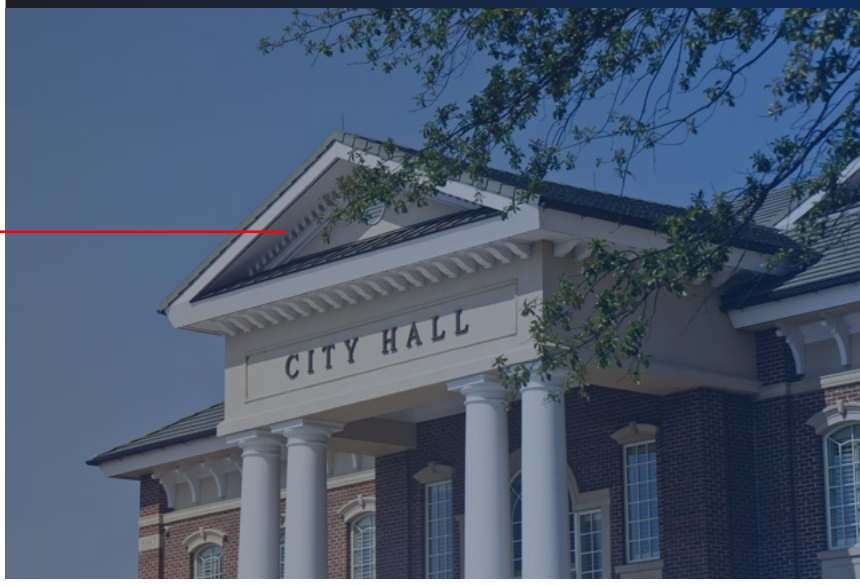
IronNet™

6 Misconceptions about Collective Defense for Cybersecurity

There is a powerful strategy gaining momentum in cybersecurity: Collective Defense.

This concept has circulated before in other realms: most notably as the foundation of NATO's historic Article 5, which states that an attack on one member is an attack on all members. Now, this collaborative approach is part of an urgent call to action by the U.S. Cyberspace Solarium Commission.

> **"The U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense."**
>
> **— U.S. CYBERSPACE SOLARIUM COMMISSION REPORT (P. 96)**



IronNet™

Collective Defense is the epitome of working together to **make a greater impact.**

Representing all industries and sectors, we are standing at a historical inflection point in how we conduct cyber defense. In the face of highly sophisticated adversaries with nearly limitless time and resources, individual organizations no longer can defend sufficiently, nor should they have to with the technology now available to make Collective Defense possible.

To mount an effective and affordable defense, we have to defend as teams across sectors, cities, states, and nations. Collective Defense uses collaboration and threat information sharing in new and powerful ways to reduce risk and improve the societal, commercial, and governmental ecosystems every enterprise depends upon to thrive.

Yet while the idea of Collective Defense sounds practical, it is understandable that there are questions about how Collective Defense works; how to operationalize it; and why it is safer, more beneficial, and much needed.

In this white paper, we will address some of these common concerns and misconceptions and, in turn, share lessons learned from our experience on the front lines of this profound turning point in cybersecurity.

1

MISCONCEPTION

"With Collective Defense, we are giving away our competitive advantage."

2

MISCONCEPTION

"With Collective Defense, we are placing data privacy at risk."

3

MISCONCEPTION

"We already share threat information, so this isn't any different."

4

MISCONCEPTION

"Integrating Collective Defense into my ecosystem will take too much time and require extra resources."

5

MISCONCEPTION

"Sharing information with the government is ineffectual."

6

MISCONCEPTION

"We're good with what we already have."

MISCONCEPTION

1

“

With Collective Defense, we are giving away our competitive advantage.

