworks they desire for their business operations to follow. Or perhaps both.

Talking of compliance as it pertains to closing security gaps means addressing two salient points:

Using Baselines

The first point is baselines. More specifically their creation to establish the boundaries of what's considered normal operation levels for your infrastructure. Because of their design, baselines also provide a demarcation point for administrators, alerting them when endpoints steer out of the acceptable parameters of the baseline, indicating they may have fallen out of compliance.

Providing proof to auditors

Whether your organization dispatches internal auditors or is subject to independent third-party auditing as part of its regulatory obligations, some form of proof is always necessary to show that compliance has been maintained. The general rule of thumb among auditors applies here when proving endpoint compliance: "If it's not documented, it didn't happen."

The key to managing baselines and gathering proof for audits lies in telemetry data. It provides admins visibility into endpoint health and can be referenced at any given time to gain insight into whether devices used to access, process, store, modify, disseminate or share company data meet the guidelines or requirements set forth by your security plan or regulatory governance.

Consolidation

The third “C” also happens to be one of the most misunderstood as it is often mistaken to refer to the consolidation of solutions.

> **“Cybersecurity is much more than a matter of IT.”**
>
> **— Stephane Nappo**

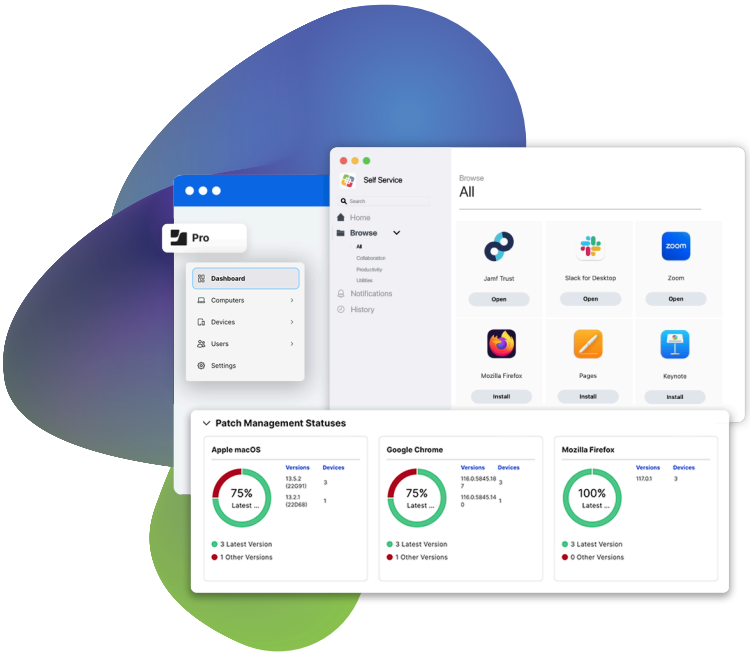
Consolidation as it is used here refers to the merging of IT and Security professionals into one cohesive team. This is a change from the disparate operating nature of both teams. Despite both falling under the umbrella term of Information Technology, organizations have typically kept the operations of these departments separate for any number of business reasons.

In considering the modern threat landscape, the problem with this method of operation is that each department manages its own set of software, vendor partnerships, processes, policies and workflows. In theory, their different approaches are intended to strengthen the security posture of the devices and the organization overall. But the reality often is that type of structure achieves the opposite effect.

Effective consolidation requires modernizing and integrating cybersecurity architectures and processes to:

- Centralize best-of-breed solutions to manage supported platforms natively
- Reduce the number of vendors and partnerships
- Break silos; increase information sharing
- Eliminate gatekeeping by establishing knowledge management practices
- Integrate management and security approach
- Unify threat prevention and hasten incident response
- Extend protections across the entire infrastructure

By shifting to an integrated security + management approach, enterprise administrators tasked with ensuring that devices and users remain secured by comprehensive security protections when accessing and working with sensitive business data, extended holistically across corporate resources.



