Protect your Zero Trust Data Center, your Castle

The data center holds your organization's crown jewels, your most sensitive data and applications, on-premises or in the cloud. No matter the location, it is essential to keep it protected. It is critical to understand the components of the Zero Trust data center and ensure you have the safeguards in place to protect your organization to keep your data safe and secure.

Lack of Visibility

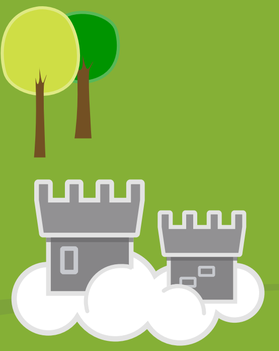
Visibility across the entire network is critical to quickly assess the application and network health and identify potentially malicious activity. You can't protect against what you can't see.

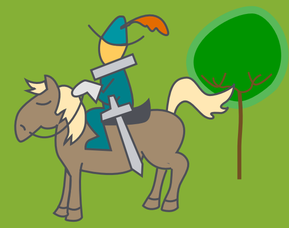
The Crown Jewels

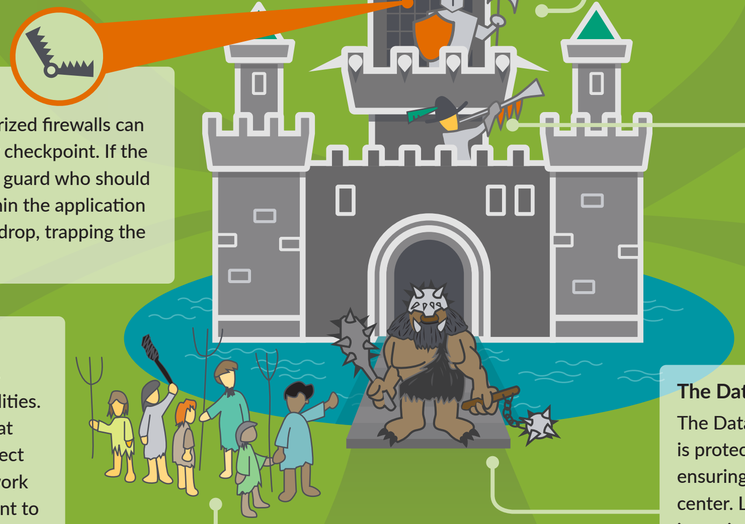
The crown jewels are your most business-critical and sensitive data and applications, whether on-premises or in the cloud. If this information got into the wrong hands, the results could be catastrophic for the business.

Threats on the Road

Threats are introduced into the network from many different vectors, and the attack objectives vary. Regardless of the intent or the techniques employed, it is essential to keep your castle protected with right tools at your disposal.







Intra-Data Center

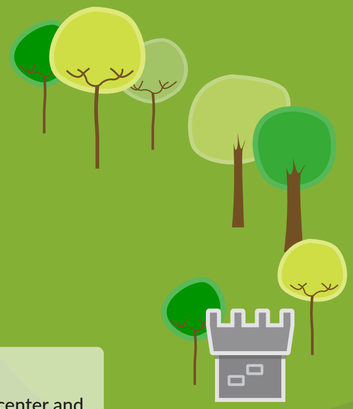
The firewall performs another check between servers with protected east-west and north-south communications between groups of services and applications, ensuring that all resources and applications on different servers aren't compromised. We can determine how traffic can access a specific application, and the way certain users can access it.

Cloud Workload Protection

We must protect individual applications. Containerized firewalls can be deployed for each application, which is another checkpoint. If the room with the crown jewels is breached, there is a guard who should stop the attack. Cloud Workload Protection is within the application itself. If the crown jewels are moved, the gate will drop, trapping the attacker, and banishing them to the dungeon.

The Data Center Interconnect

The Data Center Interconnect is the passage for communication between data center locations. Most organizations have a mix of data center environments. Having a robust router is essential for protecting traffic between clouds and on-premises environments. Then, if an attacker breaches the castle, they can't get into all of the locations.



Business Continuity

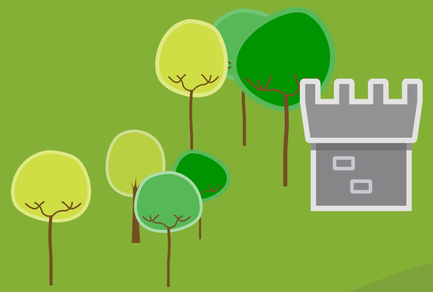
Organizations need reliable connectivity and must maintain business continuity and ensure consistent security policies with a quality experience and access to services, no matter where an organization's data centers are located. Like a Sheriff on the passages between data centers, management helps deliver orchestration and monitoring to deployments anywhere and everywhere, on-premises and in the cloud.

The Siege at the Castle

No matter what you do, there are always attackers looking to storm the castle by exploiting vulnerabilities. You must be prepared. Security must be about what you see, what you know, and what you do. To protect the castle, you must enable the threat-aware network by extending visibility, intelligence, and enforcement to every point of connection from client to workload.

The Data Center WAN Gateway

The Data Center WAN Gateway is the entry into the data center and is protected by firewalls that check the incoming and outgoing traffic, ensuring that users and devices have the right access to the data center. Like a security checkpoint to get into the castle, we check the incoming traffic to make sure hidden malware isn't sneaking in.



THE THREAT-AWARE NETWORK FOR THE CLOUD ERA

A Zero Trust Data Center delivers the threat-aware network and ultimately improves security while reducing complexity and streamlining management. When organizations empower the network to be threat-aware, attacks are detected sooner, and attackers are less likely to gain a foothold in the network, which safeguards users, applications, infrastructure, and of course, your crown jewels.

Juniper Networks

PN: 3050145