MISCONCEPTION

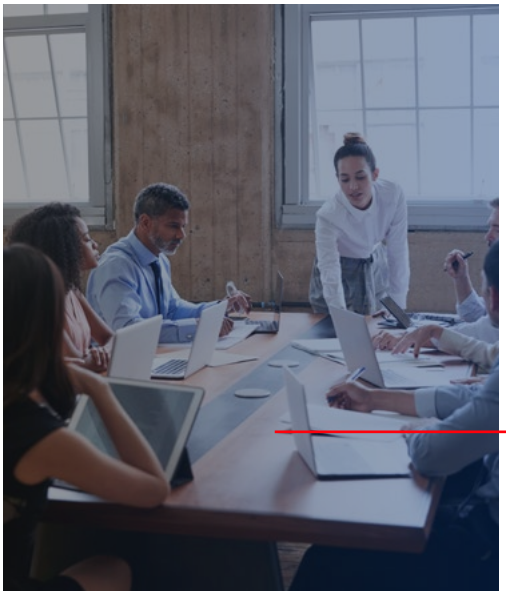
1

It is unsettling, but sometimes true, that some organizations would rather see their competitors collapse from a cyber attack than work together to confront common threats to the sector at large.Thankfully, this attitude is rare. We can look to the example of what happens during the aftermath of extreme weather events. We've all benefited from energy companies' mutual support agreements during natural disasters. The power comes back on faster because of teamwork. The next event may hit a different region of the country altogether, yet another company and population will benefit no matter where the disaster strikes.

Similarly in cyberspace, we face common threats and share global infrastructure. Working together benefits everyone in the ecosystem by keeping our shared cyber landscape healthy. A cyber attack on point-of-sale systems, inter-bank transfers, medical records, or the power grid hurts everyone, even competitors. We've seen sophisticated threat actors probe entire sectors looking for points of entry. Once in, they move laterally, either seeking to cause destruction or to gain covert access for later use.

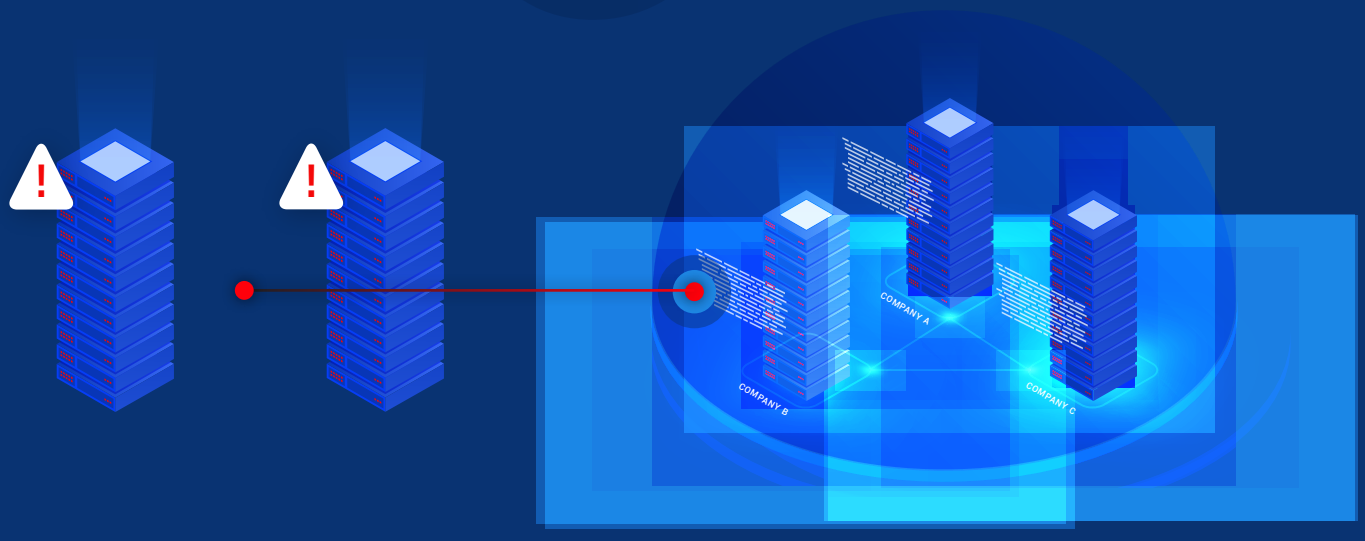
Air gap or not, no computing device or network is truly isolated over its lifetime. Due to complex interdependencies in computing systems, the effects of cyber attacks cascade and have a widespread impact on many. No single organization has sufficient analysts and threat intelligence to track all major threat groups and realistically monitor their activities in near real time. But with Collective Defense, we now have these capabilities, which we can share between and across sector ecosystems at network speed.