Cost savings

Alongside consolidating IT and Security, consideration should be given to the importance of Return on Investment (ROI). A particular feather in the cap for ROI is the cost savings that may be gleaned when organizations choose solutions that are a “best fit” for consistently addressing their unique needs on their path to compliance. This not only requires an understanding of the value relative to the cost of the solutions but also balancing the other factors that have direct (and indirect) impacts on ROI related to your defense-in-depth strategy.

Some examples of the direct and indirect factors that impact ROI alongside the greater security strategy are:

- Choosing tools that natively support the devices and OS types in your organization but also integrate to form a holistic solution
- Incorporate automation for manual and time-consuming tasks, achieving greater efficiency while freeing admins to focus on value-adding projects
- Streamlining security processes and workflows, extending them across the infrastructure and optimizing them to support endpoints and applications at scale
- Reduction in complexity between solutions and incident response minimizes discovery of security incidents and remediation timeframes = less downtime and higher productivity
- Active monitoring and reporting places rich telemetry data in the hands of administrators in real-time, proactively detecting/correcting risk vectors before compliance is impacted to proactively detect/correct risk vectors before compliance is impacted

Another consideration relating to cost savings and the modern threat landscape relates to the use of personally owned devices for work. Many organizations have an ongoing BYOD initiative, especially in remote/hybrid environments to stay connected and collaborate with team members. And there is no doubt that BYOD benefits employers, which is why Zippia has recently reported that nearly **70%** of IT decision-makers in the U.S. approve of BYOD programs.

96% of mobile devices connecting to enterprise networks are personally owned

80% of senior business leaders believe that mobile devices are essentials for employees to do their jobs

Employees augmented by wearable technologies set to increase by **30%**

It’s also a boon for organizations with employee choice programs, permitting employees to choose the hardware and software that they feel most productive using without the financial impact of purchasing and maintaining inventory for hundreds, thousands or even tens of thousands of mobile devices in addition to computers. That adds up to some serious advantages and cost savings.

Defense-in-depth: Effective, layered security

The National Institute of Standards and Technology (NIST) defines defense-in-depth (DiD) as an *"Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization."*

Adapting this to your cybersecurity plan yields additional protections that strengthen your security posture. But this approach to layering controls grants organizations a safety net if you will. One that implements stop-gap measures, preventing threats from compromising enterprise resources. Should a threat bypass a control at one level, the next one encountered along the attack's path will be there to catch and mitigate the risk before it can evolve into a compliance-impacting incident.

Some of the questions we answer in this section are:

- How does integration holistically affect your enterprise cybersecurity plan?
- What are some of the types of comprehensive security controls you can implement to achieve DiD?
- How does your DiD-enabled cybersecurity plan impact meeting compliance requirements?

Management + Identity + Security

You're likely familiar with device management concepts such as management, identity and security. On their own, each of these is considered a foundational element, notably supplying a specific set of technologies and best practices tied to their respective categories:

- **Device Management:** The administration of computers and mobile devices, which includes managing settings, deploying secure configurations, installing software and enforcing policies.
- **Identity and Access:** A framework of policies and technologies ensuring that authenticated users and/or authorized devices obtain the necessary access to protected resources based on assigned permissions.
- **Endpoint Security:** Software-based technologies designed to minimize risk and protect devices and users against threats and attacks while safeguarding protected resources.

The integration of these three foundational elements acts as the building blocks when designing a rich, deep cybersecurity defense-in-depth plan to ensure enterprise resources are safe from unauthorized access, minimize endpoint risk vectors and keep users secure and productive.

In the following sections we delve into some of the technologies that are not only made possible through integration but highlight how they work to minimize risk, prevent malware and detect and mitigate advanced threats:

- Zero-touch deployment
- Threat hunting
- Zero Trust Network Access (ZTNA)
- Advanced threat response

Zero-touch deployment: secure from the start

Security is often a reactive process. The name "incident response" speaks to the reactionary nature of waiting until threats are detected before they can be addressed. Like cause and effect.