A cyber attack on point-of-sale systems, inter-bank transfers, medical records, or the power grid hurts everyone, even competitors.



If we keep operating as individual organizations in silos, we will lack visibility of our extensive supply chain and third-party networks. Within a mutual ecosystem, all stakeholders benefit from broader visibility across the threat landscape.

For example, large companies don't know the threats faced by the smaller partner companies they depend upon. Smaller companies can't invest sufficient resources and have limited threat information sharing, so they benefit from the visibility only a Collective Defense ecosystem provides.



Organizations of all sizes would save time and money through Collective Defense by avoiding redundancy and sharing resources. Tools such as behavioral analytics, which automate detection and simplify threat hunting, are powerful, complementary amplifiers that can reduce cost and improve efficiency.

What's more, Collective Defense weakens adversaries' ability to reuse the same tactics, techniques, and procedures (TTPs) to "cherry pick" enterprises individually as they do today.

Threat information isn't any single entity's competitive advantage; it benefits the sector at large, while also strengthening consumers' and B2B customers' trust in the business impact of digitally transformed enterprises. True, how a company operationalizes threat information can provide a competitive edge.

CISOs can measure the maturity of their organizations on how effectively threat intelligence is operationalized to ensure progress.

And that is how it should be. CISOs can measure the maturity of their organizations on how effectively threat intelligence is operationalized to ensure progress. Organizations also can measure the quality of the intelligence they receive so their company isn't awash in a sea of marginally useful Indicators of Compromise (IOCs) and wasting money on irrelevant noise. With insufficient intelligence, threat teams do not have the details to make appropriate assessments and recommendations. Additional context from a sharing partner will lead to more effective threat research and incident response teams, as well as build the reputation of the companies that choose to collaborate at network speed. Collective Defense is a win-win.

MISCONCEPTION

2

“

With Collective Defense, we are placing data privacy at risk.

MISCONCEPTION

2

Another misconception about Collective Defense is that it compromises data security and data privacy. At IronNet, we've been enabling companies to share threat information, even between competitors. The information shared in IronNet's Collective Defense platform, IronDome, isn't public, and corporate data privacy is protected through anonymized data sharing and encryption upon transit to / from the ecosystem. From our experience, useful threat information sharing does not have to disclose sensitive information about the internals of an individual company's network. By focusing on external threat actor activities, correlation, and anonymized alerts, IronDome can provide a common operating picture for all participants, while preserving privacy best practices and meeting regulatory requirements.

In other words, no company must give up data ownership or privacy by engaging in the IronDome Collective Defense ecosystem.

No company must give up data ownership or privacy by engaging in the IronDome Collective Defense ecosystem.

Data minimization is possible with the following steps:

Data protection

IronNet uses a rigorous, automated process for preventing disclosure of sensitive information. We leverage customer input and security expertise on metadata that contains sensitive information, in turn eliminating enterprise-identifying information such as IP addresses, domains, and other sensitive information such as personnel names or passwords.

Encryption

All data sent to the IronDome Collective Defense platform is encrypted before transmission. This encrypted information is pushed to the IronDome data repository where it is stored and analyzed. Data within the IronDome system is encrypted while at rest. All transmissions back to an individual participant's IronDefense system(s), where the network behavior data originates for analysis, are encrypted in the same manner.

Data enrichment protection

Within CloudConnect, the purpose of enrichment is to retrieve up-to-date information about external domains and IP addresses to enhance the behavior detections of IronDefense. These enrichments require constant updating and connection to the public internet. The enrichments are then used to prioritize the IronDefense detections.

In addition to these efforts, we prevent the disclosure of sensitive information by restricting data access according to privacy best practices and regulatory requirements.

MISCONCEPTION

3

“

We already share threat information, so this isn’t any different.

MISCONCEPTION

3

In light of advanced cybersecurity technologies, it is time to revisit the idea of sharing threat information. This approach is not new, as governments, intelligence agencies, and militaries have done this for ages. Nor is threat information sharing new to cybersecurity. Information Sharing and Analysis Center (ISAC) organizations, for instance, emerged 20 years ago to answer the U.S. government's call to action for public-private partnerships to defend against cyber threats. The ISACs have proven the value of sharing threat information. Collective Defense builds on the momentum and complements the strategic solutions of the ISACs to foster comprehensive sector-wide information sharing in near-real-time, in high quality, and with crowdsourced analysis. Lack of participation should be a risky exception rather than the rule.