While there isn't much admins can do to change this cause-and-effect nature, there are several things that can be done to reduce the attack surface, which in turn, minimizes the "how" and "where" threats can impact a device.

And what better place to start than the first time a device is powered on, right? This is the magic of provisioning and zero-touch deployments... and it is especially easy to take advantage of zero-touch deployment when tasked with managing Apple devices.

This is because enterprise zero-touch deployments rely on management and identity and access workflows proactively delivered to devices during the initial setup screens. Specifically, after the user authenticates successfully using corporate credentials and completes enrolling their device and installs the management profile. The MDM immediately begins to deploy everything the user needs to get work accomplished, configuring the device to organizational standards.

What can be deployed during the provisioning phase of zero-touch?

- Hardening device security
- Installing managed apps
- Configuring application settings
- Assigning user accounts
- Curating Self Service options
- Updating system patches
- Deploying security software
- Setting enforcement policies

You may be thinking, that's great for company-owned devices, but what about BYO devices?

Zero-touch workflows extend to any ownership model, including personally owned devices. For these instances, Apple designed User Enrollment so that user privacy is maintained without sacrificing corporate security protections.

Some of the features of user-initiated enrollment of personal devices with the corporate MDM are:

- Secure access to institutional resources such as email, contacts, calendars, Wi-Fi and encrypted network connections
- Business data is stored in a separate, encrypted volume on the device while personal data remains untouched
- Two Apple IDs may be used: a personal one for personal data and settings, and a managed one for institutional data
- Administrators can only see, access and remove institutional data from BYO devices; personal and privacy data remain inaccessible and unimpacted
- Standardize security across the entire enterprise, ensuring all devices maintain the same level of protection, regardless of their ownership level

Threat hunting: proactive > reactive

Among the more specialized tasks administrative teams are empowered to perform is incident response. The detection and triaging of potential issues begin when admins are alerted by endpoint security software that a malicious behavior or threat has been flagged. Response teams are dispatched to confirm, contain and ultimately remediate the issue.

While addressing known issues is par for the course for responders, there are added components that convert the largely reactive process into one that is proactive by integrating management and security solutions to augment workflows and processes.

Establish secure baselines

Baselines, as they pertain to cybersecurity, refer to the normal operation of enterprise endpoints. Building up a baseline requires more than just measuring performance, it entails secure configurations, settings, endpoint security software, apps and services – in short, the things that are necessary for users to perform their job functions safely and securely. This also infers adherence to compliance requirements and/or alignment with company policies.

Prevent known threats

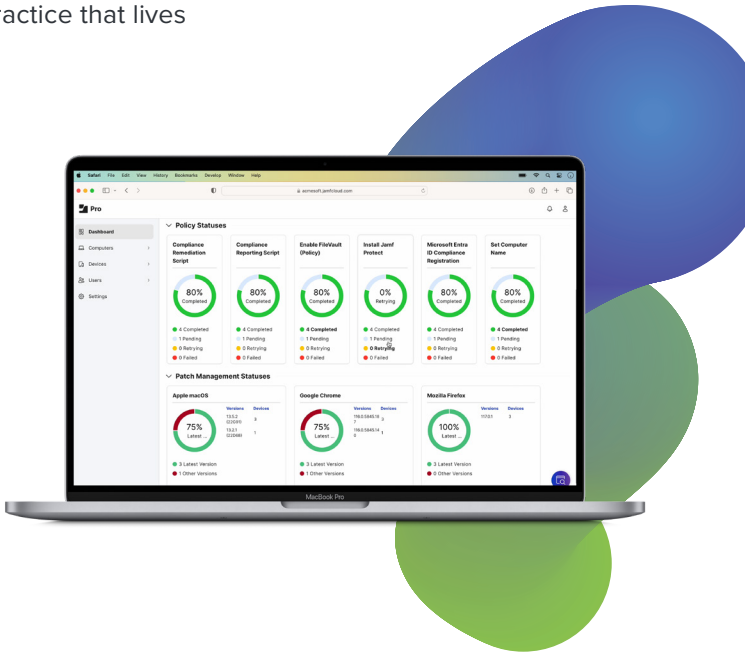
By setting up and capturing requisite parameters as baselines, administrators can better determine if endpoint health lies within acceptable boundaries. If not, endpoint logging will alert admins as to any discrepancies while providing the opportunity for manual mitigation to occur. Or, in the event of configured integration with your management solution, the telemetry data shared between both solutions will trigger the execution of automated workflows to remediate the incident.