Consider Experian's Data Breach Preparedness Study, released in February 2020, which found that **57% of more than 1,000 IT security, compliance, and privacy professional respondents** surveyed either are participating, or plan to participate, in a program to share data breach information and incident response plans. Collective Defense can raise the bar even higher in terms of speed, quality, and participation–well above today's levels.

The willingness is there.

Collective Defense can raise the bar even higher in terms of speed, quality, and participation–well above today's levels.

We shouldn't confuse today's threat intelligence platforms with Collective Defense. While there are similarities, the vast majority of threat information feeds are noisy and simply based on indicators of compromise, such as hashes or IP addresses.

Collective Defense is transformational, employing multilateral sharing of threats, machine-speed behavioral analytics, and collaborative analysis in near-real-time across communities facing common threat actors.

The result is both big picture context and tailored sector-specific intelligence that is actionable immediately.

We've had success facilitating threat information sharing within critical infrastructure sectors; however, we shouldn't stop at sector-level sharing. As Collective Defense builds critical mass, sector-level information can be aggregated into national-level views. With this data, we can do many things. Imagine sector-and national-level network behavioral analysis that operates in real time to detect and respond to previously uncorrelated threat actor behavior.

Collective Defense is transformational, employing multilateral sharing of threats, machine-speed behavioral analytics, and collaborative analysis in near-real-time across communities facing common threat actors.

We've already seen pilot programs that prove this idea. Further imagine an appropriately anonymized real-time map of the market visualization of cybersecurity threats and the advantages that would provide. Holistic visibility with big-picture, situational context and details on demand is the end state where we need to head.

MISCONCEPTION

4

“

Integrating Collective Defense into my ecosystem will take too much time and require extra resources.

MISCONCEPTION

4

We see Collective Defense in cyberspace as a social responsibility and a powerful opportunity to fortify digital trust.

Organizations across all national borders and industries research and respond to common threats, often on their own island. If Company A has 10 analysts and Company B has 20, these companies are duplicating research and wasting valuable time. A more effective model is to coordinate research efforts, allowing each company to dedicate more of their limited resources to implementation and remediation.

We have found that it is possible to quickly integrate Collective Defense technologies into security analyst workflows and senior leader decision making. The key is to ensure interoperability with existing security technologies, especially SIEMs and logging systems. By improving our technologies and leveraging APIs and cloud platforms, we have massively reduced complexity and the time required to get Collective Defense systems up and running quickly.

Collaboration and threat sharing are industry best practices, and organizations should align their security programs accordingly. While collaboration may be initially disruptive or cause concerns of propriety or prioritization, consider that your peers are undergoing the same transformation. As momentum builds, companies that don't form Collective Defense alliances will be left behind. We see Collective Defense in cyberspace as a social responsibility and a powerful opportunity to fortify digital trust.

We see Collective Defense in cyberspace as a social responsibility and **a powerful opportunity to fortify digital trust.**

IronNet CYBERSECURITY

MISCONCEPTION

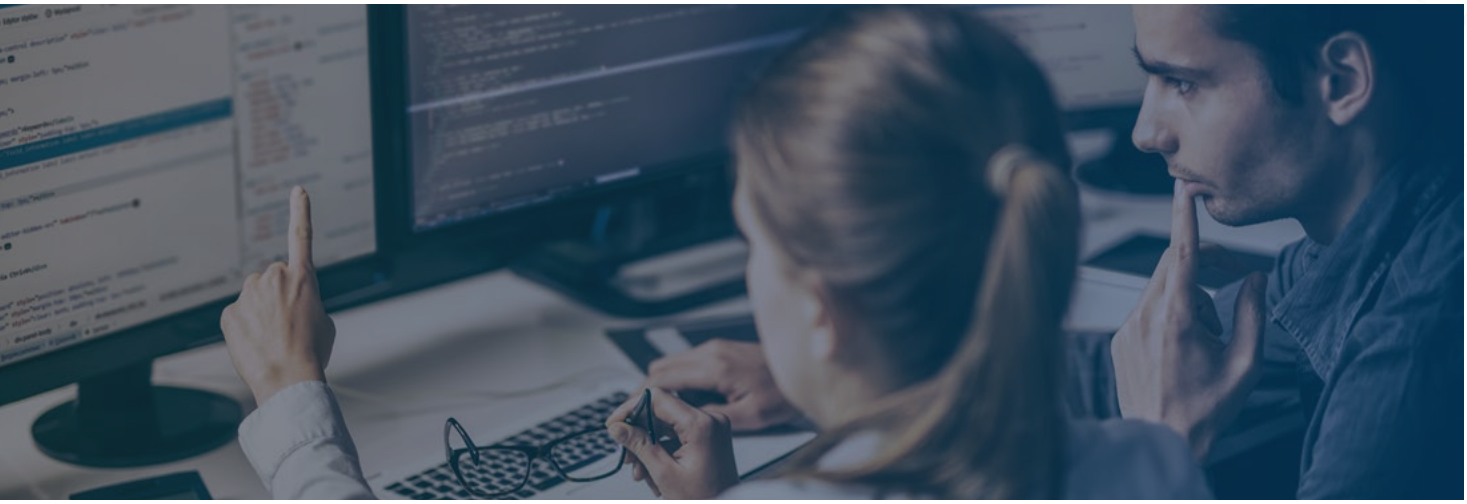
5

“

Sharing information with the government is ineffectual.

MISCONCEPTION

5



"While the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat … the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification."

— U.S. CYBERSPACE SOLARIUM COMMISSION REPORT, P. 101

The government cannot help defend the private sector if it is not aware of an event happening in the moment. The visibility just isn't there. If we incorporate government information sharing into a common operating picture, and in near real time, we will be better informed and be able to respond faster. In fact, the U.S. Cyberspace Solarium Commission recently called for the need for this bigger threat picture.

At present, without this broader visibility, response to detect threats is severely delayed; 60 days later is not adequate. With quicker detection and rapid response, national, state, and local governments can rapidly impose costs on attackers in ways that private organizations can't.

Based on our cyber experts' experience with the U.S. Cyber Command, we can say that the offense often wins by actively creating new exploits, constantly modifying malware, and massively scaling. If any entity only defends in any type of war, eventually it will lose. In most countries, the government maintains a monopoly on the use of force. Even companies and organizations that have strong cyber defenses, and many do not, sooner or later breaches do occur. We can direct more of the scarce people, money, and technology at the problem, but defense without offense remains a losing proposition.

Barring the discovery of perfect security, we need to take on a united, stronger defense posture to weaken threat actors. Government agencies have offensive capabilities and authorities at their disposal that private organizations simply do not. Yes, there are some interesting active defense measures, and the perennial bad idea of hacking back, but these techniques pale in comparison with what governments can bring to bear.

Barring the discovery of perfect security, we need to take on a united, stronger defense posture to weaken threat actors.

Governments have the ability to create and enforce laws, leverage diplomatic power, enact economic sanctions, conduct offensive cyber operations, and, when necessary, conduct kinetic military operations. Further, nations possess powerful intelligence communities that span the globe. The intelligence these organizations create is world-class and highly valuable for private sector defense.

Additionally, Collective Defense in the private sector generates the critical mass to get the government's attention among many competing priorities. Yes, there will be growing pains in working with the government, but the will is there.

MISCONCEPTION

6

“

We’re good with what we already have.

MISCONCEPTION

6

Cybersecurity is constantly evolving, and threat actors are continuously adapting threat techniques and creating more sophisticated attacks. Who wouldn't want to improve their organization's security posture? Even if a company does have robust defenses, we all should look left and right at the supplier and partner organizations ecosystems we so heavily depend on.

Organizations will sneak into a side door of this broader network to undermine the common and expansive ecosystems it needs to thrive.