Detecting unknown threats

The theme of proactive versus reactive is a central one to technology, and critical to keeping endpoints managed and secured as threats converge and evolve. One practice that lives on the edge proactively is threat hunting.

Effective performance of this task requires:

- Excellent data fertility for your environment
- Strong data analysis and pattern recognition skills
- Intimate knowledge of hardware and software
- Powerful security tools and how to use them
- Time, patience and diligence to investigate unknowns



ZTNA: Never trust, always verify

As time progresses, technologies once believed to be cutting-edge are relegated to become outdated, then obsolete, eventually becoming completely discontinued in favor of something typically faster, better and stronger. Zero Trust is a security model that addresses modern threat landscape challenges in a way that legacy technologies like VPN simply weren't designed to address.

Below are a few of the ways in which ZTNA, which integrates security, identity and management, establishes a new paradigm in cybersecurity.

Stop network-based threats

As a technologist, you're no doubt familiar with Firewalls. Namely, what they're used for and what they can do. While they're powerful appliances that provide perimeter-based security against network-based attacks, given today's migration to distributed workforces and reliance on personal devices for work, a Firewall protecting the perimeter of your LAN is not very useful for protecting employees working remotely and from their personal, unmanaged devices. ZTNA provides on-device and in-network protection against threats and attacks. Not only that, but it extends protection across multiple platforms to standardize security on computers and mobile devices alike running macOS, iOS, iPadOS, Windows or Android operating systems.

Isolate and encrypt connections

ZTNA also encrypts tunnels over any network connection and secures it further by remaining always-on – even enabling itself automatically if it becomes disabled by a user or malware. Additionally, ZTNA adds another layer of protection thanks to its integration with identity and access management: each time a connection to a protected resource is made, ZTNA generates its own unique microtunnel for that specific app or service. Not only does this stop Man-in-the-Middle (MitM) attacks which are common when using public hotspots, but it also prevents lateral movement across the network because microtunnels are isolated from each other. Lastly, it enforces the principle of least privilege, requiring users to authenticate but granting them explicit access to the resources assigned to them – all other parts of the network infrastructure are denied by default (unlike legacy VPN which grants access to the entire network once authenticated).

Verify endpoint health and access requests

Instead of "trusting" devices implicitly, zero-trust models require verification of endpoint and credential health each time a request is made. It compares the endpoint's current health status to what's tolerable by your organization. If it passes both checkpoints, access to the requested resource is granted. If either authentication or device health fails, access remains denied (default behavior) and remediation workflows are deployed to correct any discrepancies. After remediation has occurred, the checkpoints are performed again. Not until the device and credentials are verified does ZTNA grant access to the requested resource.

It does not matter if the mobile device:

- is company-issued or personally owned
- connects to the company network or public hotspot
- passes the device checkpoint but fails the credential checkpoint

Nor does not matter if the user account:

- belongs to a particular job role, like c-suite or executive
- successfully authenticated one hour before or five minutes ago
- passes the credential checkpoint yet fails the device checkpoint

"Never trust – always verify" means access is disabled, by default. Devices and credentials must pass verification: each and every time a request is made.

Advanced threat response: executive-level protection

Advanced Persistent Threats, or APTs have proliferated, targeting organizations in all industries globally.

In this section, we discuss defensive aspects that are open to administrators when integrating security and management solutions. By virtue of the threat intelligence data gathered and shared between both tools, a more comprehensive solution provides robust threat response and remediation of advanced threats that increasingly target key employee/role-targeted cyberattacks, like CEOs, among other high-risk individuals.

Key benefits of integrating security and management in mitigating risk from advanced threats are:

Gain visibility into mobile attacks

Mobile threats are on the rise. The modern threat landscape continues evolving threats and they are being aimed squarely at mobile devices and targeting their users year-over-year.

But, don't just take our word for it, here are some key findings that support our claims by the numbers:

- **43%** of all compromised devices were fully exploited (not jailbroken or rooted), an increase of **187%** year-over-year
- **80%** of phishing sites target mobile devices specifically or are designed to function both on desktop and mobile
- There was a **138%** increase in critical Android vulnerabilities discovered in 2022, while Apple iOS accounted for **80%** of the zero-day vulnerabilities actively being exploited in the wild
- Improper cloud storage configurations in mobile apps are a leading attack surface. **±2%** of all iOS and **±10%** of all Android mobile apps accessed insecure cloud instances
- The total number of unique mobile malware samples increased by **51%**, with more than **920,000** samples detected

Active monitoring and visibility are keys to obtaining insight into mobile attacks. Not only to identify them but also to realize the health status of endpoints accessing resources in your enterprise and to minimize risk factors before they can be exploited by threat actors.

After completing the task, the endpoint security solution re-scans the device to confirm threat mitigation. If successful, access to company resources is granted; if not, the request remains denied, and additional remediation steps may be needed.

Eliminate advanced, persistent threats

"An ounce of prevention is worth a pound of cure." – Benjamin Franklin

Understanding the threat landscape means realizing that while preventing threats is far and above greater than responding to one, we'd be remiss if we failed to point out that sometimes threats will affect devices and impact your network. When it comes to the level of sophistication behind APTs, it's more a question of "when", not "if", endpoints will be impacted. The key to being able to pivot quickly lies in how prepared your team is. To that end, their level of preparedness to tackle APTs will undoubtedly be affected by the tooling they're using and the quality of the data they're working with to remediate advanced threat types.

This is where security and management intersect to create advanced procedures and workflows that:

- Detect suspicious behavior
- Alert admins of the incident
- Assess threats for Indicators of Compromise (IoC) or Attack (IoA)
- Analyze findings from multiple threat intelligence sources
- Verify threat(s) as true-positive(s)
- Deploy mitigation strategies
- Perform remediation tasks, if necessary
- Scan the device to validate compliance

Depending on the severity level of the threat, the integration between security and management could augment manual incident response processes carried out by humans or may be performed automatically by your integrated solutions provider.

Reduce investigation times from weeks to minutes

Not all threats are created equally, and the increasing level of sophistication shown by some of the more recent threats and proof of concept (PoC) attacks requires a deeper, more thorough investigation by response teams and threat hunters to uncover the full impact of unknown threats. Historically, investigations could take weeks to complete, depending on the criticality of the threat and its complexity.

Advanced threats require advanced tools to detect and respond to incidents and attacks on mobile devices in an efficient method. Given the "mobile" nature of these endpoints, incident response must be capable of being performed remotely to not only discover but also respond to mobile attacks, this is made possible by converging desktop and mobile security to:

- Perform deep analysis to identify IoCs
- Construct timelines of suspicious events, showing when and how devices were compromised
- Present straightforward incident summaries that surface sophisticated zero-day attacks (that would otherwise remain hidden)
- Eliminate APTs with built-in tools while ongoing monitoring ensures threats are destroyed

Summary

Closing security gaps requires a modern cybersecurity approach. Layering comprehensive protections that extend security and privacy to all the devices, users and data across your infrastructure holistically. A single, powerful defense-in-depth solution that integrates management, identity and security.