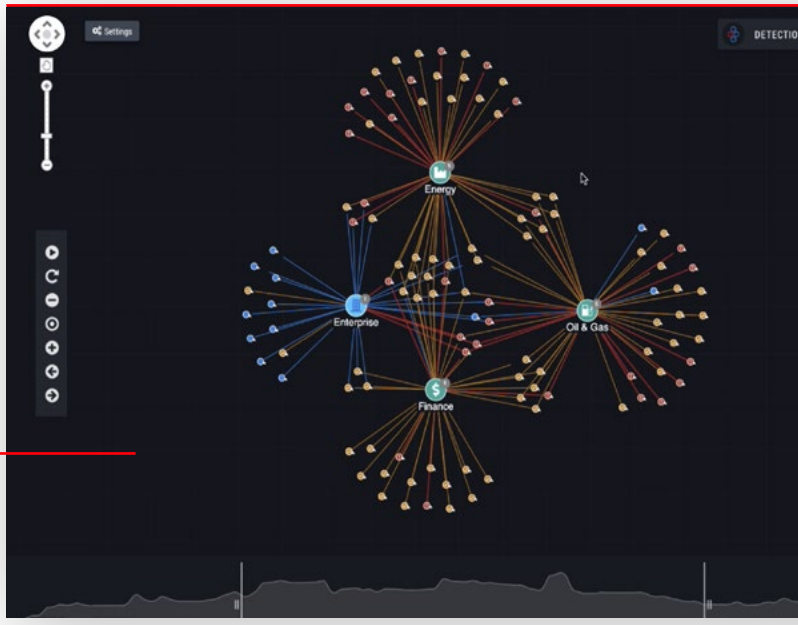
Whether that door is accounting software or an HVAC system, or even a lobby fish tank, attackers will find and exploit the weakest link in your layered defenses.

Even if a company does have robust defenses, we all should look left and right at the supplier and partner organizations ecosystems we so heavily depend on.

Collective Defense strengthens cybersecurity by providing broader visibility across the threat landscape. The ability to share threat information in near real time is transformative, as this is how cybersecurity teams across participating organizations in IronDome communities learn from threats that affect every member, reducing "alert fatigue" while improving mitigation prioritization, triage, and efficiency for all. Consider the ripple effect that results from more accurate and timely threat intelligence sharing: **proactive defense.**

The IronDome's Detection Correlation Dashboard (DCD) maps this threatscape visually, with the situational context necessary for knowing the severity level and behavior of each threat. Often these threats are the covert marks of cyber adversaries working undetected in our networks. Once we can share these contextualized, visualized patterns (e.g., lateral movement, malicious DNS tunneling) in near real time across a community of companies, organizations, states, and even nations, we have the ability to respond and defend more quickly and on a larger scale.

Once we can share these contextualized, visualized patterns (e.g., lateral movement, malicious DNS tunneling) in near real time across a community of companies, organizations, states, and even nations, we have the ability to respond and defend more quickly and on a larger scale.



Collective Defense: working together to strengthen cybersecurity for all

In this white paper, we explained some misconceptions surrounding Collective Defense and why every organization or company should seriously consider this powerful strategy.

A new paradigm, Collective Defense, is urgently needed to defend companies, corporate ecosystems (including supply chains), cities, states, business sectors, and nations. A business-as-usual individual defense is costly and less secure. Collective Defense has many benefits, including greater visibility, greater speed, reduced redundancy, and lower cost. We must change the way we are doing things today — today.

The power of Collective Defense grows exponentially via the network effect — the addition of each new member increases visibility, correlation capability, and analytic resources. We've seen Collective Defense exceed expectations in the energy sector where we've brought together a wide range of companies, both large and small, using real-time threat information sharing infrastructure and behavioral analytics. Now we are launching similar initiatives in other sectors, and internationally.

The future of Collective Defense is bright. As the volume of data grows, so does its utility. Once a Collective Defense system gains enough critical mass, it becomes a highly valuable multidimensional repository of anonymized information. Members of the collective then can generate multiple desired views of the data, based on their own particular needs. Our ambitious roadmap will allow organizations to view the security status of their sector, city, corporate ecosystem, and supply chain — all at the same time.

Shared threat information is just the start of true Collective Defense. We are moving forward in a number of complementary areas: collective exercises and training, interoperability, standardized operating procedures, automated response, and mutual support agreements, among others. If you are interested in learning more about what Collective Defense can do for you, please contact us. **Together, we are stronger.**

DISCOVER IRONNET
COLLECTIVE DEFENSE.

ironnet.com/CollectiveDefense

(443)-300-6761 | info@ironnet.com
ironnet.com

IronNet™